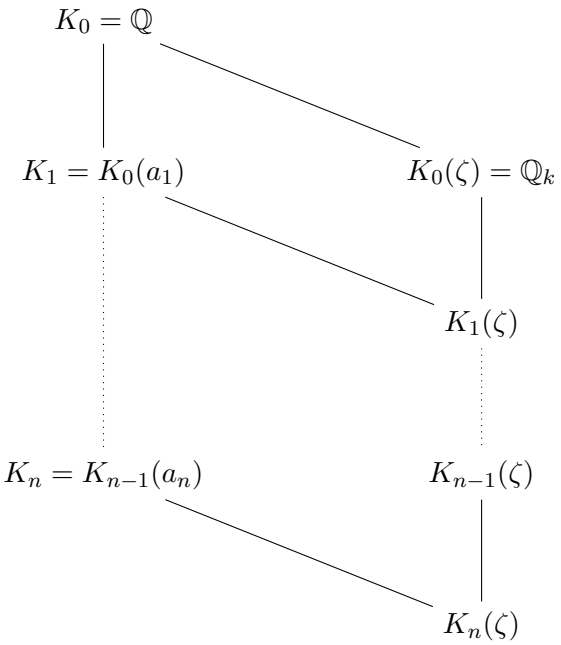
Algebra

Lecture notes winter semester 2018/19
and summer semester 2019

Benjamin Sambale

Version: April 11, 2026



Contents

Preface 6

Algebra I 7

I.1 Motivation 8

I.2 Number Theory 9

I.3 Groups 19

I.4 Group Actions 29

I.5 Abelian Groups 36

I.6 Solvable and simple groups 40

I.7 Rings 45

I.8 Polynomials 52

I.9 Field Extensions 63

I.10 Galois Theory 67

I.11 Finite Fields 73

I.12 Cyclotomic Fields 78

I.13 Algebraic Closure 84

I.14 Solvability of Equations 88

I.15 Construction with Compass and Straightedge 96

Exercises 101

Algebra II 113

II.1 Set Theory 114

II.2 Applications of Zorn's Lemma 118

II.3 Separable Extensions 121

II.4 Transcendental Extensions 128

II.5 Divisibility in Integral Domains 135

II.6 Modules 143

II.7 Finiteness conditions 147

II.8 Semisimple and Artinian Rings 155

II.9 Modules over Principal Ideal Rings 165

II.10 Frobenius Normal Form 175

II.11 Prime Ideal Decomposition in Dedekind Domains 181

II.12 Finite-dimensional algebras 194

II.13 Symmetric Algebras and Group Algebras 206

II.14 Representations and Characters 218

Exercises 236

Algebra III 249

III.1 Commutative Algebra 250

III.2 Algebraic Geometry 260

III.3 Modular Representation Theory 276

III.4 Representations of the symmetric group 297

III.5 Category Theory 315

III.6 Morita Theory 325

III.7 Central Simple Algebras 340

III.8 Path algebras 357

III.9 Lie Algebras 367

III.10 Valuation Rings 396

III.11 General Galois Theory 416

III.12 Coding Theory 430

Exercises 447

Appendix 459

A.1 Quadratic Residues 460

A.2 Zero regions and eigenvalues 464

A.3 Cyclotomic Polynomials 468

A.4 Analytical Proof of the Fundamental Theorem of Algebra 479

A.5 Transcendental Extensions 480

A.6 Automorphism Groups of Number Fields 484

A.7 Artin-Schreier Theory 486

A.8 Separable Algebras 490

A.9 Profinite groups 496

A.10 The Lindemann-Weierstraß Theorem 504

A.11 Rings with Finiteness Condition 509

A.12 Free Modules with Infinite Rank 510

A.13 Group Determinants 512

A.14 Frobenius-Schur Indicators 515

GAP Commands 520

Index 523

Warning: This is an AI-translated version of my German lecture notes, performed by *Gemini 3 Flash Preview*. I have not checked whether Gemini introduced errors. Use with care!

Preface

The first two parts (Algebra I & II) of the present notes originated from $(4+2)$-lectures in the winter semester 2018/19 (15 weeks) and summer semester 2019 (14 weeks) at the Friedrich Schiller University Jena and are primarily aimed at students in the Bachelor and Master of Mathematics programs. Knowledge of Linear Algebra 1–2 and Analysis 1 is assumed. The topics can mostly be found in the following books:

- Karpfinger, Meyberg: *Algebra*, 4th edition, Springer Spektrum, 2017
- Wüstholz: *Algebra*, 2nd edition, Springer Spektrum, 2013
- Bosch: *Algebra*, 7th edition, Springer Spektrum, 2013
- Jantzen, Schwermer : *Algebra*, 2nd edition, Springer Spektrum, 2014
- Rotman: *Advanced Modern Algebra 1 & 2*, 3rd edition, AMS, 2017
- Isaacs: *Algebra*, AMS, 1994

Many contents were added later (in particular, the lecture "Algebra III" never existed). In the appendix, some highlights of algebra are discussed that do not find a place in an ordinary lecture. The notes in its current form serves me mainly as my own reference. Further lecture notes are available on my homepage. I would like to thank Darij Grinberg, Burkhard Külshammer, Till Müller and Claude Sonnet for several corrections.

Algebra I

I.1 Motivation

Is there a solution formula for the equation

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0 \qquad (a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q})? \tag{I.1.1}$$

- $n = 1$: $x = -a_0$ is the only solution.
- $n = 2$: $x = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_0}$ (p-q-formula).
- $n = 3$: Solved by Tartaglia, del Ferro and Cardano:[1] The substitution $y = x + \frac{a_2}{3}$ leads to

  $$y^3 + py + q = 0$$

  for certain $p, q \in \mathbb{Q}$. The ansatz $y = u + v$ yields $u^3 + v^3 = -q$ and $u^3 v^3 = -p^3/27$. Therefore u^3 and v^3 are the solutions of

  $$z^2 + qz - \frac{p^3}{27} = 0.$$

  One obtains

  $$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

  with a suitable choice of the cubic roots. Even if all solutions are real, complex numbers are usually required for their representation (this phenomenon is called *casus irreducibilis*).
- $n = 4$: Solved by Ferrari and Cardano: With the substitution $y = x + \frac{a_3}{4}$ one obtains

  $$y^4 + py^2 + qy + r = 0.$$

  The ansatz $y^4 + py^2 + qy + r = (y^2 + sy + u)(y^2 - sy + v)$ leads to

  $$s^6 + 2ps^4 + (p^2 - 4r)s^2 - q^2 = 0.$$

  Thus, the problem has been reduced to a cubic equation in s^2. Subsequently, one calculates $u = \frac{1}{2}(s^2 + p - q/s)$, $v = s^2 + p - u$ and solves the two quadratic equations for y.
- $n \geq 5$: There is no general formula! (Theorem of Abel-Ruffini)

Further goals of the lecture:

- Fundamental Theorem of Algebra: Equation I.1.1 has exactly n complex solutions counted with multiplicities.
- Which regular n-gons can be constructed with compass and straightedge? (equilateral triangle and square are easy, pentagon more difficult, 7-gon is not possible).
- Squaring the circle: With compass and straightedge, it is not possible to construct a square that has the same area as the unit circle.

[1] for the historical background see Wikipedia

I.2 Number Theory

Remark I.2.1. We use the usual number systems:

- Natural numbers: $\mathbb{N} = \{1, 2, \ldots\}$, $\mathbb{N}_0 = \{0, 1, \ldots\}$.
- Integers: $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$.
- Rational numbers: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\}$.
- Real numbers: $\mathbb{R}$ (Analysis).
- Complex numbers: $\mathbb{C} = \{a + b\mathrm{i} : a, b \in \mathbb{R}\}$.

Theorem I.2.2 (Euclidean division)**.** *For $a \in \mathbb{Z}$ and $d \in \mathbb{N}$, there exist uniquely determined $q, r \in \mathbb{Z}$ with $a = qd + r$ and $0 \leq r < d$.*

Proof. Obviously, the set $M := \{a - cd : c \in \mathbb{Z} \text{ with } a - cd \geq 0\} \subseteq \mathbb{N}_0$ is not empty and therefore possesses a minimal element $r := a - qd \geq 0$ with $q \in \mathbb{Z}$. In the case $r \geq d$, then $a - (q+1)d = r - d \in M$ would also hold, in contradiction to the minimality of r. Thus $0 \leq r < d$. Now let $q', r' \in \mathbb{Z}$ with $a = q'd + r'$ and $0 \leq r' < d$. From $d|q - q'| = |dq - dq'| = |r' - r| < d$ it then follows that $q = q'$ and $r = r'$. □

Remark I.2.3. One calls r in Theorem I.2.2 the *remainder* in the division of a by d.

Example I.2.4. The division of 20 by 7 leaves remainder 6, because $20 = 2 \cdot 7 + 6$.

Definition I.2.5. For $a, b \in \mathbb{Z}$, one says a *divides* b (or a is a *divisor* of b or b is *divisible* by a), if there exists a $c \in \mathbb{Z}$ with $ac = b$. One then writes $a \mid b$.

Lemma I.2.6. *For $a, b, c, d, e \in \mathbb{Z}$ the following holds:*

(i) $\pm 1 \mid a \mid 0$,

(ii) $0 \mid a \iff a = 0$,

(iii) $a \mid b \mid c \implies a \mid c$,

(iv) $a \mid b \mid a \implies a = \pm b$,

(v) $a \mid b, c \implies a \mid (bd + ce)$,

(vi) $a \mid b \neq 0 \implies |a| \leq |b|$.

Proof. All statements are easy. We prove (iv) as a sample. Because of $a \mid b \mid a$, there exist $c, d \in \mathbb{Z}$ with $ac = b$ and $bd = a$. Thus $a = bd = cda$. In the case $a = 0$, then $b = ac = 0$ as well. Otherwise, $cd = 1$ and $c = \pm 1$. Then $a = \pm b$. □

Definition I.2.7. For $a_1, \ldots, a_n \in \mathbb{Z}$ let

$$\mathrm{cd}(a_1, \ldots, a_n) := \{d \in \mathbb{Z} : d \mid a_1, \ldots, a_n\}$$

be the set of *common divisors* of $a_1, \ldots, a_n$. A $g \in \mathrm{cd}(a_1, \ldots, a_n) \cap \mathbb{N}_0$ is called the *greatest common divisor* of $a_1, \ldots, a_n$, if $d \mid g$ holds for all $d \in \mathrm{cd}(a_1, \ldots, a_n)$. One then writes $\gcd(a_1, \ldots, a_n) := g$. In the case $\gcd(a_1, \ldots, a_n) = 1$, one calls $a_1, \ldots, a_n$ *coprime*.

Remark I.2.8.

(i) If g and g' are greatest common divisors of $a_1, \ldots, a_n$, then $g \mid g' \mid g$ and $g = \pm g'$ according to Lemma I.2.6(iv). Since $g, g' \geq 0$, it follows that $g = g'$, i. e. there exists at most one common divisor of $a_1, \ldots, a_n$ (this justifies the notation gcd).

(ii) The term "greatest common divisor" is misleading, because $\mathrm{cd}(0, 0) = \mathbb{Z}$, but $\gcd(0, 0) = 0$.

(iii) For the calculation of $\gcd(a_1, \ldots, a_n)$, one can obviously assume $a_1 > \ldots > a_n > 0$. For $d \in \mathrm{cd}(a_1, \ldots, a_n)$, it holds that $d \mid a_1$ and $d \mid \gcd(a_2, \ldots, a_n)$. Thus

$$\mathrm{cd}(a_1, \ldots, a_n) \subseteq \mathrm{cd}(a_1, \gcd(a_2, \ldots, a_n)).$$

Conversely, for $d \in \mathrm{cd}(a_1, \gcd(a_2, \ldots, a_n))$, it holds that $d \mid \gcd(a_2, \ldots, a_n) \mid a_i$ for $i = 2, \ldots, n$, hence $d \in \mathrm{cd}(a_1, \ldots, a_n)$. This shows

$$\gcd(a_1, \ldots, a_n) = \gcd(a_1, \gcd(a_2, \ldots, a_n)).$$

It is therefore sufficient to be able to calculate the gcd of two natural numbers.

(iv) Let $a > b > 0$. Euclidean division yields $a = bq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < b$. According to Lemma I.2.6(v), $\mathrm{cd}(a, b) = \mathrm{cd}(bq + r, b) = \mathrm{cd}(r, b)$ and therefore $\gcd(a, b) = \gcd(r, b)$. In the case $r > 0$, one can divide b by r with remainder and thereby obtain increasingly smaller numbers. At the end, $\gcd(a, b) = \gcd(r, b) = \ldots = \gcd(d, 0) = d$. In particular, the gcd always exists. The following theorem provides more precise information.

Theorem I.2.9 (Extended Euclidean algorithm)**.**
Input: $a, b \in \mathbb{N}$.
Initialization: $(x_0, y_0, z_0) := (1, 0, a)$, $(x_1, y_1, z_1) := (0, 1, b)$ *and* $k := 0$.
While $z_{k+1} > 0$ *repeat:*
Euclidean division: $z_k = q_{k+1} z_{k+1} + r_{k+1}$ *with* $0 \leq r_{k+1} < z_{k+1}$.
Set $(x_{k+2}, y_{k+2}, z_{k+2}) := (x_k - x_{k+1} q_{k+1}, y_k - y_{k+1} q_{k+1}, r_{k+1})$ *and* $k := k + 1$.
Output: $z_k = x_k a + y_k b = \gcd(a, b)$.

Proof. Because $z_1 > r_1 = z_2 > r_2 = z_3 > \ldots$, the algorithm terminates. At the end, it holds that

$$\begin{aligned} z_k &= \gcd(z_k, 0) = \gcd(z_k, z_{k+1}) = \gcd(z_k, r_k) = \gcd(z_k, z_{k-1} - q_k z_k) \\ &= \gcd(z_k, z_{k-1}) = \ldots = \gcd(z_0, z_1) = \gcd(a, b). \end{aligned}$$

For $i = 0, 1$, it holds that $x_i a + y_i b = z_i$. Inductively, it follows that

$$\begin{aligned} x_{i+1} a + y_{i+1} b &= (x_{i-1} - x_i q_i) a + (y_{i-1} - y_i q_i) b = x_{i-1} a + y_{i-1} b - (x_i a + y_i b) q_i \\ &= z_{i-1} - z_i q_i = r_i = z_{i+1}. \end{aligned}$$

Therefore $\gcd(a, b) = z_k = x_k a + y_k b$. □

Example I.2.10. For $a := 45$ and $b := 24$, one obtains:

x_i	y_i	z_i	q_i
1	0	45	
0	1	24	1
1	-1	21	1
-1	2	$\boxed{3}$	7
		0	

Thus $\gcd(45, 24) = 3 = -45 + 2 \cdot 24$.

Corollary I.2.11. *For $a_1, \ldots, a_n, b \in \mathbb{Z}$, it holds that*

$$\gcd(a_1, \ldots, a_n) \mid b \iff \exists b_1, \ldots, b_n \in \mathbb{Z} : a_1 b_1 + \ldots + a_n b_n = b.$$

Proof. Let $g := \gcd(a_1, \ldots, a_n)$.

$\Rightarrow$: Let $gd = b$. According to Remark I.2.8(iii) and Theorem I.2.9, there exist $c_1, \ldots, c_n \in \mathbb{Z}$ with $g = a_1 c_1 + \ldots + a_n c_n$. The assertion follows with $b_i := dc_i$ for $i = 1, \ldots, n$.

$\Leftarrow$: Because $g \mid a_i$ for $i = 1, \ldots, n$, it holds that $g \mid a_1 b_1 + \ldots + a_n b_n = b$. □

Definition I.2.12. One calls $v \in \mathbb{Z}$ a *common multiple* of $a_1, \ldots, a_n \in \mathbb{Z}$ if $a_i \mid v$ holds for $i = 1, \ldots, n$. A common multiple $v \in \mathbb{N}_0$ is called the *least common multiple* if v divides every common multiple of $a_1, \ldots, a_n$. One then writes $\operatorname{lcm}(a_1, \ldots, a_n) := v$.

Remark I.2.13. As with the gcd, one shows that at most one lcm exists. Furthermore,

$$\operatorname{lcm}(a_1, \ldots, a_n) = \operatorname{lcm}(a_1, \operatorname{lcm}(a_2, \ldots, a_n)).$$

We calculate the lcm via a detour.

Definition I.2.14. One calls $p \in \mathbb{N}$ a *prime number* if p has exactly two positive divisors, namely 1 and p. We denote the set of prime numbers by $\mathbb{P}$. One calls $p \in \mathbb{P}$ a *prime divisor* of $a \in \mathbb{Z}$ if $p \mid a$.

Remark I.2.15.

(i) Note: 1 is *not* a prime number!

(ii) Two different prime numbers are always coprime.

Lemma I.2.16.

(i) For $a, b \in \mathbb{Z}$ and $p \in \mathbb{P}$, it holds that $p \mid ab \Longrightarrow p \mid a \vee p \mid b$.

(ii) Every $a \in \mathbb{N} \setminus \{1\}$ possesses a prime divisor.

Proof.

(i) Let $p \mid ab$ and $p \nmid a$. According to the Euclidean algorithm, there exist $c, d \in \mathbb{Z}$ with $1 = \gcd(a, p) = ac + pd$. It follows that $p \mid abc + pbd = b1 = b$.

(ii) Let $p > 1$ be a smallest possible divisor of a (if necessary $p = a$). In the case $p \notin \mathbb{P}$, there exists $1 < q < p$ with $q \mid p \mid a$ in contradiction to the choice of p. Thus $p \in \mathbb{P}$. □

Theorem I.2.17 (EUCLID)**.** *There are infinitely many prime numbers.*

Proof. Assumption: $\mathbb{P} = \{p_1 = 2, \ldots, p_n\}$. According to Lemma I.2.16, there exists a prime divisor q of $a = p_1 \ldots p_n + 1$. According to the assumption, $q \in \{p_1, \ldots, p_n\}$ and one obtains the contradiction $q \mid (a - p_1 \ldots p_n) = 1$. □

Theorem I.2.18 (Unique prime factorization)**.** *For every $n \in \mathbb{N}$, there exist uniquely determined $a_p \in \mathbb{N}_0$ for $p \in \mathbb{P}$ with*

$$n = \prod_{p \in \mathbb{P}} p^{a_p}.$$

Proof. Induction on n: In the case $n = 1$, $a_p = 0$ for all $p \in \mathbb{P}$. Now let $n \geq 2$ and p be a prime divisor of n. By induction, n/p has a prime factorization and therefore so does $n = p \cdot n/p$. Let $n = \prod p^{a_p} = \prod p^{b_p}$ and $a_q < b_q$ for some $q \in \mathbb{P}$. Then

$$q \mid \frac{n}{q^{a_q}} = \prod_{p \neq q} p^{a_p}$$

and Lemma I.2.16(i) shows $q = p$ for some $p \in \mathbb{P} \setminus \{q\}$. Contradiction. □

Example I.2.19. Let $k \geq 2$ and $n \in \mathbb{N}$ not be the k-th power of a natural number. Then $\sqrt[k]{n}$ is irrational, because otherwise there exist coprime $a, b \in \mathbb{N}$ with $\sqrt[k]{n} = a/b$. Then $nb^k = a^k$. The unique prime factorization shows $b^k = 1$ and one obtains the contradiction $n = a^k$.

Remark I.2.20.

(i) The divisors of $n = \prod_{p \in \mathbb{P}} p^{a_p}$ have the form $n = \prod_{p \in \mathbb{P}} p^{a'_p}$ with $0 \leq a'_p \leq a_p$ for all $p \in \mathbb{P}$. For $m = \prod_{p \in \mathbb{P}} p^{b_p}$ it therefore holds that

$$\boxed{\gcd(n, m) = \prod_{p \in \mathbb{P}} p^{\min\{a_p, b_p\}}, \quad \operatorname{lcm}(n, m) = \prod_{p \in \mathbb{P}} p^{\max\{a_p, b_p\}}.}$$

This shows

$$\boxed{nm = \gcd(n, m) \operatorname{lcm}(n, m),}$$

since $a_p + b_p = \min\{a_p, b_p\} + \max\{a_p, b_p\}$. Since no fast algorithm for prime factorization is known, the Euclidean algorithm for calculating gcd and lcm is generally to be preferred.

(ii) Theorem I.2.18 allows the following generalization of Lemma I.2.16(i): If $a, b \in \mathbb{Z}$ are coprime and $a \mid bc$, then $a \mid c$ follows.

Definition I.2.21. For $a, b \in \mathbb{Z}$ and $d \in \mathbb{N}$ we write $a \equiv b \pmod{d}$, if $d \mid (a - b)$. One then says: a and b are *congruent modulo d*.

Example I.2.22.

(i) In the decimal system one calculates modulo 10 and in the binary system modulo 2.

(ii) One considers seconds and minutes modulo 60 and hours modulo 12 or 24.

(iii) Days of the week are counted modulo 7.

(iv) Euro cents are calculated modulo 100.

(v) In music one considers notes modulo 8 (*c, d, e, f, g, a, h*) or 12 (*c, cis, d, ..., h*).

Theorem I.2.23. *The congruence modulo $d \in \mathbb{N}$ is an equivalence relation on $\mathbb{Z}$, i. e. it holds that*

(i) $a \equiv a \pmod{d}$ (*reflexive*),

(ii) $a \equiv b \pmod{d} \Longrightarrow b \equiv a \pmod{d}$ (*symmetric*),

(iii) $a \equiv b \equiv c \pmod{d} \Longrightarrow a \equiv c \pmod{d}$ (*transitive*).

Furthermore, it holds that

(iv)

$$\left.\begin{array}{ll} a \equiv a' & \pmod{d} \\ b \equiv b' & \pmod{d} \end{array}\right\} \Longrightarrow a \dot{+} b \equiv a' \dot{+} b' \pmod{d}.$$

Proof.

(i) $d \mid 0 = a - a$.

(ii) $d \mid a - b \Longrightarrow d \mid -(a - b) = b - a$.

(iii) $d \mid a - b \wedge d \mid b - c \Longrightarrow d \mid (a - b) + (b - c) = a - c$.

(iv) Let $d \mid a - a'$ and $d \mid b - b'$. Then it follows that $d \mid (a - a') + (b - b') = (a + b) - (a' + b')$ as well as $d \mid (a - a')b + (b - b')a' = ab - a'b'$. □

Remark I.2.24. The equivalence classes in the situation of Theorem I.2.23 are called *residue classes* modulo d. They have the form $a + d\mathbb{Z} := \{a + cd : c \in \mathbb{Z}\}$ for $a \in \mathbb{Z}$ (all elements in $a + d\mathbb{Z}$ leave the same remainder upon division by d). The set of all residue classes modulo d is denoted by $\mathbb{Z}/d\mathbb{Z}$. Obviously,

$$\mathbb{Z}/d\mathbb{Z} = \{0 + d\mathbb{Z} = d\mathbb{Z},\, 1 + d\mathbb{Z}, \ldots, d - 1 + d\mathbb{Z}\}$$

and $|\mathbb{Z}/d\mathbb{Z}| = d$.

Example I.2.25.

(i) Equation (iv) simplifies many calculations. We check whether $7^{90} + 111^7$ is divisible by 5:

$$7^{90} + 111^7 \equiv 2^{90} + 1^7 \equiv 4^{45} + 1 \equiv (-1)^{45} + 1 \equiv 0 \pmod{5}.$$

In Corollary I.7.18 we show that one may also reduce the exponents, however modulo 4.

(ii) (DHM *key exchange*) For confidential communication, Euler and Gauss must first agree on a secret key. For this purpose, a prime number $p > 10^{1000}$ and a number $1 < n < p$ are chosen (publicly). Euler chooses secretly and randomly $a \in \mathbb{N}$ and sends $n^a + p\mathbb{Z}$ to Gauss. Gauss chooses secretly and randomly $b \in \mathbb{N}$ and sends $n^b + p\mathbb{Z}$ to Euler. Both can now use $(n^a + p\mathbb{Z})^b = n^{ab} + p\mathbb{Z} = (n^b + p\mathbb{Z})^a$ as a secret key. Since no efficient algorithm for calculating the *discrete logarithm* (for example, to calculate a from $n^a + p\mathbb{Z}$ and n) is known so far, this procedure is currently secure.[1]

[1] This simple principle was only discovered in the 1970s by Diffie, Hellman, and Merkle. At that time, Alan Turing, the decoder of the Enigma from the Second World War, had already been dead for 20 years.

Lemma I.2.26 (Cancellation of congruences)**.** *For $a, b \in \mathbb{Z}$ and $d, e \in \mathbb{N}$ it holds that*

$$\boxed{ae \equiv be \pmod{d} \iff a \equiv b \pmod{\frac{d}{\gcd(d,e)}}.}$$

Proof. Let $ae \equiv be \pmod{d}$ and $g := \gcd(d, e)$. Then $d \mid (a-b)e$ and $\frac{d}{g} \mid (a-b)\frac{e}{g}$. Because of $\gcd(\frac{d}{g}, \frac{e}{g}) = 1$ it follows that $\frac{d}{g} \mid (a-b)$ (Remark I.2.20(ii)) and $a \equiv b \pmod{\frac{d}{g}}$. Conversely, if $a \equiv b \pmod{\frac{d}{g}}$, then $d \mid d\frac{e}{g} = \frac{d}{g}e \mid (a-b)e$, thus $ae \equiv be \pmod{d}$. □

Example I.2.27. An ISBN for indexing books consists of nine digits $z_1, \ldots, z_9 \in \{0, \ldots, 9\}$ as well as a check digit $s \in \{0, \ldots, 9, X\}$ with

$$s \equiv \sum_{k=1}^{9} k z_k \pmod{11},$$

where 10 is replaced by X. Because of

$$\begin{aligned} kz_k \equiv kz'_k \pmod{11} &\iff z_k \equiv z'_k \pmod{11}, \\ kz_k + lz_k \equiv kz_l + lz_k \pmod{11} &\iff (k-l)z_k \equiv (k-l)z_l \pmod{11} \iff z_k \equiv z_l \pmod{11} \end{aligned}$$

the check digit detects a faulty digit or a transposition of two digits (but not both simultaneously). See chapter III.12.

Theorem I.2.28 (Congruence equations)**.** *Let $a, b \in \mathbb{Z}$ and $d \in \mathbb{N}$. An $x \in \mathbb{Z}$ with $ax \equiv b \pmod{d}$ exists if and only if $\gcd(a, d) \mid b$. If applicable, these x form a residue class modulo $\frac{d}{\gcd(a,d)}$.*

Proof. First statement:

$$\exists x \in \mathbb{Z} : ax \equiv b \pmod{d} \iff \exists x, c \in \mathbb{Z} : b = ax + cd \overset{\text{I.2.11}}{\iff} \gcd(a, d) \mid b.$$

Second statement:

$$ax \equiv ay \pmod{d} \overset{\text{I.2.26}}{\iff} x \equiv y \pmod{\frac{d}{\gcd(a,d)}}.$$ □

Remark I.2.29. Theorem I.2.28 states that the equation $ax \equiv b \pmod{d}$, in the case of solvability, is equivalent to an equation of the form $x \equiv c \pmod{d/\gcd(a, d)}$.

Example I.2.30. How valuable is a 124.76 g pile of 1- and 2-cent coins? A 1-cent coin weighs 2300 mg and a 2-cent coin 3060 mg. Approach: $2300x + 3060y = 124,760$. We divide by $\gcd(2300, 3060) = 20$ and obtain $115x + 153y = 6238$. Modulo 115 this yields

$$38y \equiv 28 \pmod{115}.$$

According to the Euclidean algorithm, $1 = \gcd(38, 115) = -3 \cdot 38 + 115 \equiv -3 \cdot 38 \pmod{115}$. Substitution yields $38y \equiv 28 \cdot (-3 \cdot 38) \pmod{115}$. Lemma I.2.26 shows

$$y \equiv -3 \cdot 28 \equiv 31 \pmod{115}.$$

For $y \geq 31 + 115$, $3060y \geq 446,760 > 124,760$ would hold. Thus $y = 31$ is the only solution and $x = \frac{6238 - 153y}{115} = 13$ follows.

Answer: $13 + 2 \cdot 31 = 75$ cents.

Remark I.2.31. For $\alpha, \beta, \gamma \in \mathbb{N}_0$, $\min\{\max\{\alpha,\beta\},\gamma\} = \max\{\min\{\alpha,\gamma\},\min\{\beta,\gamma\}\}$ holds (consider wlog. $\alpha \geq \beta$). This shows

$$\gcd\big(\operatorname{lcm}(a,b),c\big) = \operatorname{lcm}\big(\gcd(a,c),\gcd(b,c)\big) \tag{I.2.1}$$

for $a, b, c \in \mathbb{Z}$ (Remark I.2.20).

Theorem I.2.32 (Chinese Remainder Theorem)**.** *Let $a_1, \ldots, a_n \in \mathbb{Z}$ and $d_1, \ldots, d_n \in \mathbb{N}$. An $x \in \mathbb{Z}$ with $x \equiv a_i \pmod{d_i}$ for $i = 1, \ldots, n$ exists if and only if $a_i \equiv a_j \pmod{\gcd(d_i, d_j)}$ holds for all i, j. If applicable, the x form a residue class modulo $\operatorname{lcm}(d_1, \ldots, d_n)$.*

Proof. If there exists $x \in \mathbb{Z}$ with $x \equiv a_i \pmod{d_i}$ for $i = 1, \ldots, n$, then $\gcd(d_i, d_j) \mid (a_i - x) + (x - a_j) = a_i - a_j$, thus $a_i \equiv a_j \pmod{\gcd(d_i, d_j)}$ for all i, j.

Uniqueness:

$$\begin{aligned} \forall i : x \equiv y \pmod{d_i} &\iff \forall i : d_i \mid x - y \iff \operatorname{lcm}(d_1, \ldots, d_n) \mid x - y \\ &\iff x \equiv y \pmod{\operatorname{lcm}(d_1, \ldots, d_n)}. \end{aligned}$$

Existence: Let $a_i \equiv a_j \pmod{\gcd(d_i, d_j)}$ for i, j be given. We argue by induction on n. For $n = 1$, $x := a_1$ solves the congruence. Now let $n \geq 2$. According to the Euclidean algorithm, there exist $e_1, e_2 \in \mathbb{Z}$ with $g := \gcd(d_1, d_2) = d_1 e_1 + d_2 e_2$. We set $b := a_1 + d_1 e_1 \frac{a_2 - a_1}{g} \in \mathbb{Z}$. Then it holds that

$$\begin{aligned} &b \equiv a_1 \pmod{d_1}, \\ &b = a_1 + (g - d_2 e_2)\frac{a_2 - a_1}{g} = a_1 + (a_2 - a_1) - d_2 e_2 \frac{a_2 - a_1}{g} \equiv a_2 \pmod{d_2}, \end{aligned}$$

i. e. b solves the first two equations. According to the uniqueness already shown, these equations are equivalent to

$$x \equiv b \pmod{\operatorname{lcm}(d_1, d_2)}.$$

To use the induction hypothesis, we must show $b \equiv a_i \pmod{\gcd(\operatorname{lcm}(d_1, d_2), d_i)}$ for $i = 3, \ldots, n$. It holds that $b \equiv a_1 \equiv a_i \pmod{\gcd(d_1, d_i)}$ and $b \equiv a_2 \equiv a_i \pmod{\gcd(d_2, d_i)}$. This shows

$$b \equiv a_i \pmod{\operatorname{lcm}(\gcd(d_1, d_i), \gcd(d_2, d_i))}$$

and the claim follows from (I.2.1). □

Remark I.2.33. The conditions $a_i \equiv a_j \pmod{\gcd(d_i, d_j)}$ in Theorem I.2.32 are always satisfied if $d_1, \ldots, d_n$ are pairwise coprime.[2]

Example I.2.34.

(i) Consider the system

$$\begin{aligned} x &\equiv 3 \pmod{7}, \\ x &\equiv 4 \pmod{11}, \\ x &\equiv 5 \pmod{13}. \end{aligned}$$

[2] $\gcd(d_1, \ldots, d_n) = 1$ is *not* sufficient! (consider $\gcd(6, 10, 15)$)

The approach $x = 3 + 7a$ initially solves the first equation and yields $7a \equiv 1 \pmod{11}$ in the second equation. According to Theorem I.2.28, this is equivalent to $a \equiv -3 \pmod{11}$ (the solution -3 can be easily guessed). We now set $a = -3 + 11b$ and obtain $x = -18 + 77b$. This solves the first two equations. The third equation yields $77b \equiv 23 \pmod{13}$, thus $b \equiv 3 \pmod{13}$. The general solution of the system is therefore $x = -18 + 77(3 + 13c) = 213 + 1001c$ with $c \in \mathbb{Z}$.

(ii) What are the last two decimal digits of 47^{88}? We are looking for $0 \leq x \leq 99$ with

$$x \equiv 47^{88} \pmod{100}.$$

Because of $\operatorname{lcm}(4, 25) = 100$, this congruence is equivalent to the system

$$\begin{aligned} x &\equiv 47^{88} \pmod{4}, \\ x &\equiv 47^{88} \pmod{25} \end{aligned}$$

according to Theorem I.2.32. It holds that $47^{88} \equiv (-1)^{88} \equiv 1 \pmod{4}$ and

$$47^{88} \equiv (-3)^{3 \cdot 29 + 1} \equiv (-2)^{29}(-3) \equiv (-2)^{7 \cdot 4 + 1}(-3) \equiv (-3)^4 6 \equiv 11 \pmod{25}.$$

The approach $x = 1 + 4a$ solves the first equation and results in $4a \equiv 10 \pmod{25}$ in the second equation. It follows that $2a \equiv 5 \pmod{25}$ and $a \equiv 13 \cdot 2a \equiv 13 \cdot 5 \equiv 15 \pmod{25}$. Thus $x = 1 + 4 \cdot 15 = 61$.

Definition I.2.35. One calls

$$\begin{aligned} \varphi \colon \mathbb{N} &\to \mathbb{N}, \\ n &\mapsto |\{1 \leq k \leq n : \gcd(n, k) = 1\}| \end{aligned}$$

Euler's *φ-function*.

Remark I.2.36. For $b \in a + n\mathbb{Z}$, it holds that $\gcd(b, n) = \gcd(a, n)$. Since $a + n\mathbb{Z}$ has exactly one representative b with $1 \leq b \leq n$, it holds that

$$\varphi(n) = |\{a + n\mathbb{Z} : \gcd(a, n) = 1\}|.$$

Theorem I.2.37. *It holds that*

(i) $\varphi(nm) = \varphi(n)\varphi(m)$, *if* $\gcd(n, m) = 1$.

(ii) $\varphi(p^n) = p^n - p^{n-1}$ *for every prime power* $p^n \neq 1$.

Proof.

(i) Let $1 \leq a \leq n$ and $1 \leq b \leq m$ with $\gcd(a, n) = 1 = \gcd(b, m)$. According to the Chinese Remainder Theorem, there exists exactly one $1 \leq c \leq \operatorname{lcm}(n, m) = nm$ with $c \equiv a \pmod{n}$ and $c \equiv b \pmod{m}$. Obviously, then $\gcd(c, nm) = 1$. Conversely, if $1 \leq c \leq nm$ with $\gcd(c, nm) = 1$ is given, then also $\gcd(c, n) = 1 = \gcd(c, m)$. Therefore, the sets

$$\{1 \leq a \leq n : \gcd(a, n) = 1\} \times \{1 \leq b \leq m : \gcd(b, m) = 1\}$$

and $\{1 \leq c \leq nm : \gcd(c, nm) = 1\}$ have the same cardinality and the assertion follows.

(ii) It holds that $\gcd(p^n, k) = 1$ if and only if $p \nmid k$. Between 1 and p^n there are exactly p^{n-1} multiples of p, namely $p, 2p, \ldots, p^{n-1}p$. This shows the assertion. □

Remark I.2.38. Let $n = \prod_{p\in\mathbb{P}} p^{a_p} \in \mathbb{N}$. According to Theorem I.2.37, it is then

$$\boxed{\varphi(n) = \prod_{p\in\mathbb{P}} \varphi(p^{a_p}) = \prod_{\substack{p\in\mathbb{P}\\ a_p>0}} (p^{a_p} - p^{a_p-1}).}$$

Example I.2.39. It holds that

$$\varphi(36) = \varphi(2^2 \cdot 3^2) = (2^2 - 2^1)(3^2 - 3^1) = 2 \cdot 6 = 12$$

and

$$\{1 \le a \le 36 : \gcd(a, 36) = 1\} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}.$$

Definition I.2.40. One calls

$$\mu\colon \mathbb{N} \to \mathbb{Z},$$
$$n \mapsto \begin{cases} (-1)^s & \text{if } n = p_1 \dots p_s \text{ with pairwise distinct } p_1, \dots, p_s \in \mathbb{P}, \\ 0 & \text{otherwise} \end{cases}$$

the MÖBIUS *function*. Here $\mu(1) = 1$ $(s = 0)$.

Remark I.2.41. If $p_1, \dots, p_s$ are the distinct prime divisors of $n > 1$, then

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{s} \sum_{q_1,\dots,q_k\in\{p_1,\dots,p_s\}} \mu(q_1 \dots q_k) = \sum_{k=0}^{s} \sum_{\substack{M\subseteq\{p_1,\dots,p_s\}\\ |M|=k}} (-1)^k = \sum_{k=0}^{s} (-1)^k \binom{s}{k} = (1-1)^s = 0,$$

where the sum is taken only over the positive divisors.

Theorem I.2.42 (MÖBIUS inversion)**.** *For $f, F\colon \mathbb{N} \to \mathbb{C}$, the following are equivalent:*

(1) $F(n) = \sum_{d|n} f(d)$ *for all* $n \in \mathbb{N}$.

(2) $f(n) = \sum_{d|n} \mu(d)F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d})F(d)$ *for all* $n \in \mathbb{N}$.

Proof.

(1) $\Rightarrow$ (2):

$$\sum_{d|n} \mu(d)F(n/d) \overset{(1)}{=} \sum_{d|n} \sum_{e|\frac{n}{d}} \mu(d)f(e) = \sum_{de|n} \mu(d)f(e) = \sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d) \overset{\text{I.2.41}}{=} f(n).$$

(2) $\Rightarrow$ (1):

$$\sum_{d|n} f(d) \overset{(2)}{=} \sum_{d|n} \sum_{e|d} \mu(d/e)F(e) = \sum_{e|n} F(e) \sum_{d|\frac{n}{e}} \mu(d) \overset{\text{I.2.41}}{=} F(n). \qquad \square$$

Example I.2.43. For $n = \prod_{p\in\mathbb{P}} p^{a_p} \in \mathbb{N}$ it holds that

$$\sum_{d|n} \varphi(d) \overset{\text{I.2.20}}{=} \prod_{p\in\mathbb{P}} \sum_{k=0}^{a_p} \varphi(p^k) \overset{\text{I.2.37}}{=} \prod_{p\in\mathbb{P}} (1 + (p-1) + (p^2-p) + \ldots + (p^{a_p} - p^{a_p-1})) = \prod_{p\in\mathbb{P}} p^{a_p} = n.$$

For $f = \varphi$, we thus have $F = \mathrm{id}_{\mathbb{N}}$ in Theorem I.2.42 and one obtains

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

for all $n \in \mathbb{N}$.

I.3 Groups

Definition I.3.1. A *group* is a set G together with an operation $\cdot\colon G \times G \to G$, $(x, y) \mapsto x \cdot y$, such that the following properties hold:

- $\forall x, y, z \in G : (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (*associative*),
- $\exists e \in G : \forall x \in G : e \cdot x = x$ (*identity element*),
- $\forall x \in G : \exists y \in G : y \cdot x = e$ (*inverse element*).

If additionally

- $\forall x, y \in G : x \cdot y = y \cdot x$ (*commutative*),

then G is called *abelian*. The *order* of G is the cardinality $|G|$.

Remark I.3.2.

(i) In the following, let G always be a group. If the operation is clear, we write xy instead of $x \cdot y$.

(ii) For $x \in G$ there exist $y, z \in G$ with $yx = e = zy$. It follows

$$xy = e(xy) = (zy)(xy) = z(yx)y = z(ey) = zy = e$$

and $xe = x(yx) = (xy)x = ex = x$. If $e' \in G$ is also an identity element, then $e' = e'e = e$ holds. Thus e is uniquely determined and we write $e = 1_G = 1$. Now let $y' \in G$ with $y'x = e$. Then $y' = y'e = y'(xy) = (y'x)y = ey = y$. Thus x has exactly one inverse and we write $y = x^{-1}$.

(iii) For $x, y \in G$, $\boxed{(x^{-1})^{-1} = x}$ and $\boxed{(xy)^{-1} = y^{-1}x^{-1}}$ (Attention!).

(iv) For $x_1, \ldots, x_n \in G$, the parenthesization in $x_1 \ldots x_n$ does not matter: For $n = 3$ this follows from associativity. If the assertion already holds for $n - 1$, then every parenthesization of $x_1 \ldots x_n$ has the form $(x_1 \ldots x_k)(x_{k+1} \ldots x_n)$ with $1 \leq k < n$. Now it holds that

$$x_1(x_2 \ldots x_n) = x_1(x_2(x_3 \ldots x_n)) = (x_1x_2)(x_3 \ldots x_n) = \ldots = (x_1 \ldots x_{n-1})x_n.$$

(v) For $x \in G$ and $k \in \mathbb{Z}$ we define

$$x^k := \begin{cases} 1_G & \text{if } k = 0, \\ x \ldots x \ (k \text{ factors}) & \text{if } k > 0, \\ (x^{-1})^{-k} & \text{if } k < 0. \end{cases}$$

Then certainly $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{mn}$ for $n, m \in \mathbb{Z}$. In the case $G = \{x^i : i \in \mathbb{Z}\}$, G is called *cyclic*. Because of $x^m x^n = x^{m+n} = x^n x^m$, G is then also abelian.

Example I.3.3.

(i) The *trivial* group $G = \{1\}$. We then also write $G = 1$.

(ii) The integers $\mathbb{Z}$ form an abelian group with respect to addition. The identity element is 0. In contrast, $\mathbb{Z}$ is *not* a group with respect to multiplication (2 has no inverse).

(iii) For every field K, $K^\times := K \setminus \{0\}$ is an abelian group with respect to multiplication.

(iv) The invertible $n \times n$ matrices over a field K form, with respect to matrix multiplication, the *general linear group* $\mathrm{GL}(n, K)$ of *degree* n over K. The identity element is the identity matrix 1_n. It holds that $\mathrm{GL}(1, K) = K^\times$. For $n \geq 2$, $\mathrm{GL}(n, K)$ is non-abelian.

(v) The bijections of a set Ω to itself form, with respect to composition of mappings, the *symmetric group* $\mathrm{Sym}(\Omega)$ with identity element id_Ω. The elements of $\mathrm{Sym}(\Omega)$ are called *permutations*. For $\Omega = \{1, \ldots, n\}$, we write $S_n := \mathrm{Sym}(\Omega)$ and call n the *degree* of S_n. It holds that $|S_n| = n!$.

(vi) For groups $G_1, \ldots, G_n$, the Cartesian product $G_1 \times \ldots \times G_n$ becomes a group with identity element $(1_{G_1}, \ldots, 1_{G_n})$ via

$$(g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) := (g_1 h_1, \ldots, g_n h_n)$$

for $g_i, h_i \in G_i$ (verify by calculation). One calls $G_1 \times \ldots \times G_n$ the *direct product* of $G_1, \ldots, G_n$. In the case $G_1 = \ldots = G_n$, we also write G_1^n instead of $G_1 \times \ldots \times G_n$.

Definition I.3.4. A non-empty subset $H \subseteq G$ with $xy^{-1} \in H$ for all $x, y \in H$ is called a *subgroup* of G. We then write $H \leq G$ and $H < G$ if H is a *proper* subgroup, i. e., $H \neq G$. The sets of the form $gH := \{gh : h \in H\}$ are called (*left*) *cosets* of H in G. The set of all left cosets is $G/H := \{gH : g \in G\}$ and $|G : H| := |G/H|$ is the *index* of H in G.

Remark I.3.5. Let $H \leq G$. Then there exists an $x \in H$. Thus also $1_G = xx^{-1} \in H$ and $x^{-1} = 1_G x^{-1} \in H$. For $x, y \in H$, we furthermore have $xy = x(y^{-1})^{-1} \in H$. This shows that H with the restricted operation is itself a group. If G is abelian, then so is H. From $K \leq H$ follows $K \leq G$, i. e., $\leq$ is transitive and thus a (partial) ordering relation.

Example I.3.6.

(i) Every group G possesses the subgroups 1 and G.

(ii) For every family of subgroups $H_i \leq G$ $(i \in I)$, $\bigcap_{i \in I} H_i \leq G$ (verify).

(iii) For $U \subseteq G$,

$$\langle U \rangle := \bigcap_{U \subseteq H \leq G} H$$

is the subgroup *generated* by U (the "smallest" subgroup containing U). Obviously, $\langle U \rangle$ contains all elements of the form $x_1^{\pm 1} \ldots x_n^{\pm 1}$ with $x_1, \ldots, x_n \in U$. Conversely, these elements themselves form a subgroup, which then must coincide with $\langle U \rangle$. In the case $\langle U \rangle = G$, U is a *generating set* of G. We also write $\langle x_1, \ldots, x_n \rangle := \langle \{x_1, \ldots, x_n\} \rangle$. The subgroups of the form $\langle x \rangle$ are cyclic. One then calls $|\langle x \rangle|$ the *order* of x.

(iv) For $n \in \mathbb{Z}$, $n\mathbb{Z} = \langle n \rangle \leq \mathbb{Z}$. The left cosets are then exactly the residue classes modulo n (note: the operation is $+$).

(v) The upper triangular matrices in $\mathrm{GL}(n, K)$ form a subgroup.

(vi) For $n \leq m$, $S_n \leq S_m$ holds.

Lemma I.3.7. *For $x \in G$,*

$$|\langle x\rangle| = \inf\{n \in \mathbb{N} : x^n = 1\},$$

where $\inf \varnothing := \infty$. *In the case* $n := |\langle x\rangle| < \infty$, *the following hold:*

(i) $x^k = 1 \iff n \mid k$ *for* $k \in \mathbb{Z}$.

(ii) $x^k = x^l \iff k \equiv l \pmod{n}$ *for* $k, l \in \mathbb{Z}$.

(iii) $\boxed{|\langle x^k\rangle| = \dfrac{n}{\gcd(n,k)}}$ *for* $k \in \mathbb{Z}$.

Proof. First, let $n \in \mathbb{N}$ be minimal with $x^n = 1$. For $k \in \mathbb{Z}$, there exist $q, r \in \mathbb{Z}$ with $k = qn + r$ and $0 \le r < n$ (Euclidean division). Then $x^k = x^{qn+r} = (x^n)^q x^r = 1^q x^r = x^r$ and it follows that $\langle x\rangle = \{1, x, x^2, \dots, x^{n-1}\}$. Suppose there exist $0 \le k < l < n$ with $x^k = x^l$. Then $x^{l-k} = 1$ with $1 \le l - k < n$, contradicting the choice of n. This shows $|\langle x\rangle| = n$.

Now let $x^n \neq 1$ for all $n \in \mathbb{N}$. For $1 \le k < l$, then $x^k \neq x^l$, because otherwise $x^{l-k} = 1$. This shows that the elements $x, x^2, \dots$ are pairwise distinct. In particular, $|\langle x\rangle| = \infty$.

(i) Euclidean division yields $k = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \le r < n$. As above, $x^k = x^r$ and it follows that $x^k = 1 \iff r = 0 \iff n \mid k$.

(ii) According to (i), $x^k = x^l \iff x^{k-l} = 1 \iff n \mid k - l \iff k \equiv l \pmod{n}$.

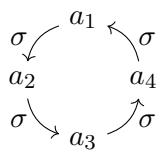
(iii) It holds that

$$\begin{aligned} |\langle x^k\rangle| &= \inf\{m \in \mathbb{N} : x^{km} = (x^k)^m = 1\} \overset{\text{(i)}}{=} \inf\{m \in \mathbb{N} : km \equiv 0 \pmod{n}\} \\ &\overset{\text{I.2.26}}{=} \inf\left\{m \in \mathbb{N} : m \equiv 0 \pmod{\frac{n}{\gcd(n,k)}}\right\} = \frac{n}{\gcd(n,k)}. \end{aligned}$$

□

Remark I.3.8 (Review of Linear Algebra)**.** For $k \ge 2$, one calls $\sigma \in S_n$ a (k-)*cycle* (or cycle of *length* k), if pairwise distinct $1 \le a_1, \dots, a_k \le n$ exist, such that

$$\sigma(x) = \begin{cases} a_{i+1} & \text{if } x = a_i \text{ with } i < k, \\ a_1 & \text{if } x = a_k, \\ x & \text{otherwise} \end{cases}$$



holds. One then writes $\sigma = (a_1, \dots, a_k)$. This notation is unique up to "rotation", i. e.

$$\sigma = (a_2, \dots, a_k, a_1) = \dots = (a_k, a_1, \dots, a_{k-1}).$$

Furthermore, $(a_1, \dots, a_k)^{-1} = (a_k, a_{k-1}, \dots, a_1)$.

Cycles of length 2 are called *transpositions*. Cycles $\sigma = (a_1, \dots, a_k)$ and $\tau = (b_1, \dots, b_l)$ are called *disjoint*, if

$$\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_l\} = \varnothing.$$

In this case, $\sigma\tau = \tau\sigma$ holds. As is well known, every permutation $\sigma \in S_n$ is a product of pairwise disjoint cycles $\sigma = \sigma_1 \dots \sigma_s$, which are uniquely determined up to their order. If σ_i has length l_i, then $(l_1, \dots, l_s)$ is called the *cycle type* of σ, where one can assume $l_1 \ge \dots \ge l_s$. Because of $(a_1, \dots, a_k) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k)$ (evaluating maps from right to left), every permutation is a product of (not necessarily disjoint) transpositions.

Lemma I.3.9. *For $\sigma \in S_n$ with cycle type $(l_1, \ldots, l_s)$, it holds that*

$$\boxed{|\langle\sigma\rangle| = \operatorname{lcm}(l_1, \ldots, l_s).}$$

Proof. Let $\sigma = \sigma_1 \ldots \sigma_s$ with disjoint cycles σ_i of length l_i. Obviously, $|\langle\sigma_i\rangle| = l_i$ for $i = 1, \ldots, s$. For $k \in \mathbb{N}$, the powers $\sigma_1^k, \ldots, \sigma_s^k$ are also pairwise disjoint and therefore commute. With Lemma I.3.7 it follows that

$$\begin{aligned}\sigma^k = 1 &\iff \sigma_1^k \ldots \sigma_s^k = 1 \iff \sigma_1^k = \ldots = \sigma_s^k = 1 \\ &\iff l_1 \mid k, \ldots, l_s \mid k \iff \operatorname{lcm}(l_1, \ldots, l_s) \mid k.\end{aligned}$$

This shows the claim. □

Example I.3.10.

(i) In S_6 is $\begin{pmatrix}1&2&3&4&5&6\\4&1&6&2&5&3\end{pmatrix} = (1,4,2)(3,6)$ an element of order 6. On the other hand, S_6 possesses no element of order 10, because for that one needs at least seven digits.

(ii) In S_5 the following holds: $(2,5,3,1)(3,1,6) = (1,6)(2,5,3)$.

(iii) It holds that $S_3 = \{1, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$. Because of $(1,2)(1,3) = (1,3,2) \neq (1,2,3) = (1,3)(1,2)$, S_n is abelian if and only if $n \leq 2$.

Theorem I.3.11 (Lagrange)**.** *For every group G and $H \leq G$ it holds that*

$$\boxed{|G| = |G : H||H|.}$$

In particular, $|H|$ and $|G : H|$ are divisors of $|G|$, if $|G| < \infty$.

Proof. For $x, y \in G$ let

$$x \sim y :\iff x^{-1}y \in H.$$

Because of $1 \in H$, $x \sim x$ holds. For $x \sim y$, it holds that $y^{-1}x = (x^{-1}y)^{-1} \in H$ and $y \sim x$. From $x \sim y \sim z$ it finally follows that $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$ and $x \sim z$. Thus $\sim$ is an equivalence relation. Because of

$$x \sim y \iff x^{-1}y \in H \iff y \in xH$$

the equivalence classes are exactly the left cosets of H in G. In particular, G is the disjoint union of all left cosets. Since the map $H \to xH$, $h \mapsto xh$ is a bijection (with inverse map $g \mapsto x^{-1}g$), all left cosets are of the same size. This shows

$$|G| = \Big|\bigcup_{gH \in G/H} gH\Big| = \sum_{gH \in G/H} |gH| = |G : H||H|.$$ □

Remark I.3.12.

(i) The proof shows

$$\boxed{xH = yH \iff x^{-1}y \in H}$$

for all $x, y \in G$. One can define $x \sim y :\iff xy^{-1} \in H$ completely analogously and then obtains the *right cosets* Hg of H in G as equivalence classes. The proof shows that there are exactly as many left as right cosets. In general, however, $gH \neq Hg$.

(ii) For $|G| < \infty$ and $x \in G$, $|\langle x \rangle|$ is a divisor of $|G|$. By Lemma I.3.7 it follows that $x^{|G|} = 1$.

Definition I.3.13. For $X, Y \subseteq G$ let $XY := \{xy : x \in X,\, y \in Y\}$.

Lemma I.3.14. *For $U, V, W \leq G$ it holds that*

(i) $U \subseteq V \Longrightarrow |G : U| = |G : V||V : U|$.

(ii) $UV \leq G \iff UV = VU$.

(iii) $\boxed{|UV| = |U : U \cap V||V| = |V : U \cap V||U|.}$

(iv) $U \subseteq W \Longrightarrow UV \cap W = U(V \cap W)$ (Dedekind *identity*).

Proof. Exercise I.19. □

Remark I.3.15. For $U, V \leq G$, $UV \leq G$ is not necessarily true (Exercise I.21)!

Definition I.3.16. A subgroup $H \leq G$ is called a *normal subgroup* of G (or *normal* in G), if $gH = Hg$ holds for all $g \in G$. If applicable, we write $H \trianglelefteq G$ and $H \triangleleft G$, if $H < G$.

Example I.3.17.

(i) 1 and G are always normal in G.

(ii) Subgroups of abelian groups are always normal. In particular, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

(iii) Subgroups $H \leq G$ with index 2 are normal, because for $g \in G \setminus H$ it holds that $gH = G \setminus H = Hg$.

(iv) For $N, M \trianglelefteq G$ and $g \in G$, we have $g(N \cap M) = gN \cap gM = Ng \cap Mg = (N \cap M)g$ and $N \cap M \trianglelefteq G$. Furthermore,

$$NM = \bigcup_{x \in N} xM = \bigcup_{x \in N} Mx = MN$$

and Lemma I.3.14(ii) shows $NM \leq G$. Because of $gNM = NgM = NMg$ for $g \in G$, we also have $NM \trianglelefteq G$.

(v) Because of

$$(1,3)S_2 = \{(1,3), \underbrace{(1,3)(1,2)}_{=(1,2,3)}\} \neq \{(1,3), \underbrace{(1,2)(1,3)}_{=(1,3,2)}\} = S_2(1,3)$$

it holds that $S_2 \not\trianglelefteq S_3$.

(vi) From $M \trianglelefteq N \trianglelefteq G$ it does not necessarily follow that $M \trianglelefteq G$ (Exercise I.21), i. e. $\trianglelefteq$ is not transitive.

Lemma I.3.18. *$H \leq G$ is normal in G if and only if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.*

Proof. Let $H \trianglelefteq G$, $g \in G$ and $h \in H$. Then $ghg^{-1} \in gHg^{-1} = Hgg^{-1} = H$. Conversely, if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$, then it follows that

$$gH = \{ghg^{-1}g : h \in H\} \subseteq Hg = \{gg^{-1}hg : h \in H\} = \{gg^{-1}h(g^{-1})^{-1} : h \in H\} \subseteq gH.$$

This shows $H \trianglelefteq G$. □

Theorem I.3.19. *Let G be a group and $N \trianglelefteq G$. Then G/N becomes a group with the operation*

$$xN \cdot yN := xyN$$

for $xN, yN \in G/N$ with neutral element $1N = N$.

Proof. We must first show that the operation does not depend on the choice of the representatives x and y. For this, let $xN = x'N$ and $yN = y'N$. Because of $N \trianglelefteq G$, it then holds that

$$x'y'N = x'yN = x'Ny = xNy = xyN.$$

Thus $xN \cdot yN = xyN$ is well-defined. For $xN, yN, zN \in G/N$ we have

$$(xN \cdot yN) \cdot zN = xyN \cdot zN = (xy)zN = x(yz)N = xN \cdot yzN = xN \cdot (yN \cdot zN).$$

Furthermore, $1N \cdot xN = 1xN = xN$ as well as $x^{-1}N \cdot xN = x^{-1}xN = 1N$. □

Definition I.3.20. In the situation of Theorem I.3.19, G/N is called the *factor group* of G by N.

Remark I.3.21. If G is abelian, then so is G/N.

Example I.3.22. For $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ is a group of order n (cf. Theorem I.2.23).

Definition I.3.23. A map $f\colon G \to H$ for groups G and H is called

- *homomorphism*, if $f(xy) = f(x)f(y)$ holds for $x, y \in G$.
- *monomorphism*, if f is an injective homomorphism.
- *epimorphism*, if f is a surjective homomorphism.
- *isomorphism*, if f is a bijective homomorphism.
- *endomorphism*, if f is a homomorphism with $G = H$.
- *automorphism*, if f is a bijective endomorphism.

Remark I.3.24.

(i) For a homomorphism $f\colon G \to H$, it holds that

$$f(1_G) = f(1_G)f(1_G)f(1_G)^{-1} = f(1_G1_G)f(1_G)^{-1} = f(1_G)f(1_G)^{-1} = 1_H$$

and

$$f(x^{-1}) = f(x^{-1})f(x)f(x)^{-1} = f(x^{-1}x)f(x)^{-1} = f(1_G)f(x)^{-1} = 1_Hf(x)^{-1} = f(x)^{-1}$$

for $x \in G$. If x has finite order, then $|\langle f(x)\rangle|$ is a divisor of $|\langle x\rangle|$, because $f(x)^{|\langle x\rangle|} = f(x^{|\langle x\rangle|}) = f(1_G) = 1_H$ (Lemma I.3.7).

(ii) For $U \leq G$ and $V \leq H$, we have $f(U) \leq H$ and $f^{-1}(V) := \{x \in G : f(x) \in V\} \leq G$ (verify). In particular, $f(G) \leq H$. In the case $U \trianglelefteq G$, it holds that $f(U) \trianglelefteq f(G)$, but not necessarily $f(U) \trianglelefteq H$ (Exercise I.21)! For $V \trianglelefteq H$, it always holds that $f^{-1}(V) \trianglelefteq G$. In particular,

$$\mathrm{Ker}(f) := f^{-1}(1) \trianglelefteq G.$$

One calls $\mathrm{Ker}(f)$ the *kernel* of f.

(iii) If $g\colon H \to K$ is another homomorphism, then $g \circ f\colon G \to K$ is also a homomorphism, because

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$$

for $x, y \in G$.

(iv) If $f\colon G \to H$ is an isomorphism, then so is $f^{-1}\colon H \to G$, because

$$f^{-1}(xy) = f^{-1}(f(f^{-1}(x))f(f^{-1}(y))) = f^{-1}(f(f^{-1}(x)f^{-1}(y))) = f^{-1}(x)f^{-1}(y)$$

for $x, y \in H$. One then says G and H are *isomorphic* and writes $G \cong H$. Obviously, the isomorphism of groups is an equivalence relation. Since isomorphic groups have the same properties, one is usually only interested in groups up to isomorphism.

(v) According to (iii) and (iv), the automorphisms of G form a subgroup $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$. One calls $\mathrm{Aut}(G)$ the *automorphism group* of G.

Example I.3.25.

(i) There always exists the trivial homomorphism $G \to H$, $g \mapsto 1_H$ and the trivial automorphism $\mathrm{id}_G\colon G \to G$, $g \mapsto g$ (neutral element of $\mathrm{Aut}(G)$).

(ii) For $H \leq G$, the inclusion map $H \to G$, $h \mapsto h$ is a monomorphism.

(iii) For $N \trianglelefteq G$, there is the *canonical* epimorphism $G \to G/N$, $g \mapsto gN$ with kernel N.

(iv) For every field K and $n \in \mathbb{N}$, $\det\colon \mathrm{GL}(n, K) \to K^\times$ is an epimorphism (Linear Algebra). One calls

$$\mathrm{SL}(n, K) := \mathrm{Ker}(\det) = \{A \in \mathrm{GL}(n, K) : \det(A) = 1\} \trianglelefteq \mathrm{GL}(n, K)$$

the *special linear group* of *degree* n over K.

(v) The exponential function $\exp\colon (\mathbb{R}, +) \to \mathbb{R}^\times$, $a \mapsto e^a$ is a monomorphism, because $e^{a+b} = e^a e^b$ for $a, b \in \mathbb{R}$.

Theorem I.3.26. *For $n \in \mathbb{N}$, there exists a homomorphism $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ with*

$$\boxed{\mathrm{sgn}(\sigma) = (-1)^{l_1 + \ldots + l_s - s}}$$

for $\sigma \in S_n$ with cycle type $(l_1, \ldots, l_s)$.

Proof. We define

$$\mathrm{sgn}(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \in \{\pm 1\}$$

for $\sigma \in S_n$. For $\sigma, \tau \in S_n$, it then holds that

$$\begin{aligned}\mathrm{sgn}(\sigma\tau) &= \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} = \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \frac{\tau(j) - \tau(i)}{j - i} \\ &= \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{i<j} \frac{\tau(j) - \tau(i)}{j - i} = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau).\end{aligned}$$

Thus sgn is a homomorphism. For every transposition $\sigma = (s,t)$ with $s < t$, it holds that

$$\operatorname{sgn}(\sigma) = \frac{s-t}{t-s} \prod_{s<j\neq t} \frac{j-t}{j-s} \prod_{s\neq i<t} \frac{s-i}{t-i}.$$

The factors are negative if and only if $s < j < t$ or $s < i < t$ holds. One obtains $\operatorname{sgn}(\sigma) = -(-1)^{2(t-s-1)} = -1$. Since every k-cycle $\sigma = (a_1, \ldots, a_k)$ can be written as a product of $k-1$ transpositions $\sigma = (a_1, a_2)(a_2, a_3)\ldots(a_{k-1}, a_k)$, it holds that $\operatorname{sgn}(\sigma) = (-1)^{k-1}$. The claim follows from this. □

Definition I.3.27. One calls sgn *signum* (or *sign*) and

$$A_n := \operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in S_n : \operatorname{sgn}(\sigma) = 1\} \trianglelefteq S_n$$

the *alternating group* of *degree* n. The elements in A_n (resp. $S_n \setminus A_n$) are called *even* (resp. *odd*) permutations. Note: A cycle of even length is odd.

Lemma I.3.28. *A homomorphism $f\colon G \to H$ is injective if and only if* $\operatorname{Ker}(f) = 1$.

Proof. If f is injective, then $f(x) = 1 = f(1)$ if and only if $x = 1$. This shows $\operatorname{Ker}(f) = 1$. Conversely, let $\operatorname{Ker}(f) = 1$ and $x, y \in G$ with $f(x) = f(y)$. Then $f(y^{-1}x) = f(y)^{-1}f(x) = 1$ and $y^{-1}x \in \operatorname{Ker}(f) = 1$. This shows $x = y$ and f is injective. □

Theorem I.3.29.

(i) (*Homomorphism theorem*[1]) *For every homomorphism $f\colon G \to H$, it holds that*

$$\boxed{G/\operatorname{Ker}(f) \cong f(G).}$$

(ii) (*Correspondence theorem*) *For $N \trianglelefteq G$, the canonical epimorphism $G \to G/N$ induces a bijection between the set of subgroups $H \leq G$ with $N \leq H$ and the set of subgroups of G/N.*

(iii) (*1st Isomorphism theorem*) *For $H \leq G$ and $N \trianglelefteq G$, it holds that $N \trianglelefteq HN \leq G$, $H \cap N \trianglelefteq H$ and*

$$\boxed{HN/N \cong H/H \cap N.}$$

(iv) (*2nd Isomorphism theorem*) *For $N \trianglelefteq G$ and $N \leq H \leq G$, $H \trianglelefteq G$ if and only if $H/N \trianglelefteq G/N$. If applicable,*

$$\boxed{G/H \cong (G/N)/(H/N).}$$

Proof.

(i) Let $x, y \in G$ and

$$\begin{aligned} F\colon G/\operatorname{Ker}(f) &\to f(G), \\ x\operatorname{Ker}(f) &\mapsto f(x). \end{aligned}$$

[1] Some authors use different numberings for the isomorphism theorems, see Wikipedia.

Because of

$$x\mathrm{Ker}(f) = y\mathrm{Ker}(f) \overset{\text{I.3.12}}{\iff} y^{-1}x \in \mathrm{Ker}(f) \iff f(y)^{-1}f(x) = f(y^{-1}x) = 1 \iff f(x) = f(y)$$

F is well-defined and injective. By definition, F is also surjective. Finally,

$$F\big(x\mathrm{Ker}(f) \cdot y\mathrm{Ker}(f)\big) = F(xy\mathrm{Ker}(f)) = f(xy) = f(x)f(y) = F\big(x\mathrm{Ker}(f)\big)F\big(y\mathrm{Ker}(f)\big).$$

Thus F is a bijective homomorphism, i. e. an isomorphism.

(ii) Let $f\colon G \to G/N$ be the canonical epimorphism, $\mathcal{H} := \{H \leq G : N \leq H\}$ and $\mathcal{K} := \{U \leq G/N\}$. For $H \in \mathcal{H}$ it is certain that $H/N = f(H) \in \mathcal{K}$. For $U \in \mathcal{K}$ conversely $N \leq f^{-1}(U) \leq G$ holds, because $f(N) = 1 \leq U$. Thus $f^{-1}(U) \in \mathcal{H}$ and one obtains maps

$$\begin{aligned} \varphi\colon \mathcal{H} &\to \mathcal{K}, & \psi\colon \mathcal{K} &\to \mathcal{H}, \\ H &\mapsto f(H), & U &\mapsto f^{-1}(U). \end{aligned}$$

Let $H \in \mathcal{H}$ and $x \in f^{-1}(f(H))$. Then there exists $h \in H$ with $f(x) = f(h)$. It follows $f(h^{-1}x) = f(h)^{-1}f(x) = 1$ and $x = h(h^{-1}x) \in H\mathrm{Ker}(f) = HN = H$. This shows $f^{-1}(f(H)) = H$ and $\psi \circ \varphi = \mathrm{id}_{\mathcal{H}}$. Since f is surjective, $f(f^{-1}(U)) = U$ also holds for all $U \in \mathcal{K}$, i. e. $\varphi \circ \psi = \mathrm{id}_{\mathcal{K}}$. Therefore φ and ψ are inverse bijections to each other.

(iii) We consider the map $f\colon H \to G/N$, $h \mapsto hN$. Because of $f(xy) = xyN = xNyN = f(x)f(y)$ for $x, y \in H$, f is a homomorphism. For $h \in H$ we have $f(h) = 1 \iff hN = N \iff h \in H \cap N$. This shows $\mathrm{Ker}(f) = H \cap N \trianglelefteq H$ and (i) yields $H/H \cap N = H/\mathrm{Ker}(f) \cong f(H) = HN/N \leq G/N$. From (ii) it follows $HN \leq G$.

(iv) According to (ii) we have $H/N \leq G/N$. For $g \in G$ and $h \in H$ we have

$$ghg^{-1} \in H \iff (gN)(hN)(gN)^{-1} = ghg^{-1}N \in H/N.$$

It follows $H \trianglelefteq G \iff H/N \trianglelefteq G/N$ according to Lemma I.3.18. Now let $H \trianglelefteq G$ and $f\colon G/N \to G/H$, $gN \mapsto gH$. For $x, y \in G$ we have

$$xN = yN \Longrightarrow y^{-1}x \in N \leq H \Longrightarrow xH = yH.$$

Therefore f is well-defined. Obviously f is an epimorphism with $\mathrm{Ker}(f) = \{gN \in G/N : gH = H\} = H/N$. Thus $(G/N)/(H/N) = (G/N)/\mathrm{Ker}(f) \cong f(G/N) = G/H$ follows from (i). □

Example I.3.30.

(i) The homomorphism theorem for $\det\colon \mathrm{GL}(n, K) \to K^\times$ shows $\mathrm{GL}(n, K)/\mathrm{SL}(n, K) \cong K^\times$.

(ii) For $n \geq 2$, $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ is surjective because of $\mathrm{sgn}((1, 2)) = -1$. It follows $S_n/A_n \cong \{\pm 1\}$ and $|A_n| = n!/2$.

(iii) For $n, m \in \mathbb{N}$ with $n \mid m$, we have $m\mathbb{Z} \leq n\mathbb{Z}$ as well as $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.

Theorem I.3.31. *For every cyclic group G there exists exactly one $n \in \mathbb{N}_0$ with $G \cong \mathbb{Z}/n\mathbb{Z}$.*

Proof. Let $G = \langle x \rangle$ and $f\colon \mathbb{Z} \to G$, $k \mapsto x^k$. Because of $f(a + b) = x^{a+b} = x^a x^b = f(a)f(b)$ for $a, b \in \mathbb{Z}$, f is an epimorphism with

$$\mathrm{Ker}(f) = \{k \in \mathbb{Z} : x^k = 1\} = \begin{cases} 0\mathbb{Z} & \text{if } |G| = \infty, \\ n\mathbb{Z} & \text{if } |G| = n \end{cases}$$

according to Lemma I.3.7. The assertion now follows from the homomorphism theorem. □

Definition I.3.32. According to Theorem I.3.31, there is essentially only one cyclic group for each order n. We denote this by C_n (this is shorter than $\mathbb{Z}/n\mathbb{Z}$).

Example I.3.33. Let G be a group of prime order p. For $x \in G \setminus \{1\}$, it then holds that $\langle x \rangle = G$ according to Lagrange. Thus $G \cong C_p$.

Theorem I.3.34.

(i) For coprime $n, m \in \mathbb{N}$, it holds that $\boxed{C_n \times C_m \cong C_{nm}.}$

(ii) For every $d \mid n$, C_n possesses exactly one subgroup (and exactly one factor group) of order d. This is isomorphic to C_d.

Proof.

(i) According to the Chinese Remainder Theorem, the homomorphism $f\colon \mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, $a \mapsto (a + n\mathbb{Z}, a + m\mathbb{Z})$ is surjective. Here it holds that

$$\operatorname{Ker}(f) = \{a \in \mathbb{Z} : a \in n\mathbb{Z} \cap m\mathbb{Z} = \operatorname{lcm}(n, m)\mathbb{Z} = mn\mathbb{Z}\} = mn\mathbb{Z}.$$

The homomorphism theorem shows $C_{nm} \cong \mathbb{Z}/mn\mathbb{Z} \cong f(\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \cong C_n \times C_m$.

(ii) Let $\langle x \rangle \cong C_n$. For $d \mid n$, $\langle x^{n/d} \rangle$ is a subgroup of order d according to Lemma I.3.7. Conversely, let $H \leq \langle x \rangle$ with $|H| = d \mid n$ (Lagrange). According to Remark I.3.12(ii), it holds that $x^{n/d}H = (xH)^{|G/H|} = H$ and $x^{n/d} \in H$. This shows $H = \langle x^{n/d} \rangle$. Because of $\langle x \rangle / H = \langle xH \rangle \cong C_{n/d}$, the assertion about factor groups is also clear. □

I.4 Group Actions

Definition I.4.1. An *action* of G on a non-empty set Ω is a map $G \times \Omega \to \Omega$, $(x, \omega) \mapsto {}^x\omega$ with the following properties:

- $\forall \omega \in \Omega : {}^1\omega = \omega$.
- $\forall x, y \in G,\ \omega \in \Omega : {}^x({}^y\omega) = {}^{xy}\omega$.

One then says: G *acts* on Ω or Ω is a G*-set*. For $\omega \in \Omega$, one calls

$$ {}^G\omega := \{{}^g\omega : g \in G\} \subseteq \Omega $$

the *orbit* of ω and $G_\omega := \{g \in G : {}^g\omega = \omega\}$ the *stabilizer* of ω in G. One calls $|{}^G\omega|$ the *length* of the orbit. If ${}^G\omega = \Omega$ for some $\omega \in \Omega$, then the action is called *transitive*.

Remark I.4.2. Let Ω be a G-set and $f_x \colon \Omega \to \Omega$, $\omega \mapsto {}^x\omega$ for $x \in G$. For $x, y \in G$ and $\omega \in \Omega$, it then holds that $(f_x \circ f_y)(\omega) = f_x({}^y\omega) = {}^x({}^y\omega) = {}^{xy}\omega = f_{xy}(\omega)$. In particular, $f_x \circ f_{x^{-1}} = f_1 = \mathrm{id}_\Omega = f_{x^{-1}} \circ f_x$ and $f_x \in \mathrm{Sym}(\Omega)$. Furthermore, $f \colon G \to \mathrm{Sym}(\Omega)$, $x \mapsto f_x$ is a homomorphism.

Conversely, let a homomorphism $f \colon G \to \mathrm{Sym}(\Omega)$ be given. Then one obtains an action (verify) via

$$ {}^x\omega := (f(x))(\omega) \qquad (x \in G,\ \omega \in \Omega) $$

Thus, actions are nothing other than homomorphisms into the symmetric group. The action is called *faithful* (or *trivial*) if $\mathrm{Ker}(f) = 1$ (or $\mathrm{Ker}(f) = G$) holds. In the first case, G is isomorphic to a subgroup of $\mathrm{Sym}(\Omega)$ by the Homomorphism Theorem. G is then called a *permutation group* on Ω.

Lemma I.4.3. *Every G-set Ω is the disjoint union of orbits and $G_\omega \leq G$ for all $\omega \in \Omega$.*

Proof. We show that

$$ \alpha \sim \beta \ :\Longleftrightarrow\ \exists g \in G : {}^g\alpha = \beta $$

defines an equivalence relation on Ω. Because of ${}^1\alpha = \alpha$, $\sim$ is reflexive. From ${}^g\alpha = \beta$ follows ${}^{g^{-1}}\beta = {}^{g^{-1}}({}^g\alpha) = {}^{g^{-1}g}\alpha = {}^1\alpha = \alpha$. Thus $\sim$ is symmetric. Finally, let ${}^g\alpha = \beta$ and ${}^h\beta = \gamma$ for $g, h \in G$ and $\alpha, \beta, \gamma \in \Omega$. Then ${}^{hg}\alpha = {}^h({}^g\alpha) = {}^h\beta = \gamma$. Therefore $\sim$ is transitive and an equivalence relation. The equivalence classes are exactly the orbits. In particular, Ω is the disjoint union of the orbits of G.

For the second assertion, we observe $1 \in G_\omega \neq \varnothing$. For $x, y \in G_\omega$ we have

$$ {}^{xy^{-1}}\omega = {}^{xy^{-1}}({}^y\omega) = {}^{xy^{-1}y}\omega = {}^x\omega = \omega. $$

This shows $xy^{-1} \in G_\omega$ and $G_\omega \leq G$. □

Example I.4.4.

(i) Every subgroup $H \leq G$ acts faithfully on G by left multiplication, i. e. ${}^h g := hg$ for $g \in G$, $h \in H$ (since: ${}^1 g = g$, ${}^h({}^k g) = h(kg) = (hk)g = {}^{hk} g$ and ${}^h g = g \iff h = 1$). The orbits are the right cosets of H in G. Analogously, H acts from the right by ${}^h g := gh^{-1}$ (Attention!) and one obtains the left cosets as orbits.

(ii) G acts on itself by *conjugation* ${}^x g := xgx^{-1}$ for $x, g \in G$. The orbits are called *conjugacy classes* and the stabilizer of $g \in G$ is the *centralizer*

$$\mathrm{C}_G(g) := \{x \in G : gx = xg\}.$$

The number $k(G)$ of conjugacy classes is called the *class number* of G. Two elements in the same conjugacy class are called *conjugate*. The kernel of the action is the *center*

$$\mathrm{Z}(G) := \{x \in G : \forall y \in G : xy = yx\} \trianglelefteq G$$

of G and the image is the *inner automorphism group* $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ (Exercise I.22).

(iii) Analogously, G acts by conjugation on the set of subgroups of G, i. e. ${}^x H := xHx^{-1} \leq G$ for $x \in G$ and $H \leq G$. The orbits are also called conjugacy classes here and the stabilizer of $H \leq G$ is the *normalizer*

$$\mathrm{N}_G(H) := \{x \in G : xHx^{-1} = H\}.$$

This is the "largest" subgroup in which H is normal (cf. Exercise I.17). The orbits of length 1 correspond to the normal subgroups. More generally, $\mathrm{N}_G(H)$ acts by conjugation on H with kernel

$$\mathrm{C}_G(H) := \bigcap_{h \in H} \mathrm{C}_G(h) \trianglelefteq \mathrm{N}_G(H).$$

Theorem I.4.5 (Cayley)**.** *Every finite group G is isomorphic to a subgroup of $S_{|G|}$.*

Proof. According to Example I.4.4(i), G acts faithfully by left multiplication on itself. This yields a monomorphism $f\colon G \to \mathrm{Sym}(G)$. According to the isomorphism theorem, G is isomorphic to a subgroup of $\mathrm{Sym}(G)$. Finally, we show $\mathrm{Sym}(G) \cong S_{|G|}$. Let $|G| = n$ and $F\colon \{1, \ldots, n\} \to G$ be a bijection. Then the map $\Delta\colon S_n \to \mathrm{Sym}(G)$, $\sigma \mapsto F \circ \sigma \circ F^{-1}$ is a bijection with inverse map $\tau \mapsto F^{-1} \circ \tau \circ F$. Because of

$$\Delta(\sigma\tau) = F\sigma\tau F^{-1} = (F\sigma F^{-1})(F\tau F^{-1}) = \Delta(\sigma)\Delta(\tau)$$

Δ is an isomorphism. □

Remark I.4.6.

(i) If $H \leq G$, then G acts on G/H by left multiplication, i. e. ${}^g(xH) := gxH$ (the case $H = 1$ corresponds to Theorem I.4.5). For the corresponding homomorphism $f\colon G \to \mathrm{Sym}(G/H)$, it holds that $\mathrm{Ker}(f) \leq H$, because for $g \in \mathrm{Ker}(f)$ we have $1H = {}^g(1H) = gH$. The action is also transitive, because for every $xH \in G/H$ it holds that ${}^x(1H) = xH$.

(ii) Cayley's Theorem has no practical relevance, because $S_{|G|}$ is much larger than G. In most cases, however, one can embed G into a smaller symmetric group using (i), in which one can calculate efficiently. For example, one can realize the

$$43.252.003.274.489.856.000$$

states of the $3 \times 3 \times 3$ Rubik's Cube as a subgroup of S_{48}.

(iii) Since S_n possesses only finitely many subgroups, there are also only finitely many groups of order n up to isomorphism.

Theorem I.4.7. *For every G-set Ω and $\omega \in \Omega$, it holds that* $\boxed{|{}^G\omega| = |G : G_\omega|.}$ *In particular, $|{}^G\omega|$ is a divisor of $|G|$ if $|G| < \infty$. If G additionally acts transitively, then $|\Omega|$ is a divisor of $|G|$.*

Proof. We show that the map

$$\begin{aligned} F\colon G/G_\omega &\to {}^G\omega, \\ xG_\omega &\mapsto {}^x\omega \end{aligned}$$

is well-defined and injective:

$$xG_\omega = yG_\omega \iff y^{-1}x \in G_\omega \iff {}^{y^{-1}x}\omega = \omega \iff {}^x\omega = {}^y({}^{y^{-1}x}\omega) = {}^y\omega.$$

Obviously, F is also surjective. This shows the first claim. The last two statements follow by Lagrange. □

Remark I.4.8. If $\Delta \subseteq \Omega$ is a system of representatives for the orbits of G on Ω, then the *orbit equation*

$$\boxed{|\Omega| = \sum_{\delta \in \Delta} |{}^G\delta| = \sum_{\delta \in \Delta} |G : G_\delta|}$$

holds by Lemma I.4.3 and Theorem I.4.7. In the special case of the conjugation action, one obtains the *class equation*

$$\boxed{|G| = \sum_{x \in R} |G : \mathrm{C}_G(x)|,}$$

where R is a system of representatives for the conjugacy classes of G. For $x \in \mathrm{Z}(G)$, $\{x\}$ is a conjugacy class and one obtains $x \in R$ as well as $\mathrm{C}_G(x) = G$. This shows

$$|G| = |\mathrm{Z}(G)| + \sum_{x \in R \setminus \mathrm{Z}(G)} |G : \mathrm{C}_G(x)|.$$

Example I.4.9. Let Ω be a G-set with $|G| = 77$ and $|\Omega| = 23$. According to the orbit equation, there exist $a, b, c \in \mathbb{N}_0$ with $23 = a + 7b + 11c$. It follows that $a > 0$, i. e. G always has a fixed point on Ω.

Definition I.4.10. For a prime number p, G is called a *p-group* if $|G| = p^n$ for some $n \in \mathbb{N}_0$.

Theorem I.4.11. *For every p-group $G \neq 1$, it holds that $\mathrm{Z}(G) \neq 1$.*

Proof. Let R be a system of representatives for the conjugacy classes of G. The class equation shows

$$0 \equiv |G| = |\mathrm{Z}(G)| + \sum_{x \in R \setminus \mathrm{Z}(G)} |G : \mathrm{C}_G(x)| \equiv |\mathrm{Z}(G)| \pmod{p}.$$

In particular, $\mathrm{Z}(G) \neq 1$. □

Corollary I.4.12. *Every p-group of order p^2 is abelian.*

Proof. Let $|G| = p^2$. According to Theorem I.4.11, $|G : \mathrm{Z}(G)| \leq p$. In particular, $G/\mathrm{Z}(G)$ is cyclic and the claim follows from Exercise I.22. □

Theorem I.4.13 (Frattini argument[1]). *Let Ω be a G-set and $H \leq G$. If H acts transitively on Ω, then $G = HG_\omega$ for all $\omega \in \Omega$.*

Proof. Let $g \in G$ be arbitrary. Then there exists an $h \in H$ with ${}^g\omega = {}^h\omega$. Thus $h^{-1}g \in G_\omega$ and $g = h(h^{-1}g) \in HG_\omega$. Conversely, $HG_\omega \subseteq G$ certainly holds as well. □

Theorem I.4.14 (Sylow). *Let G be a group of order $p^a m$ for a prime $p \nmid m$ and $a \in \mathbb{N}_0$. Then:*

(i) For every $b \in \{0, \ldots, a\}$, G possesses a subgroup of order p^b. In particular, the set of Sylow p-subgroups $\mathrm{Syl}_p(G) := \{P \leq G : |P| = p^a\}$ *is not empty.*

(ii) Every p-subgroup of G is contained in a Sylow p-subgroup.

(iii) Any two Sylow p-subgroups are conjugate in G.

(iv) For $P \in \mathrm{Syl}_p(G)$, $|\mathrm{Syl}_p(G)| = |G : \mathrm{N}_G(P)| \equiv 1 \pmod p$. In particular, $|\mathrm{Syl}_p(G)|$ is a divisor of m.

Proof (Robinson).

(i) We argue by induction on $|G|$. In the case $b = 0$, the claim is trivial. So let $0 < b \leq a$. Let $R \subseteq G$ be a system of representatives for the conjugacy classes of G. Let us first assume that $|G : \mathrm{C}_G(x)| \not\equiv 0 \pmod p$ for some $x \in R \setminus \mathrm{Z}(G)$. Then $|\mathrm{C}_G(x)| = p^a m'$ with $m' < m$. By induction, $\mathrm{C}_G(x)$ has a subgroup of order p^b and thus so does G. We can therefore assume $|G : \mathrm{C}_G(x)| \equiv 0 \pmod p$ for all $x \in R \setminus \mathrm{Z}(G)$. The class equation then shows

$$0 \equiv |G| = |\mathrm{Z}(G)| + \sum_{x \in R \setminus \mathrm{Z}(G)} |G : \mathrm{C}_G(x)| \equiv |\mathrm{Z}(G)| \pmod p,$$

i. e. $|\mathrm{Z}(G)|$ is divisible by p. In the case $\mathrm{Z}(G) < G$, $\mathrm{Z}(G)$ has a subgroup Z of order p by induction. Certainly $Z \trianglelefteq G$ and by induction there exists $P/Z \leq G/Z$ with $|P/Z| = p^{b-1}$ (Correspondence Theorem). Obviously then $P \leq G$ with $|P| = |P/Z||Z| = p^b$. We can therefore assume $\mathrm{Z}(G) = G$, i. e. G is abelian. Let $M < G$ be a maximal proper subgroup. If $|M|$ is divisible by p, then by induction there exists a $Z \leq M$ with $|Z| = p$ and the claim follows as above. So let $|G/M| \equiv 0 \pmod{p^a}$. For $x \in G \setminus M$ we have $G = M\langle x \rangle$, since G is abelian and $|M|$ is maximal. Because of

$$|\langle x \rangle / \langle x \rangle \cap M| = |\langle x \rangle M/M| = |G/M| \equiv 0 \pmod{p^a}$$

$|\langle x \rangle|$ is divisible by p^a. By Theorem I.3.34, $\langle x \rangle$ has a subgroup of order p^b and thus so does G.

(ii) Let $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ be a p-subgroup. As usual, Q acts on G/P by left multiplication (Remark I.4.6(i)), where the orbit lengths are divisors of $|Q|$, hence p-powers. Since $|G/P| = m \not\equiv 0 \pmod p$, there exists an orbit of length 1, i. e. there exists an $x \in G$ with $QxP = xP$. It follows $Q = Qx1x^{-1} \subseteq QxPx^{-1} = xPx^{-1} \in \mathrm{Syl}_p(G)$ (note $|xPx^{-1}| = |P|$).

(iii) Follows from the proof of (ii) by choosing $P, Q \in \mathrm{Syl}_p(G)$.

[1] actually goes back to Capelli, see [M. Brescia, F. de Giovanni, M. Trombetti, *The true story behind Frattini's argument*, Adv. Group Theory Appl. 3 (2017), 117–129]

(iv) By (iii), G acts transitively on $\mathrm{Syl}_p(G)$ by conjugation. The stabilizer of P is $\mathrm{N}_G(P)$. The orbit equation shows $|\mathrm{Syl}_p(G)| = |G : \mathrm{N}_G(P)|$. Obviously P also acts on $\mathrm{Syl}_p(G)$. Let $Q \in \mathrm{Syl}_p(G)$ be a fixed point, i. e. $P \subseteq \mathrm{N}_G(Q)$. By (iii) there then exists an $x \in \mathrm{N}_G(Q)$ with $P = xQx^{-1} = Q$. Thus P is the unique fixed point of P on $\mathrm{Syl}_p(G)$. The orbit equation yields $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$. □

Corollary I.4.15. *For $P \in \mathrm{Syl}_p(G)$ we have $P \trianglelefteq G \iff \mathrm{Syl}_p(G) = \{P\}$.*

Proof. We have

$$P \trianglelefteq G \iff \mathrm{N}_G(P) = G \iff |\mathrm{Syl}_p(G)| = 1.$$ □

Theorem I.4.16 (Cauchy)**.** *For every prime divisor p of $|G|$, G possesses an element of order p.*

Proof. Choose $b = 1$ in Theorem I.4.14(i). □

Example I.4.17.

(i) For $|G| = 15 = 3 \cdot 5$, $|\mathrm{Syl}_3(G)|$ is a divisor of 5 and 1 modulo 3 according to Theorem I.4.14(iv). This shows $|\mathrm{Syl}_3(G)| = 1$. Analogously, one shows that G possesses only one 5-Sylow subgroup. Thus G contains only seven elements of order 1, 3 or 5. Therefore, elements of order 15 exist, i. e. $G \cong C_{15}$.

(ii) Let $|G| = 12 = 2^2 \cdot 3$. As in (i), then $|\mathrm{Syl}_3(G)| \in \{1, 4\}$. Let us assume $\mathrm{Syl}_3(G) = \{P_1, \ldots, P_4\}$. According to Lagrange, $P_i \cap P_j = 1$ for $i \neq j$. This shows $|P_1 \cup \ldots \cup P_4| = 1 + 4 \cdot 2 = 9$. Thus there is only room for one 2-Sylow subgroup. In any case, G has a normal subgroup of order 3 or 4.

(iii) According to Sylow, A_4 possesses subgroups of order $1, 2, 3, 4, 12$. However, there is no subgroup of order 6 (Exercise I.21). The converse of Lagrange is therefore false.

(iv) Let $N \trianglelefteq G$ and $P \in \mathrm{Syl}_p(N)$. Then G acts by conjugation on $\mathrm{Syl}_p(N)$ and N acts transitively according to Sylow. The Frattini argument shows $G = N\mathrm{N}_G(P)$.

Lemma I.4.18. *Let $N \trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$. Then $P \cap N \in \mathrm{Syl}_p(N)$ and $PN/N \in \mathrm{Syl}_p(G/N)$.*

Proof. Because of $P \cap N \leq P$, $P \cap N$ is a p-subgroup of N. According to the first isomorphism theorem, $PN \leq G$ and Lemma I.3.14 shows

$$|N : P \cap N| = |PN : P| \not\equiv 0 \pmod{p}.$$

Thus $P \cap N \in \mathrm{Syl}_p(N)$. Because of $PN/N \cong P/P \cap N$, PN/N is a p-subgroup of G/N and the second isomorphism theorem yields

$$|G/N : PN/N| = |G : PN| = \frac{|G : P|}{|PN : P|} \not\equiv 0 \pmod{p}.$$

This shows $PN/N \in \mathrm{Syl}_p(G/N)$. □

Theorem I.4.19 (Burnside's Lemma[2]). *Let G be a finite group and Ω a G-set. For $g \in G$, let $f(g) := |\{\omega \in \Omega : g \in G_\omega\}|$ be the number of fixed points of g on Ω. Then*

$$\boxed{\frac{1}{|G|}\sum_{g\in G} f(g)}$$

is the number of orbits of G on Ω.

Proof. If $\alpha, \beta \in \Omega$ lie in the same orbit, then $|G : G_\alpha| = |{}^G\alpha| = |{}^G\beta| = |G : G_\beta|$ holds according to Theorem I.4.7. By Lagrange, it follows that $|G_\alpha| = |G_\beta|$ (note $|G| < \infty$). Let $\Delta \subseteq \Omega$ be a system of representatives for the orbits of G on Ω. Then

$$\begin{aligned}\sum_{g\in G} f(g) &= |\{(g,\omega) \in G \times \Omega : {}^g\omega = \omega\}| = \sum_{\omega\in\Omega} |G_\omega| = \sum_{\delta\in\Delta} |{}^G\delta||G_\delta| \\ &= \sum_{\delta\in\Delta} |G : G_\delta||G_\delta| = \sum_{\delta\in\Delta} |G| = |\Delta||G|.\end{aligned}$$

□

Example I.4.20.

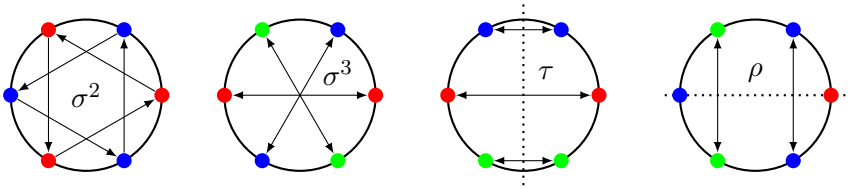
(i) In the case of the conjugation action of G on G, one obtains

$$k(G) = \frac{1}{|G|}\sum_{g\in G} |\mathrm{C}_G(g)|.$$

(ii) Let G be a finite group that acts transitively on Ω with $|\Omega| > 1$. According to Burnside's Lemma, 1 is the average number of fixed points of elements from G. On the other hand, $f(1) = |\Omega| > 1$. There must therefore always be fixed-point-free elements in G.

(iii) We want to count necklaces with six beads, where beads in three colors are available. Naively, there are initially 3^6 such necklaces, some of which are however identical. We arrange the necklace such that the beads form a regular 6-gon. Rotation by $\pi/3$ will not change the necklaces. Likewise, we can rotate the necklace in space and thereby realize a reflection of the 6 vertices. Two necklaces are thus identical if and only if they lie in the same orbit under the dihedral group $G := D_{12}$ (see Exercise I.20). We apply Burnside's Lemma to the set Ω of the 3^6 necklaces.

Certainly $f(1) = 3^6$. A rotation $\sigma \in G$ by $\pi/3$ leaves only the three monochromatic necklaces fixed, i. e. $f(\sigma) = 3$. The rotation σ^2 by $2\pi/3$ leaves the monochromatic necklaces and the necklaces with alternating colors fixed. There are $f(\sigma^2) = 3^2$ of these. Analogously, one shows $f(\sigma^3) = 3^3$. Furthermore, $f(\sigma^4) = f(\sigma^{-2}) = 3^2$, $f(\sigma^5) = f(\sigma^{-1}) = 3$ as well as $\sigma^6 = 1$. Now let τ be one of the three reflections through two midpoints of sides. Then $f(\tau) = 3^3$. Finally, if ρ is one of the three reflections through two vertices, then $f(\rho) = 3^4$.



[2]was already known before Burnside, see [P. M. Neumann, *A lemma that is not Burnside's*, Math. Sci. 4 (1979), 133–141]

According to Burnside's Lemma, there are

$$\begin{aligned}\frac{1}{12}\left(3^6+2\cdot 3+2\cdot 3^2+3^3+3\cdot 3^3+3\cdot 3^4\right) &= \frac{1}{4}\left(3^4(3+1)+3^2(1+3)+2+6\right)\\ &= 81+9+2=92\end{aligned}$$

different necklaces.

I.5 Abelian Groups

Remark I.5.1. With direct products, new groups can be constructed from old ones. We now try, conversely, to write given groups as direct products.

Lemma I.5.2. *For $N, M \trianglelefteq G$ with $N \cap M = 1$, it holds that $xy = yx$ for all $x \in N$ and $y \in M$. This holds in particular if* $\gcd(|N|, |M|) = 1$.

Proof. For $x \in N$ and $y \in M$ it holds that

$$\underbrace{\overbrace{xyx^{-1}}^{\in N}y^{-1}}_{\in M} \in N \cap M = 1,$$

i. e. $xy = yx$. According to Lagrange, $|N \cap M|$ is a divisor of $\gcd(|N|, |M|)$. Therefore, the second statement follows from the first. □

Lemma I.5.3. *Let $N_1, \ldots, N_k \trianglelefteq G$ with $G = N_1 \ldots N_k$ and $N_i \cap \prod_{j \neq i} N_j = 1$ for $i = 1, \ldots, n$. Then $G \cong N_1 \times \ldots \times N_k$.*

Proof. We show that the map

$$\begin{aligned} F \colon N_1 \times \ldots \times N_k &\to G, \\ (x_1, \ldots, x_k) &\mapsto x_1 \ldots x_k \end{aligned}$$

is an isomorphism. By assumption, $N_i \cap N_j \subseteq N_i \cap \prod_{l \neq i} N_l = 1$ for $i \neq j$. Lemma I.5.2 shows $xy = yx$ for $x \in N_i$ and $y \in N_j$. Now let $x_i, y_i \in N_i$ for $i = 1, \ldots, k$. Then

$$F(x_1, \ldots, x_k)F(y_1, \ldots, y_k) = x_1 \ldots x_k y_1 \ldots y_k = x_1 y_1 x_2 y_2 \ldots x_k y_k = F((x_1, \ldots, x_k)(y_1, \ldots, y_k)).$$

Thus F is a homomorphism. Because of $G = N_1 \ldots N_k$, F is surjective. Let $(x_1, \ldots, x_k) \in \mathrm{Ker}(F)$. Suppose there exists $1 \leq l \leq k$ with $x_l \neq 1$. Let l be maximal. Then $x_l^{-1} = x_1 \ldots x_{l-1} \in N_l \cap N_1 \ldots N_{l-1} = 1$. Thus $\mathrm{Ker}(F) = 1$ and F is also injective. □

Definition I.5.4. In the situation of Lemma I.5.3, G is called the *direct sum* of $N_1, \ldots, N_k$ and one writes $G = N_1 \oplus \ldots \oplus N_k$.

Remark I.5.5.

(i) Conversely, if $G = G_1 \times \ldots \times G_k$ is given, then $G = N_1 \oplus \ldots \oplus N_k$ holds with

$$N_i := \{(g_1, \ldots, g_k) \in G : g_j = 1 \, \forall j \neq i\}$$

for $i = 1, \ldots, k$. Therefore, direct sums and direct products are only different perspectives of the same fact (as with vector spaces).

(ii) In general, the summands of a direct sum are not uniquely determined. For example,

$$V_4 = \langle (1,2)(3,4)\rangle \oplus \langle (1,3)(2,4)\rangle = \langle (1,2)(3,4)\rangle \oplus \langle (1,4)(2,3)\rangle = \langle (1,3)(2,4)\rangle \oplus \langle (1,4)(2,3)\rangle$$

(Exercise I.16).

(iii) Certainly $N_1 \oplus N_2 = N_2 \oplus N_1$. Let

$$G = (N_1 \oplus N_2) \oplus N_3.$$

Since $\trianglelefteq$ is not transitive, it is not immediately clear whether $N_1 \trianglelefteq G$ holds. Because of $N_1 \cap N_3 \subseteq N_1N_2 \cap N_3 = 1$, we have $xy = yx$ for $x \in N_1$ and $y \in N_3$. This shows $N_3 \leq \mathrm{C}_G(N_1) \leq \mathrm{N}_G(N_1)$. Furthermore, $N_1 \trianglelefteq N_1 \oplus N_2$ and therefore $N_1N_2 \leq \mathrm{N}_G(N_1)$. Overall,

$$G = (N_1N_2)N_3 \leq \mathrm{N}_G(N_1),$$

i. e. $N_1 \trianglelefteq G$. Analogously $N_2 \trianglelefteq G$. Finally, let $x = yz \in N_1 \cap N_2N_3$ with $y \in N_2$ and $z \in N_3$. Then $z = y^{-1}x \in N_3 \cap N_2N_1 = 1$ and $x = y \in N_1 \cap N_2 = 1$. This shows $N_1 \cap N_2N_3 = 1$ and analogously $N_2 \cap N_1N_3 = 1$. Thus $G = N_1 \oplus N_2 \oplus N_3$. Direct sums are therefore commutative and associative.

Example I.5.6. Let $p_1, \ldots, p_n$ be the prime divisors of $|G|$. Suppose $\mathrm{Syl}_{p_i}(G) = \{P_i\}$ for $i = 1, \ldots, n$ (groups with this property are called *nilpotent*). According to Corollary I.4.15, $P_1, \ldots, P_n \trianglelefteq G$ holds. By Lagrange, $P_i \cap P_j = 1$ for $i \neq j$. According to Lemma I.3.14, it therefore holds that $|P_1P_2| = |P_1||P_2|$. Again by Lagrange, $P_3 \cap P_1P_2 = 1$. Inductively, it easily follows that

$$|P_1 \ldots P_n| = |P_1| \ldots |P_n| = |G|$$

and $P_i \cap \prod_{j \neq i} P_j = 1$. Thus $G = P_1 \oplus \ldots \oplus P_n$. In particular, every abelian group is the direct sum of its Sylow subgroups.

Definition I.5.7. For an abelian p-group G, let

$$\Omega(G) := \{g \in G : g^p = 1\},$$
$$\mho(G) := \{g^p : g \in G\}.$$

Because of $1^p = 1$ and $(gh^{-1})^p = g^ph^{-p}$ for $g, h \in G$, we have $\Omega(G), \mho(G) \leq G$.

Example I.5.8. It holds that $\Omega(G \oplus H) = \Omega(G) \oplus \Omega(H)$ and $\mho(G \oplus H) = \mho(G) \oplus \mho(H)$ as well as $\Omega(C_{p^a}) \cong C_p$ and $\mho(C_{p^a}) \cong C_{p^{a-1}}$ for $a \in \mathbb{N}$.

Theorem I.5.9 (Fundamental Theorem of Finite Abelian Groups)**.** *For every finite abelian group G, there exist uniquely determined prime powers $q_1 \geq \ldots \geq q_n > 1$ with*

$$G \cong C_{q_1} \times \ldots \times C_{q_n}.$$

Proof (MacCluer). According to Example I.5.6, G is the direct sum of its Sylow subgroups. Since direct sums are commutative and associative, we can assume that G is a p-group. Let H be a cyclic subgroup of G with the largest possible order p^a. By induction on $|G|$, it suffices to show that H is a direct summand of G. First, assume that an element $x \in G \setminus H$ of order p exists. Then $H\langle x\rangle/\langle x\rangle \cong H/H \cap \langle x\rangle = H/1 \cong H$ is a maximal cyclic subgroup of $G/\langle x\rangle$ (since G is abelian, all

subgroups are normal). By induction, $G/\langle x\rangle = H\langle x\rangle/\langle x\rangle \oplus K/\langle x\rangle$ for some $K \leq G$ (Correspondence Theorem). Then certainly $G = H\langle x\rangle K = HK$ and

$$H \cap K = H \cap H\langle x\rangle \cap K = H \cap \langle x\rangle = 1.$$

This shows $G = H \oplus K$. We can therefore assume that all elements of order $\leq p$ of G lie in H. Since H is cyclic, there are only p such elements (Theorem I.3.34). The kernel of the endomorphism $f\colon G \to G$, $g \mapsto g^p$ therefore has order p. It follows that $|f(G)| = |G|/p$ from the Homomorphism Theorem. According to Cauchy, $f(G)$ also has exactly p elements of order $\leq p$ (except in the case $f(G) = 1$). Repeated application of f therefore shows

$$1 = |f^a(G)| = |G|/p^a = |G : H|$$

by the choice of H. Thus $G = H$ is cyclic and the existence of the decomposition is proven.

For the uniqueness of the decomposition, let

$$G = G_1 \oplus \ldots \oplus G_n \cong C_{p^{a_1}} \times \ldots \times C_{p^{a_n}}$$

with $a_1 \geq \ldots \geq a_n \geq 1$. According to Example I.5.8,

$$|\Omega(G)| = |\Omega(G_1) \oplus \ldots \oplus \Omega(G_n)| = |C_p \times \ldots \times C_p| = p^n.$$

In particular, n is uniquely determined by G. Furthermore,

$$\mho(G) = \mho(G_1) \oplus \ldots \oplus \mho(G_n) \cong C_{p^{a_1-1}} \times \ldots \times C_{p^{a_n-1}}.$$

By induction, the $a_i > 1$ are uniquely determined by G. Since n is already known, the number of $a_i = 1$ is also uniquely determined. □

Example I.5.10.

(i) We already know that 1, C_2, C_3 are the only groups of order 1, 2 and 3. Now let $|G| = 4$. According to Corollary I.4.12, G is abelian and therefore isomorphic to either C_4 or $C_2 \times C_2$. For example, $V_4 \cong C_2 \times C_2$ (Exercise I.16).

(ii) Let $|G| = 6$ and $P \in \mathrm{Syl}_2(G)$. As usual, G acts on G/P with kernel $N \leq P$ (Remark I.4.6(i)). In the case $N = 1$, one obtains an isomorphism $G \to \mathrm{Sym}(G/P) \cong S_3$. Now let $P = N \trianglelefteq G$. According to Sylow, G also possesses a normal 3-Sylow subgroup Q. From Example I.5.6 and Theorem I.3.34 it follows that $G = P \oplus Q \cong C_2 \times C_3 \cong C_6$. Thus C_6 and S_3 are the only groups of order 6 up to isomorphism. In particular, $D_6 \cong S_3$, because D_6 is not abelian.

(iii) For every prime p, there are exactly three abelian groups of order p^3 up to isomorphism: C_{p^3}, $C_{p^2} \times C_p$ and $C_p \times C_p \times C_p$.

Remark I.5.11. According to Theorem I.3.34, we know the subgroups and factor groups of cyclic groups. We now determine the isomorphism types of subgroups and factor groups of an arbitrary abelian group.

Theorem I.5.12. *Let $H \leq G \cong C_{q_1} \times \ldots \times C_{q_n}$ with prime power $q_1, \ldots, q_n$. Then there exist divisors $r_i \mid q_i$ for $i = 1, \ldots, n$ with $H \cong C_{r_1} \times \ldots \times C_{r_n}$. Conversely, for given (positive) divisors $r_i \mid q_i$, there exists an $H \leq G$ with $H \cong C_{r_1} \times \ldots \times C_{r_n}$.*

Proof. Induction on $|G|$: Since the (only) Sylow p-subgroup of H lies in the Sylow p-subgroup of G, we may assume that G and H are p-groups. Thus let $G \cong C_{p^{a_1}} \times \ldots \times C_{p^{a_n}}$ and $H \cong C_{p^{b_1}} \times \ldots \times C_{p^{b_m}}$ with wlog. $a_1 \geq \ldots \geq a_n \geq 1$ and $b_1 \geq \ldots \geq b_m \geq 1$. Because of $\Omega(H) \subseteq \Omega(G)$, we have $p^m = |\Omega(H)| \leq |\Omega(G)| = p^n$ and $m \leq n$. According to Example I.5.8,

$$C_{p^{b_1-1}} \times \ldots \times C_{p^{b_m-1}} \cong \mho(H) \leq \mho(G) \cong C_{p^{a_1-1}} \times \ldots \times C_{p^{a_n-1}}.$$

Induction yields $b_i \leq a_i$ for $i = 1, \ldots, m$. This shows the first assertion.

For divisors $r_i \mid q_i$, there exists a subgroup $C_{r_i} \leq C_{q_i}$ according to Theorem I.3.34. Then certainly $C_{r_1} \times \ldots \times C_{r_n} \leq C_{q_1} \times \ldots \times C_{q_n}$ and the second assertion follows. □

Remark I.5.13. The analogous statement also holds for factor groups (Exercise I.29).

Example I.5.14. The group $C_8 \times C_4$ has subgroups (as well as factor groups) of type C_1, C_2, C_4, C_8, C_2^2, $C_4 \times C_2$, $C_8 \times C_2$, C_4^2 and $C_8 \times C_4$. It is difficult to determine how many subgroups of each type exist. For example, $V_4 \cong C_2^2$ has three subgroups of type C_2.

I.6 Solvable and simple groups

Definition I.6.1. A finite group G is called

- *simple*, if G has exactly two normal subgroups (namely 1 and $G \neq 1$; cf. prime number).
- *solvable*, if subgroups $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ exist, such that G_i/G_{i-1} is abelian for $i = 1, \ldots, n$.

Remark I.6.2. Note: For solvability, $G_i \trianglelefteq G$ is not required.

Example I.6.3.

(i) By Lagrange, the groups C_p for $p \in \mathbb{P}$ are simple.

(ii) Every abelian group is solvable (set $n = 1$).

(iii) According to Exercise I.20, D_{2n} has a cyclic normal subgroup of index 2. Thus D_{2n} is solvable. In particular, $S_3 \cong D_6$ is solvable.

(iv) Let G be simple and solvable with $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ as in Definition I.6.1. Wlog. let $G_{n-1} < G$ (note $G \neq 1$). Because of $G_{n-1} \trianglelefteq G$, it follows that $G_{n-1} = 1$ and $G \cong G_n/G_{n-1}$ is abelian. In particular, every subgroup of G is normal and due to simplicity, G has no non-trivial, proper subgroup. By Cauchy, $|G|$ is a prime number. The groups C_p ($p \in \mathbb{P}$) are therefore the only simple, solvable groups.

Theorem I.6.4. *A finite group G is solvable if and only if subgroups $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ exist, such that G_i/G_{i-1} is cyclic for $i = 1, \ldots, n$.*

Proof. Since cyclic groups are abelian, every group with the given condition is solvable. Conversely, let G be solvable and $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ with abelian factors. Between G_{i-1} and G_i we insert further subgroups, such that the resulting factors are cyclic. By the correspondence theorem, we may assume $G = G_i/G_{i-1}$ for this, i. e. G is abelian. By Theorem I.5.9 there exist cyclic normal subgroups $N_1, \ldots, N_k$ with $G = N_1 \oplus \ldots \oplus N_k$. Because of

$$N_1 \ldots N_i / N_1 \ldots N_{i-1} \cong N_i/(N_i \cap N_1 \ldots N_{i-1}) = N_i/1 \cong N_i$$

the series $1 \leq N_1 \leq N_1N_2 \leq \ldots \leq N_1 \ldots N_k = G$ has cyclic factors. □

Theorem I.6.5. *Let G be a finite group with $H \leq G$ and $N \trianglelefteq G$.*

(i) If G is solvable, then so are H and G/N.

(ii) If N and G/N are solvable, then so is G.

Proof.

(i) Let $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ with abelian factors. Then $1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \ldots \trianglelefteq G_n \cap H = H$ and

$$(G_i \cap H)/(G_{i-1} \cap H) = (G_i \cap H)/((G_i \cap H) \cap G_{i-1}) \cong (G_i \cap H)G_{i-1}/G_{i-1} \leq G_i/G_{i-1}$$

is abelian for $i = 1, \ldots, n$. Analogously, $1 = G_0N/N \trianglelefteq G_1N/N \trianglelefteq \ldots \trianglelefteq G_nN/N = G/N$ and

$$\begin{aligned}(G_iN/N)/(G_{i-1}N/N) &\cong G_iN/G_{i-1}N = G_i(G_{i-1}N)/G_{i-1}N \cong G_i/(G_i \cap G_{i-1}N) \\ &\overset{\text{I.3.14}}{=} G_i/(G_i \cap N)G_{i-1} \cong (G_i/G_{i-1})/((G_i \cap N)G_{i-1}/G_{i-1})\end{aligned}$$

is abelian for $i = 1, \ldots, n$.

(ii) Let $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_r = N$ and $1 = G_0/N \trianglelefteq \ldots \trianglelefteq G_s/N = G/N$ with abelian factors. Then $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_r = N = G_0 \trianglelefteq \ldots \trianglelefteq G_s = G$. Because of $G_i/G_{i-1} \cong (G_i/N)/(G_{i-1}/N)$, the factors of this series are also abelian. □

Example I.6.6. According to Example I.4.17, every group G of order 12 has a normal subgroup N of order 3 or 4. Obviously, N and G/N are then solvable, and thus also G. In particular, A_4 is solvable (cf. Exercise I.16). Because of $|S_4 : A_4| = 2$, S_4 is also solvable.

Theorem I.6.7. *p-groups are solvable.*

Proof. Let G be a p-group with $|G| = p^n$. Induction on n: For $n = 0$, $G = 1$ is solvable. Now let $n \geq 1$. According to Theorem I.4.11, $\mathrm{Z}(G) \neq 1$. As an abelian group, $\mathrm{Z}(G)$ is solvable. By induction, $G/\mathrm{Z}(G)$ is solvable. According to Theorem I.6.5, G is also solvable. □

Lemma I.6.8. *Groups of order pq with $p, q \in \mathbb{P}$ are solvable.*

Proof. According to Theorem I.6.7, we can assume $p < q$. For $Q \in \mathrm{Syl}_q(G)$, $|G : \mathrm{N}_G(Q)|$ is a divisor of p and 1 modulo q according to Sylow. This shows $Q \trianglelefteq G$. Since Q and $G/Q \cong C_p$ are solvable, G is also solvable. □

Lemma I.6.9. *Let G be non-abelian and simple. For $H < G$, then $|G : H| \geq 5$ holds.*

Proof. According to Remark I.4.6, there exists a homomorphism $f\colon G \to \mathrm{Sym}(G/H)$ with $\mathrm{Ker}(f) \leq H < G$. Since G is simple, $\mathrm{Ker}(f) = 1$ holds and G is isomorphic to a subgroup of $\mathrm{Sym}(G/H)$. In the case $|G : H| \leq 4$, $\mathrm{Sym}(G/H) \leq S_4$ would be solvable and thus also G. Contradiction. □

Theorem I.6.10. *Groups of order < 60 are solvable.*

Proof. Let G be a minimal counterexample. By Theorem I.6.5, G is simple. By Theorem I.6.7, G is not a p-group. For every Sylow group P of G, it therefore holds that $|G : P| \geq 5$ by Lemma I.6.9. The orders $|G| = 35 = 5 \cdot 7$ and $|G| = 55 = 5 \cdot 11$ are excluded by Lemma I.6.8. The following orders for $|G|$ remain:

$$30, 40, 42, 45, 56.$$

We consider only the first case (rest in Exercise I.30). By Sylow, $\mathrm{Syl}_5(G) = \{P_1, \ldots, P_6\}$ because $|G| = 30 = 2 \cdot 3 \cdot 5$. Because $|P_1 \cup \ldots \cup P_6| = 1 + 6 \cdot 4 = 25$, there is only room for at most two 3-Sylow groups. By Sylow, it follows that $|\mathrm{Syl}_3(G)| = 1$ in contradiction to the simplicity of G. □

Lemma I.6.11. *For $n \in \mathbb{N}$, A_n is generated by the 3-cycles.*

Proof. For $n \leq 2$, $A_n = 1 = \langle \varnothing \rangle$. So let $n \geq 3$. By Remark I.3.8 and Theorem I.3.26, $\sigma \in A_n$ can be written as a product of an even number of transpositions. For the product of two transpositions, it holds that

$$(a,b)(c,d) = \begin{cases} 1 & \text{if } \{a,b\} = \{c,d\}, \\ (a,d,b) & \text{if } a = c,\ b \neq d, \\ (a,c,b)(a,c,d) & \text{if } \{a,b\} \cap \{c,d\} = \varnothing. \end{cases}$$

□

Remark I.6.12. For $\sigma, (a_1, \ldots, a_k) \in S_n$, it holds that

$$\sigma(a_1, \ldots, a_k)\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k)). \tag{I.6.1}$$

Theorem I.6.13. *For $n \geq 5$, A_n is simple. In particular, S_n is not solvable.*

Proof. Let $1 \neq N \trianglelefteq A_n$. We must show $N = A_n$. First, let $n = 5$. According to Example I.3.30,

$$|A_5| = \frac{5!}{2} = 60 = 2^2 \cdot 3 \cdot 5$$

and A_5 consists, according to Exercise I.15, of the following elements: identity, 15 elements of order 2 (cycle type $(2,2)$), 20 elements of order 3 (cycle type (3)) and 24 elements of order 5 (cycle type (5)). Suppose that $|N|$ has a prime divisor $p \in \{3,5\}$. By Sylow, N then contains all Sylow p-subgroups and thus all p-elements of A_5. This shows $|N| = 1 + |N \setminus \{1\}| \geq 1 + 20$ and Lagrange yields $|N| \in \{30, 60\}$. Thus N even contains all 3-elements and 5-elements. This shows $|N| \geq 44$ and $N = A_5$.

Now let $|N|$ be a power of 2. In the case $|N| = 4$, A_5 would have only one 2-Sylow subgroup and only three elements of order 2. Thus $|N| = 2$, say $N = \langle (1,2)(3,4) \rangle$. Then one obtains the contradiction $(1,2,3)(1,2)(3,4)(1,2,3)^{-1} = (1,4)(2,3) \notin N$. This shows $N = A_5$ and A_5 is simple.

Now let $n \geq 6$ and $\sigma \in N \setminus \{1\}$. Choose $1 \leq a \leq n$ with $b := \sigma(a) \neq a$ and $c \in \{1, \ldots, n\} \setminus \{a, b, \sigma(b)\}$. According to (I.6.1),

$$N \ni \sigma(a,b,c)\sigma^{-1}(a,b,c)^{-1} = (b, \sigma(b), \sigma(c))(b,a,c) =: \tau \neq 1.$$

Choose $d, e \in \{1, \ldots, n\}$ with $|\{a,b,c,d,e\}| = 5$ and

$$\tau \in A_n \cap \operatorname{Sym}(\{a,b,c,d,e\}) =: H.$$

If $f \colon \{1, \ldots, 5\} \to \{a,b,c,d,e\}$ is a bijection, then $A_5 \to H$, $\alpha \mapsto f\alpha f^{-1}$ is an isomorphism. According to the first part of the proof, H is simple. By the first isomorphism theorem, $1 \neq \tau \in H \cap N \trianglelefteq H$ and it follows that $(a,b,c) \in H = H \cap N \leq N$. Let $(a',b',c') \in A_n$ be arbitrary and $\alpha \in S_n$ with $\alpha(a) = a'$, $\alpha(b) = b'$, $\alpha(c) = c'$. By possible multiplication with (d,e), one can achieve $\alpha \in A_n$. According to (I.6.1), it then holds that

$$(a',b',c') = \alpha(a,b,c)\alpha^{-1} \in N.$$

From Lemma I.6.11 it follows that $N = A_n$. Thus A_n is simple. According to Example I.6.3(iv), A_n is not solvable. The second assertion follows from Theorem I.6.5. □

Remark I.6.14.

(i) One of the largest mathematical projects was the classification of all finite simple groups. In addition to the families C_p and A_n, there are a number of matrix groups (groups of *Lie type* such as

$$\mathrm{PSL}(n,K) := \mathrm{SL}(n,K)/\mathrm{Z}(\mathrm{SL}(n,K))$$

for a finite field K with $(n,|K|) \notin \{(2,2),(2,3)\}$) as well as 26 exceptions (*sporadic* groups). The largest sporadic group is the *Monster group* with

$$808.017.424.794.512.875.886.459.904.961.710.757.005.754.368.000.000.000 \approx 10^{54}$$

elements. The proof of the classification has over $10,000$ pages[1].

(ii) Burnside proved that groups of order $p^a q^b$ for prime numbers p and q are solvable (Theorem II.14.33). Feit and Thompson proved that groups of odd order are solvable. This proof has approx. 250 pages.

(iii) In the following, we prove a unique "prime factorization" for groups.

Definition I.6.15. A sequence of subgroups $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$ is called a *composition series* if the factors G_i/G_{i-1} for $i = 1,\ldots,n$ are simple.

Remark I.6.16. Every finite group G possesses a composition series: This is clear if $G = 1$ (set $n = 0$). Now let $G \neq 1$ and $N \lhd G$ be a maximal proper normal subgroup of G. By induction on $|G|$, we can assume that N possesses a composition series $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k = N$. By the second isomorphism theorem, G/N is simple. Thus $1 = N_0 \trianglelefteq \ldots \trianglelefteq N_k \trianglelefteq G$ is a composition series of G. We now concern ourselves with the uniqueness of composition series.

Theorem I.6.17 (Jordan-Hölder)**.** *Let $1 = G_k \trianglelefteq \ldots \trianglelefteq G_0 = G$ and $1 = H_l \trianglelefteq \ldots \trianglelefteq H_0 = G$ be composition series of G. Then $k = l$ and there exists a $\pi \in S_k$ with $G_{i-1}/G_i \cong H_{\pi(i)-1}/H_{\pi(i)}$ for $i = 1,\ldots,k$. One calls $G_0/G_1,\ldots,G_{k-1}/G_k$ the* composition factors *of G.*

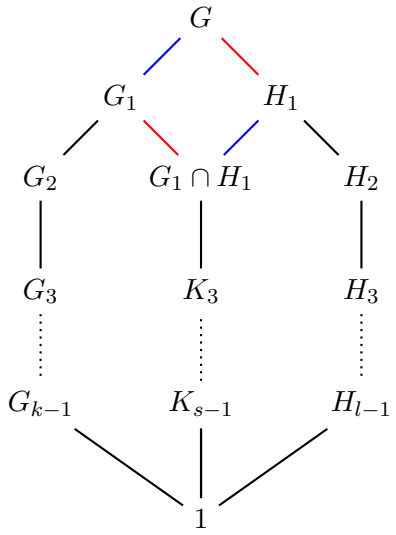
Proof. Induction on $|G|$: Wlog. let $G \neq 1$. In the case $G_1 = H_1$, the claim follows by induction. So let $G_1 \neq H_1$. Because $G_1, H_1 \trianglelefteq G$, it follows that $G_1H_1 = H_1G_1 \trianglelefteq G$. Since G/G_1 is simple, it follows that $G = G_1H_1$. The first isomorphism theorem shows

$$G/G_1 = H_1G_1/G_1 \cong H_1/H_1 \cap G_1, \qquad G/H_1 = G_1H_1/H_1 \cong G_1/G_1 \cap H_1. \tag{I.6.2}$$

Let $1 = K_s \trianglelefteq \ldots \trianglelefteq K_2 = G_1 \cap H_1$ be an arbitrary composition series. By induction, the composition series $G_k \trianglelefteq \ldots \trianglelefteq G_1$ and $K_s \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq G_1$ are then of the same length (i. e. $k = s$) and their factors are isomorphic (up to the order). Now the composition series $1 = K_k \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq H_1$ and $1 = H_l \trianglelefteq \ldots \trianglelefteq H_1$ are also of the same length with isomorphic factors. Thus $k = s = l$ and according to (I.6.2), the composition series

[1] Current status: [Solomon, *The Classification of Finite Simple Groups: A Progress Report*, Notices of the AMS 65 (2018), 646–651, `https://www.ams.org/journals/notices/201806/rnoti-p646.pdf`]

$G_k \trianglelefteq \ldots \trianglelefteq G_0$,
$K_k \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq G_1 \trianglelefteq G_0$,
$K_k \trianglelefteq \ldots \trianglelefteq K_2 \trianglelefteq H_1 \trianglelefteq H_0$,
$H_k \trianglelefteq \ldots \trianglelefteq H_0$



have isomorphic factors. □

Example I.6.18.

(i) Obviously $1 < \langle (1,2)(3,4) \rangle < V_4 < A_4 < S_4$ is a composition series of S_4 (cf. Exercise I.16). Therefore C_2, C_2, C_2, C_3 are the composition factors of S_4. If one replaces $(1,2)(3,4)$ with $(1,3)(2,4)$ or $(1,4)(2,3)$, one obtains further composition series.

(ii) According to Theorem I.6.13, $1 < A_n < S_n$ is a composition series of S_n for $n \geq 5$.

(iii) According to Theorem I.6.5, the composition factors of a solvable group are solvable and therefore of prime order. A group is thus solvable if and only if all composition factors have prime order. In particular, C_p is (up to multiplicity) the only composition factor of every non-trivial p-group.

(iv) For given simple groups $G_1, \ldots, G_n$, there always exists a group with composition factors $G_1, \ldots, G_n$, namely $G_1 \times \ldots \times G_n$. As a rule, however, there are many non-isomorphic groups with the same composition factors.

I.7 Rings

Definition I.7.1. A *ring* is a set R with operations $+$ and $\cdot$, such that:

- $(R, +)$ is an abelian group with neutral element 0,
- $\forall a, b, c \in R : a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associative),
- $\exists 1 \in R : \forall a \in R : 1 \cdot a = a = a \cdot 1$ (neutral element),
- $\forall a, b, c \in R : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (distributive).

If $\cdot$ is additionally commutative, then R is called *commutative*.

Remark I.7.2.

(i) As usual, we write ab instead of $a \cdot b$. The inverse of $a \in R$ with respect to $+$ is called $-a$ and we write $a - b := a + (-b)$. To save parentheses, we agree on "multiplication before addition", i. e. $ab + c := (ab) + c$.

(ii) For $a \in R$, $a0 = a(0 + 0) = a0 + a0 = 0 = 0a$.

(iii) In the case $0 = 1$, $a = a1 = a0 = 0$ for all $a \in R$, i. e. $R = \{0\}$ is the *zero ring*. This uninteresting ring will be neglected in the following.

(iv) If $\cdot$ is commutative, it suffices to require one of the two distributive laws. In contrast to groups, one does not speak of abelian rings.

Example I.7.3.

(i) The integers $\mathbb{Z}$ and every field are commutative rings.

(ii) For rings $R_1, \ldots, R_n$, the *direct product* $R_1 \times \ldots \times R_n$ is also a ring with component-wise operations (as for groups).

(iii) For every ring R and $n \in \mathbb{N}$, the *matrix ring* $R^{n \times n}$ is a ring with respect to addition and multiplication of matrices.[1] For $n \geq 2$, $R^{n \times n}$ is not commutative.

Definition I.7.4. Let $R \neq \{0\}$ be a ring.

- One calls $a \in R$ *invertible* (or *unit*), if $b \in R$ with $ba = 1 = ab$ exists. As usual, b is then uniquely determined and one writes $a^{-1} := b$. The invertible elements of R form a group $R^\times \subseteq R \setminus \{0\}$, which is called the *unit group* of R (verify).[2]
- One calls $a \in R \setminus \{0\}$ a *zero divisor*, if $b \in R \setminus \{0\}$ with $ab = 0$ or $ba = 0$ exists. A commutative ring without zero divisors is called an *integral domain*.
- An element $a \in R$ is called *idempotent*, if $a^2 = a$ (Exercise II.7).

[1] The calculation rules for matrices known from linear algebra do not depend on whether R is commutative.
[2] Some authors write $U(R)$ (units) instead of $R^\times$

- One calls $a \in R$ *nilpotent*, if an $n \in \mathbb{N}$ with $a^n = 0$ exists (Exercise II.43).

Example I.7.5.

(i) A ring R with $R^\times = R \setminus \{0\}$ is called a *division ring*. A commutative division ring is a field. In Algebra II, we show that every finite division ring is a field (Theorem II.8.7).

(ii) Let $a \in \mathbb{Z}$ be invertible and $b \in \mathbb{Z}$ with $ba = 1$. Then it follows that $a \in \{\pm 1\}$. This shows $\mathbb{Z}^\times = \{\pm 1\}$.

(iii) For every field K and $n \in \mathbb{N}$, $(K^{n\times n})^\times = \mathrm{GL}(n, K)$.

(iv) For rings R, S, it holds that $(R \times S)^\times = R^\times \times S^\times$.

(v) Every field is an integral domain and every finite integral domain is a field (Exercise I.36).

(vi) $\mathbb{Z}$ is an integral domain, but not a field.

(vii) $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ is a zero divisor in $K^{2\times 2}$.

Remark I.7.6. In every integral domain, the *cancellation rule* $ab = ac \Longrightarrow b = c$ holds for $a, b, c \in R$ and $a \neq 0$. This follows from $a(b - c) = 0$.

Definition I.7.7. Let R be a ring.

(i) A *subring* of R is a subset $S \subseteq R$ with $1, a - b, ab \in S$ for $a, b \in S$.

(ii) An *ideal* of R is a non-empty subset $I \subseteq R$ with $a - b, xa, ax \in I$ for $a, b \in I$ and $x \in R$. One then writes $I \trianglelefteq R$ or $I \triangleleft R$, if I is a *proper* ideal, i. e. $I \neq R$.

(iii) An $I \triangleleft R$ is called *maximal*, if no $J \triangleleft R$ with $I \subsetneq J$ exists.

Remark I.7.8.

(i) Every subring $S \subseteq R$ becomes a ring itself with the restricted operations (verify).

(ii) Every $I \trianglelefteq R$ is an abelian group with respect to $+$ (verify). In particular, $0 \in I$.

Example I.7.9.

(i) R is a subring of R, but $\{0\}$ is not (except for $R = \{0\}$).

(ii) $\{0\}$ and R are ideals of R.

(iii) For every ring R, the *center*

$$\mathrm{Z}(R) := \{x \in R : rx = xr \ \forall r \in R\}$$

is a commutative subring.

(iv) Every subring of a field is an integral domain. For example $\mathbb{Z} \subseteq \mathbb{Q}$.

(v) Intersections, sums and products of ideals are again ideals (Exercise I.37).

(vi) For $U \subseteq R$,

$$(U) := \bigcap_{U \subseteq I \trianglelefteq R} I \trianglelefteq R$$

is the ideal *generated* by U. We also write $U = (x_1, \ldots, x_n) := (\{x_1, \ldots, x_n\})$. If R is commutative, then $(x) = Rx = \{ax : a \in R\}$ for $x \in R$. One then calls (x) a *principal ideal*. For example, $\{0\} = (0)$ and $R = (1)$ are always principal ideals.

(vii) Let $\{0\} \neq I \trianglelefteq \mathbb{Z}$ and $n \in I \cap \mathbb{N}$ minimal. For $m \in I$, Euclidean division yields $m = qn + r$ with $0 \leq r < n$. Because of $r = m - qn \in I$, it follows that $r = 0$ and $I = n\mathbb{Z} = (n)$. Because of $d \mid n \iff (n) \subseteq (d)$, (n) is maximal if and only if $n \in \mathbb{P}$.

Theorem I.7.10 (Quotient ring)**.** *For every ring R and $I \trianglelefteq R$, $R/I := \{a + I : a \in R\}$ becomes a ring with zero element $0 + I$ and identity element $1 + I$ via*

$$(a + I) \dot{+} (b + I) := (a \dot{+} b) + I.$$

Proof. According to Theorem I.3.19, R/I is already a group with respect to $+$. The other axioms are proven as in Theorem I.2.23. □

Example I.7.11. $\mathbb{Z}/4\mathbb{Z}$ is a commutative ring, but not an integral domain, because $(2 + 4\mathbb{Z})^2 = 0$.

Theorem I.7.12. *Let R be a commutative ring and $I \trianglelefteq R$. R/I is a field if and only if I is maximal.*

Proof. Let R/I be a field and $J \trianglelefteq R$ with $I \subsetneq J$. Choose $a \in J \setminus I$. Then $a + I \neq 0$ in R/I and there exists $b \in R$ with $ab + I = (a + I)(b + I) = 1 + I$. Let $x \in I$ with $1 = ab + x$. Then $R = R1 = Rab + Rx \subseteq J + I = J$ and I is maximal.

Conversely, let I be maximal in R and $a + I \neq 0 + I$. Because of $I \subsetneq (a) + I \trianglelefteq R$, it follows that $R = (a) + I$. Let $b \in R$ and $x \in I$ with $1 = ba + x$. Then

$$(b + I)(a + I) = ba + I = 1 - x + I = 1 + I.$$

Thus $a + I$ is invertible in R/I and R/I is a field. □

Corollary I.7.13. *For $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n \in \mathbb{P}$ holds.*

Proof. According to Example I.7.9, $n\mathbb{Z}$ is maximal if and only if $n \in \mathbb{P}$. □

Definition I.7.14. For $p \in \mathbb{P}$, one sets $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Theorem I.7.15. *For $n \in \mathbb{N}$, $(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} : \gcd(a, n) = 1\}$ holds. In particular,*

$$\boxed{|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n).}$$

Proof. For $a \in \mathbb{Z}$, it holds that

$$\begin{aligned} \gcd(a, n) = 1 &\overset{\text{I.2.28}}{\iff} \exists x \in \mathbb{Z} : ax \equiv 1 \pmod{n} \\ &\iff \exists x \in \mathbb{Z} : (a + n\mathbb{Z})(x + n\mathbb{Z}) = ax + n\mathbb{Z} = 1 + n\mathbb{Z} \\ &\iff a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times. \end{aligned}$$

□

Remark I.7.16. The elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ are called *prime* residue classes modulo n.

Example I.7.17. We want to determine the inverse of $7 + 31\mathbb{Z}$ in $(\mathbb{Z}/31\mathbb{Z})^\times$. The Euclidean algorithm yields $1 = \gcd(7, 31) = 9 \cdot 7 - 2 \cdot 31$. Thus $(7 + 31\mathbb{Z})^{-1} = 9 + 31\mathbb{Z}$.

Corollary I.7.18 (Euler-Fermat)**.** *For $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $\gcd(a, n) = 1$, $a^{\varphi(n)} \equiv 1 \pmod{n}$ holds. In particular, $a^{p-1} \equiv 1 \pmod{p}$ for $p \in \mathbb{P}$ with $p \nmid a$.*

Proof. For $G := (\mathbb{Z}/n\mathbb{Z})^\times$, it holds that

$$a^{\varphi(n)} + n\mathbb{Z} = (a + n\mathbb{Z})^{\varphi(n)} = (a + n\mathbb{Z})^{|G|} = 1 + n\mathbb{Z}.$$

according to Remark I.3.12. The second statement follows from $\varphi(p) = p - 1$. □

Example I.7.19 (RSA method)**.**

(i) Euler wants to send Gauss a secret message $n \in \mathbb{N}$ over an insecure channel (e. g. Internet). For this, Gauss chooses distinct prime numbers $p, q > \max\{n, 10^{1000}\}$ and $d \in \mathbb{Z}$ with $\gcd(d, \varphi(pq)) = 1$. According to Theorem I.7.15, there exist $e, k \in \mathbb{Z}$ with $de = 1 + k\varphi(pq)$. The numbers pq and e form the public key of Gauss, while d remains secret (p and q are no longer needed). Now Euler sends the encrypted message $\tilde{n} \equiv n^e \pmod{pq}$. For decryption, Gauss uses the formula

$$\tilde{n}^d \equiv n^{de} \equiv n^{1+k\varphi(pq)} \equiv n(n^{\varphi(pq)})^k \equiv n \pmod{pq}$$

according to Euler-Fermat (because $n < pq$, the result is uniquely determined). Without knowledge of p and q, an attacker can calculate neither $\varphi(pq)$ nor d (cf. Exercise I.12). Since no efficient factorization algorithm (for pq) is known so far, this method is currently secure. Most websites nowadays are encrypted in this way (`https`).

(ii) Instead of calculating $\tilde{n}^d \pmod{pq}$, Gauss can also determine the smaller powers

$$\begin{aligned} \tilde{n}^d &\equiv \tilde{n}^{d_p} \pmod{p} && \text{with } d_p \equiv d \pmod{p-1}, \\ \tilde{n}^d &\equiv \tilde{n}^{d_q} \pmod{q} && \text{with } d_q \equiv d \pmod{q-1} \end{aligned}$$

and subsequently use the Chinese Remainder Theorem (cf. Example I.2.34). For the efficient calculation of $\tilde{n}^d$, one also uses the binary representation of d. For example

$$\tilde{n}^{11} = \big((\tilde{n}^2)^2\tilde{n}\big)^2\tilde{n}.$$

This requires only five (instead of ten) multiplications.

Remark I.7.20. In contrast to $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^\times$ is generally not cyclic. For every odd $a \in \mathbb{Z}$, for example, $a^2 \equiv 1 \pmod{8}$. This shows $(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$.

Definition I.7.21. A (*ring*) *homomorphism* between rings R and S is a map $f\colon R \to S$ with $f(1_R) = 1_S$ and $f(a \dot{+} b) = f(a) \dot{+} f(b)$ for all $a, b \in R$. As usual, one defines mono-, epi-, endo-, iso- and automorphisms of rings. Furthermore, let $\operatorname{Ker}(f) := \{x \in R : f(x) = 0\}$.

Remark I.7.22.

(i) The property $f(1) = 1$ prevents the map $R \to S$, $a \mapsto 0$ from being a ring homomorphism.

(ii) Every ring homomorphism $f\colon R \to S$ is a group homomorphism $(R,+) \to (S,+)$. According to Lemma I.3.28, f is injective if and only if $\mathrm{Ker}(f) = \{0\}$. By restriction, one obtains a group homomorphism $(R^\times, \cdot) \to (S^\times, \cdot)$.

Example I.7.23.

(i) If R is a subring of S, then the inclusion $R \hookrightarrow S$ is a monomorphism.

(ii) For $I \trianglelefteq R$ there exists (as for groups) the *canonical* epimorphism $R \to R/I$, $a \mapsto a + I$.

Theorem I.7.24. *For coprime $n, m \in \mathbb{N}$ it holds that* $\boxed{(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times.}$

Proof. From the proof of Theorem I.3.34 we already know the group isomorphism

$$\begin{aligned} f\colon \mathbb{Z}/nm\mathbb{Z} &\to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}), \\ a + nm\mathbb{Z} &\mapsto (a + n\mathbb{Z}, a + m\mathbb{Z}). \end{aligned}$$

Apparently f is even a ring isomorphism and the claim follows from Example I.7.5(iv). □

Example I.7.25. It holds that $(\mathbb{Z}/12\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \cong C_2 \times C_2$.

Remark I.7.26. We will later determine the structure of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for $p \in \mathbb{P}$ (Theorem I.8.34).

Theorem I.7.27. *For $n \in \mathbb{N}$ it holds that* $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Let $\langle x \rangle \cong C_n$. For $\alpha \in \mathrm{Aut}(\langle x \rangle)$ we have $\alpha(x) = x^a$ with $a \in \mathbb{Z}$. Because of

$$n = |\langle \alpha(x) \rangle| = |\langle x^a \rangle| \overset{\text{I.3.7}}{=} \frac{n}{\gcd(n,a)}$$

we have $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$. One thus obtains a map

$$\begin{aligned} \Phi\colon \mathrm{Aut}(\langle x \rangle) &\to (\mathbb{Z}/n\mathbb{Z})^\times, \\ \alpha &\mapsto a + n\mathbb{Z}. \end{aligned}$$

For $\beta \in \mathrm{Aut}(\langle x \rangle)$ with $\beta(x) = x^b$ it holds that

$$(\alpha \circ \beta)(x) = \alpha(\beta(x)) = \alpha(x^b) = \alpha(x)^b = x^{ab}.$$

This shows that Φ is a homomorphism. If $a + n\mathbb{Z} = 1 + n\mathbb{Z}$, then $\alpha(x^i) = \alpha(x)^i = (x^a)^i = x^i$ for all $i \in \mathbb{Z}$, i. e. $\alpha = 1$. Thus Φ is injective. Conversely, if $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ is given, one easily sees that the map $x^i \mapsto x^{ia}$ defines an automorphism of $\langle x \rangle$. Therefore Φ is also surjective. □

Theorem I.7.28.

(i) (Homomorphism Theorem) For every ring homomorphism $f\colon R \to S$, $\mathrm{Ker}(f) \trianglelefteq R$ and $f(R)$ is a subring of S. Furthermore,

$$\boxed{R/\mathrm{Ker}(f) \cong f(R)}$$

is an isomorphism of rings.

(ii) (*1st Isomorphism Theorem*) *Let S be a subring of R and $I \trianglelefteq R$. Then $S + I$ is a subring of R, $I \trianglelefteq S + I$, $S \cap I \trianglelefteq S$ and*

$$\boxed{S/(S \cap I) \cong (S + I)/I.}$$

(iii) (*2nd Isomorphism Theorem*) *Let $I, J \trianglelefteq R$ with $I \subseteq J$. Then $J/I \trianglelefteq R/I$ and*

$$\boxed{(R/I)/(J/I) \cong R/J.}$$

Proof. We only show the Homomorphism Theorem (for the Isomorphism Theorems see Exercise I.38). It holds that $0 \in \operatorname{Ker}(f) \neq \varnothing$. For $a, b \in \operatorname{Ker}(f)$ and $x \in R$, we have $f(a-b) = f(a) - f(b) = 0 - 0 = 0$, $f(xa) = f(x)f(a) = f(x)0 = 0$ and $f(ax) = f(a)f(x) = 0f(x) = 0$. This shows $\operatorname{Ker}(f) \trianglelefteq R$. Analogously, $1_S = f(1_R) \in f(R)$ and for $f(a), f(b) \in f(R)$, we also have $f(a) - f(b) = f(a-b) \in f(R)$ as well as $f(a)f(b) = f(ab) \in f(R)$. Thus $f(R)$ is a subring of S. We now consider

$$\begin{aligned} F\colon R/\operatorname{Ker}(f) &\to f(R), \\ a + \operatorname{Ker}(f) &\mapsto f(a). \end{aligned}$$

For $a, b \in R$, it holds that

$$\begin{aligned} a + \operatorname{Ker}(f) = b + \operatorname{Ker}(f) &\iff a - b \in \operatorname{Ker}(f) \iff f(a) - f(b) = f(a-b) = 0 \\ &\iff f(a) = f(b) \iff F(a + \operatorname{Ker}(f)) = F(b + \operatorname{Ker}(f)). \end{aligned}$$

Thus F is well-defined and injective. By definition, F is also surjective. Because of $F(1 + \operatorname{Ker}(f)) = f(1) = 1$ and

$$\begin{aligned} F((a + \operatorname{Ker}(f)) \dot{+} (b + \operatorname{Ker}(f))) &= F(a \dot{+} b + \operatorname{Ker}(f)) = f(a \dot{+} b) = f(a) \dot{+} f(b) \\ &= F(a + \operatorname{Ker}(f)) \dot{+} F(b + \operatorname{Ker}(f)), \end{aligned}$$

for $a, b \in R$, F is a ring isomorphism. □

Remark I.7.29. In category theory, one generalizes the concepts of group, ring, field, vector space, ... and then only needs to prove the Homomorphism Theorem once for categories (chapter III.5).

Theorem I.7.30 (Chinese Remainder Theorem for Rings)**.** *Let R be a ring and $I_1, \ldots, I_n \trianglelefteq R$ with $I_i + I_j = R$ for $i \neq j$. Then*

$$\begin{aligned} R/(I_1 \cap \ldots \cap I_n) &\to R/I_1 \times \ldots \times R/I_n, \\ a + I_1 \cap \ldots \cap I_n &\mapsto (a + I_1, \ldots, a + I_n) \end{aligned}$$

is a ring isomorphism. If R is commutative, then additionally $I_1 \cap \ldots \cap I_n = I_1 \ldots I_n$ holds.

Proof. Clearly,

$$\begin{aligned} f\colon R &\to R/I_1 \times \ldots \times R/I_n, \\ a &\mapsto (a + I_1, \ldots, a + I_n) \end{aligned}$$

is a ring homorphism with kernel $I := I_1 \cap \ldots \cap I_n$. By the Homomorphism Theorem, we must show that f is surjective. Let $a_1, \ldots, a_n \in R$ be given. Let $1 \leq i \leq n$ be fixed. Because of $I_i + I_j = R$ for $j \neq i$, there exist $x_j \in I_i$ and $y_j \in I_j$ with $x_j + y_j = 1$. The ideal property shows

$$1 = \prod_{j \neq i} (x_j + y_j) = \tilde{x}_i + \prod_{j \neq i} y_j = \tilde{x}_i + \tilde{y}_i \in I_i + \bigcap_{j \neq i} I_j$$

for $i = 1, \ldots, n$. For $a := a_1\tilde{y}_1 + \ldots + a_n\tilde{y}_n$, it then holds that

$$a + I_i = a_i\tilde{y}_i + I_i = a_i\tilde{y}_i + a_i\tilde{x}_i + I_i = a_i(\tilde{x}_i + \tilde{y}_i) + I_i = a_i + I_i$$

for $i = 1, \ldots, n$. Thus $f(a) = (a_1 + I_1, \ldots, a_n + I_n)$ and f is surjective.

Now let R be commutative. If one multiplies out the product $R = \prod_{i \neq j}(I_i + I_j)$ over all pairs $i \neq j$, then in each summand at least $n - 1$ distinct I_i appear (namely, if I_k and I_l did not appear, then one would have no factor from $I_k + I_l$). From the commutativity of R it follows that

$$I_1 \ldots I_n \subseteq I_1 \cap \ldots \cap I_n = (I_1 \cap \ldots \cap I_n) \prod_{i \neq j} (I_i + I_j) \subseteq I_1 \ldots I_n. \qquad \square$$

Example I.7.31. Let $R = \mathbb{Z}$ and $I_i = (d_i)$ for $i = 1, \ldots, n$. The condition $I_i + I_j = R$ is then equivalent to $\gcd(d_i, d_j) = 1$ according to Corollary I.2.11. Furthermore,

$$I_1 \cap \ldots \cap I_n = I_1 \ldots I_n = (d_1 \ldots d_n) = (\operatorname{lcm}(d_1, \ldots, d_n)).$$

Theorem I.7.30 therefore implies a special case of the classical Chinese remainder theorem I.2.32.

Remark I.7.32. In analogy to groups, a ring $R \neq \{0\}$ is called *simple*, if $\{0\}$ and R are the only ideals of R. In Algebra II (or representation theory) it is shown under certain finiteness conditions that every simple ring is isomorphic to a matrix ring over a division ring (see Remark II.8.14).

I.8 Polynomials

Remark I.8.1. In the following, let K always be a field.

Definition I.8.2.

(i) A (formal) *polynomial* over K is an infinite sequence $\alpha = (a_0, a_1, \ldots) \in K^\infty$, in which only finitely many terms a_i are unequal to 0. We usually write α as a formal sum of the form $\alpha := \sum_{n=0}^{\infty} a_n X^n = \sum a_n X^n$, where X is an *indeterminate*. Here,

$$\sum a_n X^n = \sum b_n X^n \iff a_n = b_n \ \forall n \geq 0.$$

Individual powers of X are called *monomials*. The set of polynomials over K is denoted by $K[X]$.

(ii) By identifying $a \in K$ with the *constant* polynomial $(a, 0, 0, \ldots) = aX^0$, we can view K as a subset of $K[X]$. In particular, $0, 1 \in K[X]$.

(iii) The *degree* of $\alpha = \sum a_n X^n \in K[X]$ is $\deg \alpha := \sup\{n \geq 0 : a_n \neq 0\}$ with the convention $\deg 0 = \sup \varnothing = -\infty$.

(iv) One calls $\alpha = \sum a_n X^n \in K[X] \setminus \{0\}$ *monic*, if $a_{\deg \alpha} = 1$. In general, $a_{\deg \alpha}$ is called the *leading* coefficient and a_0 the *constant term* of α.

Example I.8.3.

(i) $X^2 + 1 \in \mathbb{R}[X]$.

(ii) It holds that $\deg(\alpha) = 0$ if and only if $\alpha \in K^\times$.

(iii) Every $\alpha \in K[X] \setminus \{0\}$ can be made *monic* by multiplication with $a_{\deg \alpha}^{-1}$.

Theorem I.8.4. *By*

$$\sum a_n X^n + \sum b_n X^n := \sum (a_n + b_n) X^n,$$
$$\sum a_n X^n \cdot \sum b_n X^n := \sum_n \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) X^n$$

$K[X]$ becomes a commutative ring with subring K.

Proof. Let $\alpha = \sum a_n X^n, \beta = \sum b_n X^n, \gamma = \sum c_n X^n \in K[X]$. Because of

$$\{n \in \mathbb{N}_0 : a_n + b_n \neq 0\} \subseteq \{n \in \mathbb{N}_0 : a_n \neq 0\} \cup \{n \in \mathbb{N}_0 : b_n \neq 0\}$$

it follows that $\alpha + \beta \in K[X]$. The axioms

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma), \qquad \alpha + \beta = \beta + \alpha, \qquad \alpha + 0 = \alpha$$

follow directly from the corresponding axioms of K. For $-\alpha := \sum(-a_n)X^n$, it certainly holds that $\alpha + (-\alpha) = 0$. Thus $K[X]$ is an abelian group with respect to $+$.

For $n > \deg(\alpha) + \deg(\beta)$, we have $\sum_{k=0}^{n} a_k b_{n-k} = 0$. Therefore $\alpha\beta \in K[X]$. The n-th coefficient of $\alpha(\beta\gamma)$ is

$$\sum_{i=0}^{n} a_i \sum_{j=0}^{n-i} b_j c_{n-i-j} = \sum_{i+j+k=n} a_i b_j c_k = \sum_{i=0}^{n} \Big(\sum_{j=0}^{i} a_j b_{i-j} \Big) c_{n-i}.$$

This shows $\alpha(\beta\gamma) = (\alpha\beta)\gamma$. Because of $\sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{n} b_k a_{n-k}$, we have $\alpha\beta = \beta\alpha$. The equation $\alpha \cdot 1 = \alpha$ is easy to see. The n-th coefficient of $\alpha(\beta + \gamma)$ is

$$\sum_{k=0}^{n} a_k (b_{n-k} + c_{n-k}) = \sum_{k=0}^{n} a_k b_{n-k} + \sum_{k=0}^{n} a_k c_{n-k}$$

and $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ follows. The addition and multiplication of constant polynomials corresponds exactly to the addition and multiplication in K. Thus K is a subring of $K[X]$. □

Remark I.8.5. Obviously $K[X]$ is also a K-vector space, where the scalar multiplication corresponds to the multiplication in $K[X]$. The X-powers $1, X, X^2, \ldots$ form a basis. In particular, $\dim K[X] = \infty$.

Lemma I.8.6. *For $\alpha, \beta \in K[X]$ the following hold:*

(i) $\deg(\alpha + \beta) \le \max\{\deg(\alpha), \deg(\beta)\}$,

(ii) $\deg \alpha < \deg \beta \Longrightarrow \deg(\alpha + \beta) = \deg \beta$,

(iii) $\deg(\alpha\beta) = \deg(\alpha) + \deg(\beta)$.

In particular, $K[X]$ is an integral domain.

Proof. We may assume $\alpha \neq 0 \neq \beta$. Let $\alpha = \sum a_n X^n$, $\beta = \sum b_n X^n$, $d := \deg \alpha$ and $e := \deg \beta$. Then $a_n + b_n = 0$ if $n > \max\{d, e\}$. This shows the first assertion. For $d < e$, we have $a_e + b_e = b_e \neq 0$ and the second assertion follows. The third assertion follows from

$$\alpha\beta = \sum_{n=0}^{d+e} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) X^n = \underbrace{a_d b_e}_{\neq 0} X^{d+e} + \sum_{n=0}^{d+e-1} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) X^n.$$

Now the last assertion follows:

$$\alpha\beta = 0 \Longrightarrow \deg(\alpha) + \deg(\beta) = \deg(\alpha\beta) = -\infty \Longrightarrow \alpha = 0 \vee \beta = 0.$$ □

Remark I.8.7.

(i) The proof also shows: If $\alpha, \beta \in K[X]$ are monic, then so is $\alpha\beta$.

(ii) According to Exercise I.40, one can consider $K[X]$ as a subring of its *field of fractions*

$$K(X) := Q(K[X]) = \Big\{ \frac{\alpha}{\beta} : \alpha, \beta \in K[X],\ \beta \neq 0 \Big\}.$$

One calls $K(X)$ the field of *rational functions* over K.

Corollary I.8.8. *It holds that $K[X]^\times = K^\times$.*

Proof. Certainly $K^\times \subseteq K[X]^\times$. Now let $\alpha, \beta \in K[X]^\times$ with $\alpha\beta = 1$. Then $\deg(\alpha) + \deg(\beta) = \deg(\alpha\beta) = \deg(1) = 0$ according to Lemma I.8.6. Because of $\deg(\alpha), \deg(\beta) \geq 0$, it follows that $\deg(\alpha) = \deg(\beta) = 0$ and $\alpha, \beta \in K^\times$. □

Definition I.8.9. For $\alpha = \sum a_n X^n, \beta \in K[X]$ let $\alpha(\beta) := \sum a_n \beta^n \in K[X]$ (*substitution*). One calls $x \in K$ a *root* of α if $\alpha(x) = 0$.

Theorem I.8.10. *For $x \in K$, the map $F_x \colon K[X] \to K$, $\alpha \mapsto \alpha(x)$ is a ring homomorphism, which is called the* evaluation homomorphism.

Proof. It holds that $F_x(1) = 1(x) = 1$. For $\alpha = \sum a_n X^n \in K[X]$ and $\beta = \sum b_n X^n \in K[X]$ we have

$$(\alpha + \beta)(x) = \sum (a_n + b_n) x^n = \sum a_n x^n + \sum b_n x^n = \alpha(x) + \beta(x).$$

Analogously,

$$(\alpha\beta)(x) = \Big(\sum_n \sum_{k=0}^{n} a_k b_{n-k} X^n\Big)(x) = \sum_n \sum_{k=0}^{n} a_k b_{n-k} x^n = \Big(\sum a_n x^n\Big)\Big(\sum b_n x^n\Big) = \alpha(x)\beta(x). \qquad \square$$

Remark I.8.11.

(i) The same proof shows $(\alpha + \beta)(\gamma) = \alpha(\gamma) + \beta(\gamma)$ and $(\alpha\beta)(\gamma) = \alpha(\gamma)\beta(\gamma)$ for $\alpha, \beta, \gamma \in K[X]$. On the other hand, in general $\alpha(\beta + \gamma) \neq \alpha(\beta) + \alpha(\gamma)$ and $\alpha(\beta\gamma) \neq \alpha(\beta)\alpha(\gamma)$.

(ii) For the efficient calculation of $\alpha(x)$ for $\alpha = a_n X^n + \ldots + a_1 X + a_0 \in K[X]$ and $x \in K$, one uses the HORNER scheme:

$$\big(\ldots\big((a_n x + a_{n-1})x + a_{n-2}\big)x + \ldots\big)x + a_0.$$

This requires only n (instead of $2n - 1$) multiplications. Income tax used to be calculated this way.

(iii) If K is finite, then different polynomials can induce the same map $K \to K$ by evaluation, because there are only finitely many such maps. Thus, one cannot equate polynomials with their functions as in analysis.

Example I.8.12. For $\alpha := X^2 + X \in \mathbb{F}_2[X]$, it holds that $\alpha(x) = 0$ for all $x \in \mathbb{F}_2$.

Definition I.8.13. As in $\mathbb{Z}$, we define the divisibility $\alpha \mid \beta$ for $\alpha, \beta \in K[X]$, if there exists a $\gamma \in K[X]$ with $\alpha\gamma = \beta$. More generally, let $\alpha \equiv \beta \pmod{\gamma}$, if $\gamma \mid (\alpha - \beta)$.

Remark I.8.14. As in $\mathbb{Z}$, one proves the usual calculation rules:

- $\pm 1 \mid \alpha \mid 0$,
- $0 \mid \alpha \iff \alpha = 0$,
- $\alpha \mid \beta \mid \gamma \Longrightarrow \alpha \mid \gamma$,
- $\alpha \mid \beta \mid \alpha \Longrightarrow \exists c \in K^\times : \alpha = c\beta$,
- $\alpha \mid \beta, \gamma \Longrightarrow \alpha \mid (\beta\delta + \gamma\psi)$,
- $\alpha \mid \beta \neq 0 \Longrightarrow \deg \alpha \leq \deg \beta$

for $\alpha, \beta, \gamma, \delta, \psi \in K[X]$.

Theorem I.8.15 (Euclidean division)**.** *For $\alpha \in K[X]$ and $\beta \in K[X] \setminus \{0\}$, there exist uniquely determined $\gamma, \delta \in K[X]$ with $\alpha = \beta\gamma + \delta$ and $\deg \delta < \deg \beta$.*

Proof. Choose $\gamma \in K[X]$ such that

$$\delta := \alpha - \beta\gamma = \sum a_n X^n$$

has the smallest possible degree $d \in \mathbb{N}_0 \cup \{-\infty\}$. Let $\beta = \sum b_n X^n$ and $e := \deg \beta$. If $d \geq e$ holds, then

$$\deg\big(\alpha - \beta(\gamma + a_d b_e^{-1} X^{d-e})\big) = \deg\big(\delta - a_d b_e^{-1} X^{d-e}\beta\big) < d$$

in contradiction to the choice of γ. Thus $d < e$ and $\alpha = \beta\gamma + \delta$.

Now let $\alpha = \beta\tilde{\gamma} + \tilde{\delta}$ with $\deg \tilde{\delta} < e$. According to Lemma I.8.6,

$$e + \deg(\tilde{\gamma} - \gamma) = \deg\big(\beta(\tilde{\gamma} - \gamma)\big) = \deg(\delta - \tilde{\delta}) \leq \max\{\deg(\delta), \deg(\tilde{\delta})\} < e$$

and it follows that $(\tilde{\gamma}, \tilde{\delta}) = (\gamma, \delta)$. □

Definition I.8.16. For $\alpha_1, \ldots, \alpha_n \in K[X]$, let (as in $\mathbb{Z}$) $\mathrm{cd}(\alpha_1, \ldots, \alpha_n)$ be the set of common divisors of $\alpha_1, \ldots, \alpha_n$. A monic $\alpha \in \mathrm{cd}(\alpha_1, \ldots, \alpha_n)$ (or $\alpha = 0$) is called the *greatest common divisor* of $\alpha_1, \ldots, \alpha_n$, if $\beta \mid \alpha$ holds for all $\beta \in \mathrm{cd}(\alpha_1, \ldots, \alpha_n)$.

Remark I.8.17. If α, β are greatest common divisors of $\alpha_1, \ldots, \alpha_n$, then $\alpha \mid \beta \mid \alpha$ holds. According to Remark I.8.14, there exists $c \in K^\times$ with $\alpha = c\beta$. Since α and β are monic (or 0), $\alpha = \beta$ holds. Thus there is at most one greatest common divisor and we write (as in $\mathbb{Z}$) $\gcd(\alpha_1, \ldots, \alpha_n) := \alpha$. The following theorem shows the existence of the gcd.

Theorem I.8.18 (Extended Euclidean algorithm in $K[X]$)**.**
Input: $\alpha, \beta \in K[X] \setminus \{0\}$.
Initialization: $(\sigma_0, \tau_0, \rho_0) := (1, 0, \alpha)$, $(\sigma_1, \tau_1, \rho_1) := (0, 1, \beta)$ *and* $k := 0$.
While $\rho_{k+1} \neq 0$ *repeat:*
  Euclidean division: $\rho_k = \lambda_{k+1}\rho_{k+1} + \epsilon_{k+1}$ *with* $\deg(\epsilon_{k+1}) < \deg(\rho_{k+1})$.
  Set $(\sigma_{k+2}, \tau_{k+2}, \rho_{k+2}) := (\sigma_k - \sigma_{k+1}\lambda_{k+1}, \tau_k - \tau_{k+1}\lambda_{k+1}, \epsilon_{k+1})$ *and* $k := k + 1$.
Choose $a \in K$ *such that* $a\rho_k$ *is monic.*
Output: $a\rho_k = a\sigma_k\alpha + a\tau_k\beta = \gcd(\alpha, \beta)$.

Proof. As in $\mathbb{Z}$ (see also Linear Algebra 2). □

Example I.8.19. Let $\alpha = X^3 + 2X - 1$ and $\beta = X^2 - X + 4$ in $\mathbb{Q}[X]$. Polynomial division yields $\alpha = \beta(X + 1) - X - 5$ and $\beta = (X + 5)(X - 6) + 34$. Thus

σ_i	τ_i	ρ_i	λ_i
1	0	α	
0	1	β	$X + 1$
1	$-X - 1$	$-X - 5$	$-X + 6$
$X - 6$	$-X^2 + 5X + 7$	$\boxed{34}$	
		0	

Normalization yields $\gcd(\alpha, \beta) = 1 = \frac{1}{34}(X - 6)\alpha - \frac{1}{34}(X^2 - 5X - 7)\beta$.

Definition I.8.20. Polynomials $\alpha_1, \ldots, \alpha_n \in K[X]$ are called *coprime*, if $\gcd(\alpha_1, \ldots, \alpha_n) = 1$.

Corollary I.8.21. *$\alpha, \beta \in K[X]$ are coprime if and only if there exist $\tilde{\alpha}, \tilde{\beta} \in K[X]$ with $\alpha\tilde{\alpha} + \beta\tilde{\beta} = 1$.*

Proof. If $\gcd(\alpha, \beta) = 1$, then the existence of $\tilde{\alpha}$ and $\tilde{\beta}$ follows from Theorem I.8.18. Conversely, if $\alpha\tilde{\alpha} + \beta\tilde{\beta} = 1$, then $\gcd(\alpha, \beta) \mid (\alpha\tilde{\alpha} + \beta\tilde{\beta}) = 1$ and $\gcd(\alpha, \beta) = 1$. □

Definition I.8.22. A monic polynomial $\alpha \in K[X] \setminus K$ is called *irreducible*, if it cannot be written in the form $\alpha = \beta\gamma$ with $\beta, \gamma \in K[X] \setminus K$ (i. e. α has exactly two monic divisors, namely 1 and α, cf. prime number). Otherwise, α is called *reducible*.

Example I.8.23.

(i) Monic polynomials of degree 1 are always irreducible. We will show later that every irreducible polynomial in $\mathbb{C}[X]$ has degree 1 (Fundamental Theorem of Algebra).

(ii) $X^2 - 2$ is irreducible in $\mathbb{Q}[X]$, but not in $\mathbb{R}[X]$, because $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2}) \in \mathbb{R}[X]$ and $\sqrt{2} \notin \mathbb{Q}$.

(iii) $X^2 + 1$ is irreducible in $\mathbb{R}[X]$, but not in $\mathbb{C}[X]$, because $X^2 + 1 = (X - \mathrm{i})(X + \mathrm{i}) \in \mathbb{C}[X]$.

(iv) $X^2 + X + 1$ is irreducible in $\mathbb{F}_2[X]$, because $X^2 + X + 1 \notin \{X^2, X(X+1) = X^2 + X, (X+1)^2 = X^2 + 1\}$.

Theorem I.8.24 (Prime factorization in $K[X]$)**.** *For every polynomial $\alpha \in K[X] \setminus \{0\}$, there exist irreducible polynomials $\sigma_1, \ldots, \sigma_n \in K[X]$, unique up to their order, and a uniquely determined constant $c \in K^\times$ such that $\alpha = c\sigma_1 \ldots \sigma_n$.*

Proof.
Existence: Because of $\alpha \neq 0$, there exists $c \in K^\times$ such that $c^{-1}\alpha$ is monic. We can therefore assume that α is monic. Induction on $d := \deg \alpha$: In the case $d = 0$, $\alpha = 1$ and we choose $n = 0$ (empty product). If α is irreducible (for example $d = 1$), then we are also finished. Otherwise, $\alpha = \beta\gamma$ with $\beta, \gamma \in K[X] \setminus K$. Because of $d = \deg(\beta\gamma) = \deg(\beta) + \deg(\gamma)$, we have $\deg \beta, \deg \gamma < d$. By induction, β and γ are products of irreducible polynomials and constants, and therefore so is α.

Uniqueness: Obviously, c is uniquely determined as the leading coefficient of α. We can therefore again assume that α is monic. Let $\alpha = \sigma_1 \ldots \sigma_n = \tau_1 \ldots \tau_m$ with irreducible $\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m \in K[X]$. Induction on m: In the case $m = 1$, $n = 1$ and $\sigma_1 = \alpha = \tau_1$. Now let $m \geq 2$. In the case $\sigma_1 = \tau_1$, we have $\sigma_2 \ldots \sigma_n = \tau_2 \ldots \tau_m$ and induction yields the claim. Now let $\sigma_1 \neq \tau_1$. Then there exist $\tilde{\sigma}, \tilde{\tau} \in K[X]$ with $\sigma_1\tilde{\sigma} + \tau_1\tilde{\tau} = 1$ according to Corollary I.8.21. It follows

$$\sigma_1(\tilde{\sigma}\tau_2 \ldots \tau_m + \sigma_2 \ldots \sigma_n\tilde{\tau}) = \sigma_1\tilde{\sigma}\tau_2 \ldots \tau_m + \tau_1 \ldots \tau_m\tilde{\tau} = (\sigma_1\tilde{\sigma} + \tau_1\tilde{\tau})(\tau_2 \ldots \tau_m) = \tau_2 \ldots \tau_m.$$

Inductively, one obtains $\sigma_1 = \tau_i$ for some $i \in \{1, \ldots, m\}$. Then $\sigma_2 \ldots \sigma_n = \tau_1 \ldots \tau_{i-1}\tau_{i+1} \ldots \tau_m$ and induction yields the claim. □

Example I.8.25. In $\mathbb{F}_2$, $X^4 - X = X(X+1)(X^2 + X + 1)$ is the prime factorization of $X^4 - X$.

Remark I.8.26. Rings that allow a unique prime factorization are called *factorial* (Definition II.5.11). In algebraic number theory, one goes a step further and investigates rings in which ideals can be uniquely decomposed (Theorem II.11.29). This is relevant for the proof of *Fermat's Last Theorem* ($x^n + y^n = z^n$ has no solution $(x, y, z) \in \mathbb{N}^3$ for $n \geq 3$).

Lemma I.8.27. *If $x \in K$ is a root of $\alpha \in K[X]$, then $X - x$ is a divisor of α.*

Proof. Euclidean division yields $\alpha = (X - x)\beta + r$ with $\beta \in K[X]$ and $r \in K$. Then $r = \alpha(x) = 0$. □

Definition I.8.28. In the situation of Lemma I.8.27, $X - x$ is a *linear factor* of α. The largest natural number m with $(X - x)^m \mid \alpha$ is called the *multiplicity* of the root. In the case $m = 1$, x is a *simple* root and otherwise a *multiple* root.

Theorem I.8.29. *Every $\alpha \in K[X] \setminus \{0\}$ has at most $\deg \alpha$ roots in K (with multiplicities).*

Proof. Induction on $d := \deg \alpha$. In the case $d = 0$, α is constant and therefore has no root. Now let $d > 0$ and $x \in K$ be a root of α with multiplicity m. Then $\alpha = (X - x)^m \beta$ for some $\beta \in K[X]$ with $\deg \beta = d - m < d$. For every further root $y \neq x$ of α, it holds that $0 = \alpha(y) = (y - x)^m \beta(y) = \beta(y)$. Thus y is also a root of β. By induction, β possesses at most $d - m$ roots. In total, α thus has at most $m + d - m = d$ roots. □

Example I.8.30 (Interpolation)**.** Given coordinates $(x_1, y_1), \ldots, (x_n, y_n) \in K^2$ with pairwise distinct $x_1, \ldots, x_n$, the LAGRANGE polynomial

$$\alpha := \sum_{i=1}^{n} y_i \prod_{j \neq i} \frac{X - x_j}{x_i - x_j} \in K[X]$$

of degree $< n$ passes exactly through the points $(x_1, y_1), \ldots, (x_n, y_n)$. If $\beta \in K[X]$ is also a polynomial with $\deg \beta < n$ and $\beta(x_i) = y_i$ for $i = 1, \ldots, n$, then $x_1, \ldots, x_n$ are roots of $\alpha - \beta$ with $\deg(\alpha - \beta) < n$. Theorem I.8.29 shows $\alpha = \beta$, i. e. α is the unique polynomial of degree $< n$ that interpolates the given points.

Theorem I.8.31. *Every finite subgroup of $K^\times$ is cyclic.*

Proof. Let $G \leq K^\times$ be finite. As an abelian group, G is the direct sum of its Sylow subgroups (Example I.5.6). According to Lemma I.5.3 and Theorem I.3.34, it suffices to show that the Sylow subgroups of G are cyclic. So let $|G| = p^n$ with $p \in \mathbb{P}$ and wlog. $n \geq 1$. According to Theorem I.8.29, the polynomial $X^{p^{n-1}} - 1 \in K[X]$ has at most $p^{n-1} < |G|$ roots. Thus there exists a $g \in G$ with $g^{p^{n-1}} \neq 1$. On the other hand, by Lagrange, $|\langle g \rangle|$ is a divisor of p^n. This shows $G = \langle g \rangle$. □

Remark I.8.32. In particular, $\mathbb{F}_p^\times$ is cyclic for $p \in \mathbb{P}$. One calls $x \in \mathbb{F}_p$ with $\mathbb{F}_p^\times = \langle x \rangle$ a *primitive root* modulo p. No formula is known to calculate primitive roots for a given p, but usually one finds "small" primitive roots[1]. According to Lemma I.3.7, the number of primitive roots is $\varphi(p - 1)$. For $y \in \mathbb{F}_p^\times = \langle x \rangle$, no fast algorithm is known for calculating $k \in \mathbb{Z}$ with $y = x^k$ (discrete logarithm). This circumstance is exploited in cryptography (Example I.2.25).

[1] See `https://oeis.org/A001918`

Example I.8.33. We are looking for a primitive root modulo 7. Every $x \in \mathbb{F}_7^\times$ has order $1, 2, 3$ or $\varphi(7) = 6$ according to Lagrange. Because of $2^3 \equiv 1 \pmod 7$, 2 is not a primitive root modulo 7. Because of $3^2 \equiv 2 \pmod 7$ and $3^3 \equiv 2 \cdot 3 \equiv -1 \pmod 7$, 3 is a primitive root modulo 7.

Theorem I.8.34 (Gauss)**.** *For $p \in \mathbb{P}$ and $n \in \mathbb{N}$ it holds that*

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \begin{cases} C_2 \times C_{2^{n-2}} & \text{if } p = 2 \leq n, \\ C_{p^{n-1}(p-1)} & \text{otherwise.} \end{cases}$$

Proof. Let $G := (\mathbb{Z}/p^n\mathbb{Z})^\times$. First let $p > 2$. Because of $|G| = \varphi(p^n) = p^{n-1}(p-1)$, it suffices to show that G is cyclic. For $n = 1$, the claim follows from Theorem I.8.31. Now let $n \geq 2$. The canonical map $\Psi\colon G \to (\mathbb{Z}/p\mathbb{Z})^\times$, $a + p^n\mathbb{Z} \mapsto a + p\mathbb{Z}$ is obviously a well-defined epimorphism. According to the homomorphism theorem, $P := \operatorname{Ker}(\Psi) \in \operatorname{Syl}_p(G)$ and $G/P \cong C_{p-1}$. According to the fundamental theorem of finite abelian groups, it suffices to show that P is cyclic. We show more precisely that P is generated by $1 + p + p^n\mathbb{Z} \in P$. For this, one calculates

$$(1+p)^{p^{n-2}} = \sum_{k=0}^{p^{n-2}} \binom{p^{n-2}}{k} p^k \equiv 1 + p^{n-1} \not\equiv 1 \pmod{p^n}.$$

Now let $p = 2$ and wlog. $n \geq 2$. Then $|G| = 2^{n-1}$. Because of $(-1 + 2^n\mathbb{Z})^2 = 1 + 2^n\mathbb{Z}$, it suffices to show

$$G = \langle -1 + 2^n\mathbb{Z} \rangle \oplus \langle 5 + 2^n\mathbb{Z} \rangle.$$

The case $n = 2$ is clear. So let $n \geq 3$. One calculates

$$5^{2^{n-3}} = (1+4)^{2^{n-3}} = \sum_{k=0}^{2^{n-3}} \binom{2^{n-3}}{k} 2^{2k} \equiv 1 + 2^{n-1} \pmod{2^n}.$$

and

$$5^{2^{n-2}} \equiv (1 + 2^{n-1})^2 \equiv 1 \pmod{2^n}.$$

Thus $|\langle 5 + 2^n\mathbb{Z} \rangle| = 2^{n-2}$. Because of $-1 \not\equiv 1 + 2^{n-1} \pmod{2^n}$, it is also $\langle -1 + 2^n\mathbb{Z} \rangle \cap \langle 5 + 2^n\mathbb{Z} \rangle = 1$. □

Corollary I.8.35. *$(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n \in \{4, p^m, 2p^m\}$ for an odd prime p and $m \in \mathbb{N}_0$.*

Proof. If n has several odd prime divisors, then $C_2 \times C_2$ is a subgroup of $G := (\mathbb{Z}/n\mathbb{Z})^\times$ by Theorem I.7.24 and Theorem I.5.12. Then G cannot be cyclic (Theorem I.3.34). Likewise, n cannot be divisible by 4 and an odd prime at the same time. According to Theorem I.8.34, n also cannot be divisible by 8. Because of $(\mathbb{Z}/2p^m\mathbb{Z})^\times \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$, G is always cyclic in the specified cases. □

Remark I.8.36. For $\alpha \in K[X]$, one can form the principal ideal $(\alpha) = K[X]\alpha$, so that $K[X]/(\alpha)$ becomes a ring (Theorem I.7.10). It then holds that

$$\beta + (\alpha) = \gamma + (\alpha) \iff \beta - \gamma \in (\alpha) \iff \alpha \mid (\beta - \gamma) \iff \beta \equiv \gamma \pmod{\alpha}$$

(cf. $\mathbb{Z}/n\mathbb{Z}$).

Lemma I.8.37. *Every ideal of $K[X]$ is a principal ideal. In this case, $(\alpha) \subseteq (\beta) \iff \beta \mid \alpha$ holds.*

Proof. Let $(0) \neq I \trianglelefteq K[X]$ and $\alpha \in I \setminus \{0\}$ with minimal degree $d \geq 0$. For $\beta \in I$, there exist $\gamma, \delta \in K[X]$ with $\beta = \alpha\gamma + \delta$ and $\deg \delta < d$. Because of $\delta = \beta - \alpha\gamma \in I$, it follows that $\delta = 0$ and $\beta = \alpha\gamma \in (\alpha)$. This shows $I = (\alpha)$. The second statement follows easily. □

Theorem I.8.38. *$\alpha \in K[X]$ is irreducible if and only if $K[X]/(\alpha)$ is a field.*

Proof. The claim follows from Theorem I.7.12 and Lemma I.8.37. □

Example I.8.39. We already know that $\alpha = X^2 - 2 \in \mathbb{Q}[X]$ is irreducible. Thus $X + (\alpha)$ is invertible in the field $\mathbb{Q}[X]/(\alpha)$. The Euclidean algorithm yields

$$1 = \gcd(X, \alpha) = \frac{1}{2}X^2 - \frac{1}{2}\alpha \equiv \frac{1}{2}X^2 \pmod{\alpha}.$$

Therefore $(X + (\alpha))^{-1} = \frac{1}{2}X + (\alpha)$.

Definition I.8.40. A ring homomorphism between fields is called a *(field)homomorphism*.

Lemma I.8.41. *Every field homomorphism is injective.*

Proof. Let $\sigma\colon K \to L$ be a field homomorphism and $x \in \operatorname{Ker}(\sigma)$. In the case $x \neq 0$, it would be $1 = \sigma(1) = \sigma(xx^{-1}) = \sigma(x)\sigma(x^{-1}) = 0$. Thus $\operatorname{Ker}(\sigma) = \{0\}$ and the claim follows from Remark I.7.22. □

Remark I.8.42.

(i) $\sigma\colon K \to L$ is a field homomorphism if and only if $\sigma\colon (K, +) \to (L, +)$ and $\sigma\colon (K^\times, \cdot) \to (L^\times, \cdot)$ are group monomorphisms.

(ii) The isomorphisms $K \to K$ are called *automorphisms*. They form the automorphism group $\operatorname{Aut}(K)$ with respect to composition.

Example I.8.43.

(i) Let $\sigma \in \operatorname{Aut}(\mathbb{F}_p)$ for $p \in \mathbb{P}$. Then $\sigma(1) = 1$, $\sigma(1+1) = \sigma(1) + \sigma(1) = 1 + 1$, etc. This shows $\sigma = \mathrm{id}$ and $\operatorname{Aut}(\mathbb{F}_p) = \{\mathrm{id}\} = 1$.

(ii) According to Exercise I.53, $\operatorname{Aut}(\mathbb{Q}) = 1$ and $\operatorname{Aut}(\mathbb{R}) = 1$.

(iii) The complex conjugation is a field automorphism on $\mathbb{C}$. Using the axiom of choice, one can show that $\operatorname{Aut}(\mathbb{C})$ is uncountable (Theorem II.4.22).

Lemma I.8.44. *Every field homomorphism $\sigma\colon K \to L$ can be extended to a ring homomorphism*

$$\begin{aligned} K[X] &\to L[X], \\ \sum a_n X^n &\mapsto \sum \sigma(a_n) X^n \end{aligned}$$

which we also denote by σ. For $\alpha \in K[X]$ and $x \in K$, it holds that

$$\boxed{\sigma(\alpha(x)) = \sigma(\alpha)(\sigma(x)).}$$

Proof. Certainly $\sigma(1) = 1$. For $\alpha = \sum a_n X^n, \beta = \sum b_n X^n$ it holds that

$$\begin{aligned}\sigma(\alpha+\beta) &= \sum \sigma(a_n + b_n)X^n = \sum \sigma(a_n)X^n + \sum \sigma(b_n)X^n = \sigma(\alpha) + \sigma(\beta),\\ \sigma(\alpha\beta) &= \sum_n \sigma\Big(\sum_{k=0}^{n} a_k b_{n-k}\Big)X^n = \sum_n \Big(\sum_{k=0}^{n} \sigma(a_k)\sigma(b_{n-k})\Big)X^n\\ &= \sum \sigma(a_n)X^n \cdot \sum \sigma(b_n)X^n = \sigma(\alpha)\sigma(\beta).\end{aligned}$$

Thus $\sigma\colon K[X] \to L[X]$ is a ring homomorphism. The second statement follows with

$$\sigma(\alpha(x)) = \sigma\Big(\sum a_n x^n\Big) = \sum \sigma(a_n)\sigma(x)^n = \sigma(\alpha)(\sigma(x)).$$ □

Remark I.8.45. The polynomials with integer coefficients form the subring $\mathbb{Z}[X]$ of $\mathbb{Q}[X]$. Note: In $\mathbb{Z}[X]$ there is no Euclidean division! We prove three irreducibility criteria with the help of $\mathbb{Z}[X]$.

Definition I.8.46. One calls $\sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ *primitive*, if $\gcd(a_0, \ldots, a_n) = 1$.

Example I.8.47. Monic polynomials are primitive.

Lemma I.8.48 (Gauss)**.** *If $\alpha, \beta \in \mathbb{Z}[X]$ are primitive, then so is $\alpha\beta$.*

Proof. Let $\alpha = \sum a_n X^n$ and $\beta = \sum b_n X^n$. Assume indirectly that $p \in \mathbb{P}$ divides all coefficients of $\alpha\beta$. Since α and β are primitive, there exist minimal numbers $s, t \in \mathbb{N}_0$ with $p \nmid a_s$ and $p \nmid b_t$. For the coefficient of X^{s+t} in $\alpha\beta$, we then obtain the contradiction

$$\sum_{k=0}^{s+t} a_k b_{s+t-k} \equiv a_s b_t \not\equiv 0 \pmod{p}.$$ □

Remark I.8.49. To (naively) check whether $\alpha \in \mathbb{Q}[X]$ is irreducible, one would have to perform trial divisions by infinitely many rational polynomials of smaller degree. With Gauss' Lemma, one only needs to test finitely many factors. For example, let $\beta, \gamma \in \mathbb{Q}[X] \setminus \mathbb{Q}$ with $\alpha = \beta\gamma$. Then there exist $b, c \in \mathbb{Q}$ such that $b\beta \in \mathbb{Z}[X]$ and $c\gamma \in \mathbb{Z}[X]$ are primitive. According to Gauss, $bc\alpha = b\beta c\gamma \in \mathbb{Z}[X]$ is also primitive. Obviously, $bc\alpha$ is uniquely determined by α up to sign. The possibilities for $b\beta$ and $c\gamma$ result from comparing coefficients. However, the procedure is laborious.

Example I.8.50. If $\alpha = X^3 - \frac{1}{2}X^2 + 1 \in \mathbb{Q}[X]$ is reducible, then there exist $a, b, c, d, e \in \mathbb{Z}$ with

$$2\alpha = 2X^3 - X^2 + 2 = (aX + b)(cX^2 + dX + e).$$

Wlog. let $a, c \in \mathbb{N}$. Comparing coefficients yields

$$ac = 2, \qquad ad + bc = -1, \qquad ae + bd = 0, \qquad be = 2.$$

In the case $a = 1$, one obtains $c = 2$, $-1 = d + 2b \equiv d \pmod 2$ and $0 = e + bd \equiv e + b \pmod 2$. Thus $b \equiv e \pmod 2$ in contradiction to $be = 2$. Now let $a = 2$. Then $c = 1$, $-1 = 2d + b \equiv b \pmod 2$ and $0 = 2e + bd \equiv d \pmod 2$. It follows that $-1 = 2d + b \equiv b \pmod 4$. Because of $be = 2$, it follows that $b = -1$, $e = -2$ and $d = 0$. This contradicts $0 = 2e + bd$. Conclusion: α is irreducible.

Corollary I.8.51. *Let $\alpha \in \mathbb{Z}[X]$ and $\alpha = \beta\gamma$ with monic $\beta, \gamma \in \mathbb{Q}[X]$. Then $\beta, \gamma \in \mathbb{Z}[X]$. Every rational root of α is an integer and divides the constant term of α.*

Proof. Let $b, c \in \mathbb{Q}$ such that $b\beta, c\gamma \in \mathbb{Z}[X]$ are primitive. Since β and γ are monic, it follows that $b, c \in \mathbb{Z}$, wlog. $b, c \in \mathbb{N}$. According to Gauss, $bc\alpha$ is primitive. However, because $\alpha \in \mathbb{Z}[X]$, every coefficient of $bc\alpha$ is divisible by bc. This shows $bc = 1$ and $b = c = 1$, i.e., $\beta, \gamma \in \mathbb{Z}[X]$. Now let $x \in \mathbb{Q}$ be a root of α. According to Lemma I.8.27, there exists a monic $\beta = \sum b_n X^n \in \mathbb{Q}[X]$ with $\alpha = (X - x)\beta$. The first part of the proof shows $x, b_0 \in \mathbb{Z}$. Furthermore, $x \mid (-x)b_0 = a_0$, where a_0 is the constant term of α. □

Example I.8.52.

(i) If $\alpha = X^3 - 2X^2 + X - 1 \in \mathbb{Q}[X]$ is reducible, then there exists a root $x \in \mathbb{Q}$. Corollary I.8.51 shows $x = \pm 1$. Because of $\alpha(1) = -1 \neq 0 \neq -5 = \alpha(-1)$, this is excluded. Thus α is irreducible.

(ii) Is $x := \sqrt{2} + \sqrt[3]{3} \in \mathbb{R}$ rational? It holds that

$$3 = (x - \sqrt{2})^3 = x^3 - 3\sqrt{2}x^2 + 3 \cdot 2x - 2\sqrt{2} = x^3 + 6x - \sqrt{2}(3x^2 + 2)$$

and

$$18x^4 + 24x^2 + 8 = 2(3x^2 + 2)^2 = (x^3 + 6x - 3)^2 = x^6 + 12x^4 - 6x^3 + 36x^2 - 36x + 9.$$

Thus x is a root of $X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1$. Because of $x > 1$, x cannot be rational according to Corollary I.8.51.

Remark I.8.53. The (complex) roots of integer monic polynomials are called *algebraic integers*. According to Corollary I.8.51, every rational algebraic integer is an integer. In Algebra II, it is shown that the algebraic integers form a subring of $\mathbb{C}$ (Theorem II.11.8).

Lemma I.8.54 (Eisenstein Criterion[2])**.** *Let $\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$ with $p \mid a_0, \ldots, p \mid a_{n-1}$ and $p^2 \nmid a_0$ for some $p \in \mathbb{P}$. Then α is irreducible in $\mathbb{Q}[X]$.*

Proof. Suppose indirectly $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathbb{Q}[X] \setminus \mathbb{Q}$. We can assume that β and γ are monic. According to Corollary I.8.51, $\beta = \sum b_i X^i \in \mathbb{Z}[X]$ and $\gamma = \sum c_i X^i \in \mathbb{Z}[X]$. Because of $p \mid a_0 = b_0 c_0$ and $p^2 \nmid a_0$, we can assume wlog. $p \mid b_0$ and $p \nmid c_0$. Let $k < n$ be minimal with $p \nmid b_k$ (exists, since β is monic). Then we obtain the contradiction

$$0 \equiv a_k = \sum_{i=0}^{k} b_i c_{k-i} \equiv b_k c_0 \not\equiv 0 \pmod{p}.$$ □

Example I.8.55. Let $p \in \mathbb{P}$ and $\alpha = X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Q}[X]$. Obviously, α is irreducible if and only if $\beta := \alpha(X + 1)$ is irreducible (Definition I.8.9). Because of $(X - 1)\alpha = X^p - 1$ (geometric series), we have

$$X\beta = (X + 1)^p - 1 = \sum_{k=1}^{p} \binom{p}{k} X^k$$

[2] first discovered by Schönemann, see [D. A. Cox, *Why Eisenstein Proved the Eisenstein Criterion and Why Schönemann Discovered It First*, Amer. Math. Monthly 118 (2011), 3–21]

and

$$\beta = X^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} X^{k-1}.$$

For $1 \leq k \leq p-1$, we have $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{1\cdot 2\cdot \ldots \cdot k} \equiv 0 \pmod{p}$ and $\binom{p}{1} = p \not\equiv 0 \pmod{p^2}$. By Eisenstein, β is irreducible and thus so is α.

Lemma I.8.56 (Reduction modulo p)**.** *Let $\alpha = \sum a_n X^n \in \mathbb{Z}[X]$ be monic and reducible in $\mathbb{Q}[X]$. Then $\overline{\alpha} := \sum (a_n + p\mathbb{Z}) X^n$ is reducible in $\mathbb{F}_p[X]$ for all $p \in \mathbb{P}$.*

Proof. According to Corollary I.8.51, there exist monic $\beta, \gamma \in \mathbb{Z}[X] \setminus \mathbb{Z}$ with $\alpha = \beta\gamma$. As in Lemma I.8.44, the canonical ring homomorphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ can be extended to $f\colon \mathbb{Z}[X] \to \mathbb{F}_p[X]$. In this case, $\overline{\alpha} = f(\alpha) = f(\beta)f(\gamma)$ with $f(\beta), f(\gamma) \in \mathbb{F}_p[X] \setminus \mathbb{F}_p$. □

Example I.8.57. Since $\alpha := X^3 + X + 1 \in \mathbb{F}_2[X]$ has no root in $\mathbb{F}_2$, α is irreducible. Therefore, $\beta := X^3 + 2X^2 - 7X + 333 \in \mathbb{Q}[X]$ is also irreducible, because $\overline{\beta} = \alpha$. Caution: The converse is false. For example, $X^2 + 1$ is irreducible in $\mathbb{Q}[X]$, but not in $\mathbb{F}_2[X]$.

I.9 Field Extensions

Definition I.9.1.

(i) A *subfield* of a field L is a subset $K \subseteq L$ that forms a field itself with the restricted operations $+$ and $\cdot$. One then calls $K \subseteq L$ a *field extension*.

(ii) For every field extension $K \subseteq L$, L is a K-vector space, where the scalar multiplication is the multiplication in L. One calls $|L : K| := \dim_K L$ the *degree* of L over K. In the case $|L : K| < \infty$, the field extension is called *finite* (nevertheless, K can then be infinite).[1]

(iii) If $x \in L$ is a root of a polynomial $\mu \in K[X] \setminus K \subseteq L[X]$, then x is called *algebraic* (over K). If every $x \in L$ is algebraic over K, then the field extension $K \subseteq L$ is called *algebraic*. If $x \in L$ is not algebraic, then x is called *transcendental* (over K).

(iv) If $K \subseteq L$ and $K \subseteq M$ are field extensions and $\sigma\colon L \to M$ is an isomorphism with $\sigma_K = \mathrm{id}_K$ (restriction), then σ is called a *K-isomorphism*.

Example I.9.2.

(i) $\mathbb{Q} \subseteq \mathbb{R}$ is an infinite field extension, because $\mathbb{Q}$ is countable and $\mathbb{R}$ is uncountable.

(ii) $\mathbb{R} \subseteq \mathbb{C}$ is a field extension of degree 2 with basis $1, \mathrm{i}$.

(iii) Every intersection of subfields is again a subfield (verify). For a field extension $K \subseteq L$ and a subset $S \subseteq L$, let $K(S)$ be the intersection of all subfields of L that contain K and S. One says $K(S)$ is formed by *adjunction* of S to K. We also write $K(x_1, \ldots, x_n) := K(\{x_1, \ldots, x_n\})$.

(iv) Every $x \in K$ is algebraic over K as a root of $X - x$.

(v) $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ as a root of $X^2 - 2$.

(vi) Let $x := a + b\mathrm{i} \in \mathbb{C}$ with $a, b \in \mathbb{R}$. Then x is algebraic over $\mathbb{R}$ as a root of $(X - a)^2 + b^2 \in \mathbb{R}[X]$. Therefore $\mathbb{R} \subseteq \mathbb{C}$ is algebraic.

(vii) Since $\mathbb{Q}$ is countable, $\mathbb{Q}[X]$ is also countable. According to Theorem I.8.29, every $\alpha \in \mathbb{Q}[X] \setminus \{0\}$ has only finitely many roots. Thus, there are only countably many algebraic numbers over $\mathbb{Q}$ in $\mathbb{R}$. "Almost all" real numbers are therefore transcendental, but their explicit construction is difficult (Theorem I.13.12).

Remark I.9.3.

(i) Let $K \subseteq L$ be a field extension and $x \in L$ algebraic over K. Then the evaluation homomorphism $F_x\colon K[X] \to L$, $\alpha \mapsto \alpha(x)$ (Theorem I.8.10) has a non-trivial kernel. According to Lemma I.8.37, there exists exactly one monic polynomial $\mu_x \in K[X]$ with $\mathrm{Ker}(F_x) = (\mu_x)$. For every $\alpha \in K[X]$ with root x, it then holds that $\mu_x \mid \alpha$. In particular, $\deg \mu_x$ is minimal among all polynomials $\alpha \neq 0$ with root x. Therefore, μ_x is irreducible. One calls μ_x the *minimal polynomial* of x (over K).

[1] Attention: $|L : K|$ is *not* the index of $(K, +)$ in $(L, +)$!

(ii) With the notation from (i), the map $t_x\colon L \to L$, $a \mapsto xa$ is K-linear and μ_x is the minimal polynomial of t_x from linear algebra 2.

(iii) For subsets $S, T \subseteq L$, it obviously holds that $K(S \cup T) = K(S)(T) = K(T)(S)$. For $\sigma \in \mathrm{Aut}(L)$, it also holds that $\sigma(K(S)) = \sigma(K)(\sigma(S))$.

(iv) If $x \in L$ is transcendental, then the evaluation homomorphism $F_x\colon K[X] \to L$ is injective. Because of $\alpha(x) \in K(x)$ for all $\alpha \in K[X]$, we have $F_x(K[X]) \subseteq K(x)$. According to Exercise I.40, F_x can be extended to a field homomorphism $\hat{F}_x\colon K(X) \to K(x)$. Because of $x = F_x(X) \in \hat{F}_x(K(X))$, $\hat{F}_x(K(X))$ is a subfield of L that contains x. Therefore, $\hat{F}_x$ is surjective and it follows that $K(X) \cong K(x)$. In particular, the isomorphism type of $K(x)$ does not depend on x (as long as x is transcendental).

Example I.9.4. Because of $\sqrt{2} \notin \mathbb{Q}$, $X^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$. Analogously, $X^2 + 1$ is the minimal polynomial of $\mathrm{i} \in \mathbb{C}$ over $\mathbb{Q}$ (or over $\mathbb{R}$).

Theorem I.9.5 (Degree Theorem)**.** *For field extensions $K \subseteq L \subseteq M$, it holds that*

$$\boxed{|M : K| = |M : L||L : K|.}$$

Proof. If $|M : L|$ or $|L : K|$ is infinite, then so is $|M : K|$. So let $|M : L||L : K| < \infty$. Let $b_1, \ldots, b_n \in L$ be a K-basis of L and $c_1, \ldots, c_m \in M$ be an L-basis of M. Every $x \in M$ can be written in the form $x = \sum_{i=1}^{m} x_i c_i$ with $x_i \in L$. Furthermore, $x_i = \sum_{j=1}^{n} x_{ij} b_j$ with $x_{ij} \in K$. In total, $x = \sum_{i,j} x_{ij} b_j c_i$ and $\{b_i c_j : i = 1, \ldots, n,\ j = 1, \ldots, m\}$ is a generating set of M as a K-vector space. Now let $\sum_{i,j} x_{ij} b_i c_j = 0$ for certain $x_{ij} \in K$. Because of

$$\sum_j \Big(\underbrace{\sum_i x_{ij} b_i}_{\in L} \Big) c_j = 0$$

it follows that $\sum_i x_{ij} b_i = 0$ for all j from the linear independence of $c_1, \ldots, c_m$. Since $b_1, \ldots, b_n$ are linearly independent over K, it follows that $x_{ij} = 0$ for all i, j. Therefore, $\{b_i c_j : i = 1, \ldots, n,\ j = 1, \ldots, m\}$ is a K-basis of M. □

Theorem I.9.6. *Every finite field extension is algebraic.*

Proof. Let $K \subseteq L$ be a finite field extension and $x \in L$. Then there exists an $n \in \mathbb{N}$ such that $1, x, \ldots, x^n$ are linearly dependent over K. Thus there exist $a_0, \ldots, a_n \in K$ (not all 0) with $a_0 + a_1 x + \ldots + a_n x^n = 0$. As a root of $\sum a_i X^i \in K[X] \setminus \{0\}$, x is algebraic over K. □

Remark I.9.7. Finite field extensions of $\mathbb{Q}$ in $\mathbb{C}$ are called (*algebraic*) *number fields*.

Theorem I.9.8. *Let $K \subseteq L$ be a field extension and $x \in L$ algebraic with minimal polynomial μ_x. Then* $\boxed{K(x) \cong K[X]/(\mu_x)}$ *and* $\boxed{|K(x) : K| = \deg \mu_x.}$

Proof. Let $F_x\colon K[X] \to L$ be the evaluation homomorphism. The isomorphism theorem for rings shows

$$K[X]/(\mu_x) \cong F_x(K[X]) \subseteq K(x).$$

According to Theorem I.8.38, $K[X]/(\mu_x)$ is a field and thus so is $F_x(K[X])$. Because of $x = F_x(X) \in F_x(K[X])$, it holds that $F_x(K[X]) = K(x)$.

For the second assertion, it suffices to show that $1 + (\mu_x), X + (\mu_x), X^2 + (\mu_x), \ldots, X^{d-1} + (\mu_x)$ with $d := \deg \mu_x$ is a K-basis of $K[X]/(\mu_x)$. Euclidean division shows that these elements form a generating set of $K[X]/(\mu_x)$. Since μ_x cannot divide any polynomial of degree $e \in \{0, \ldots, d-1\}$, $1 + (\mu_x), X + (\mu_x), \ldots, X^{d-1} + (\mu_x)$ are also linearly independent over K. □

Remark I.9.9. The proof shows $K(x) = \{\alpha(x) : \alpha \in K[X]\}$ if x is algebraic over K (cf. Remark I.9.3(iv)). Furthermore, $1, x, x^2, \ldots, x^{d-1}$ is a K-basis of $K(x)$ with $d := \deg \mu_x$.

Example I.9.10. It holds that $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[X]/(X^2 - 2)$.

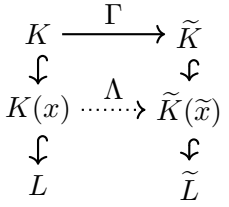
Lemma I.9.11. *If $K \subseteq L$ is an algebraic field extension, then every K-homomorphism $L \to L$ is an automorphism.*

Proof. Let $\sigma\colon L \to L$ be a K-homomorphism. According to Lemma I.8.41, σ is injective. Let $x \in L$ and $\mu \in K[X]$ be the minimal polynomial of x. According to Lemma I.8.44, it holds that

$$\mu(\sigma(x)) = \sigma(\mu)(\sigma(x)) = \sigma(\mu(x)) = \sigma(0) = 0,$$

i. e. $\sigma(x)$ is a root of μ. Since σ is injective, the roots of μ are permuted by σ. In particular, there exists a root $y \in L$ of μ with $\sigma(y) = x$. Thus σ is surjective. □

Theorem I.9.12 (Extension Theorem)**.** *Let $K \subseteq L$ and $\widetilde{K} \subseteq \widetilde{L}$ be field extensions and $x \in L$ algebraic with minimal polynomial $\mu \in K[X]$. Let $\Gamma\colon K \to \widetilde{K}$ be a field isomorphism and $\widetilde{x} \in \widetilde{L}$ a root of $\Gamma(\mu) \in \widetilde{K}[X]$ (Lemma I.8.44). Then there exists an isomorphism $\Lambda\colon K(x) \to \widetilde{K}(\widetilde{x})$ with $\Lambda_K = \Gamma$ and $\Lambda(x) = \widetilde{x}$.*



Proof. According to Lemma I.8.44, one can extend Γ to a ring isomorphism $K[X] \to \widetilde{K}[X]$ with $X \mapsto X$. Composition with the canonical epimorphism $\widetilde{K}[X] \to \widetilde{K}[X]/(\Gamma(\mu))$ yields an epimorphism $K[X] \to \widetilde{K}[X]/(\Gamma(\mu))$ with $X \mapsto X + (\Gamma(\mu))$. With the isomorphism theorem, one obtains an isomorphism

$$\Delta\colon K[X]/(\mu) \to \widetilde{K}[X]/(\Gamma(\mu))$$

with $X + (\mu) \mapsto X + (\Gamma(\mu))$. According to Theorem I.9.8, there exists an isomorphism $f_x\colon K(x) \to K[X]/(\mu)$ with $x \mapsto X + (\mu)$. Along with μ, $\Gamma(\mu) \in \widetilde{K}[X]$ is also irreducible. Therefore, $\Gamma(\mu)$ is the minimal polynomial of $\widetilde{x}$ and one obtains an isomorphism $f_{\widetilde{x}}\colon \widetilde{K}(\widetilde{x}) \to \widetilde{K}[X]/(\Gamma(\mu))$ with $\widetilde{x} \mapsto X + (\Gamma(\mu))$. The isomorphism $\Lambda := f_{\widetilde{x}}^{-1} \circ \Delta \circ f_x\colon K(x) \to \widetilde{K}(\widetilde{x})$ then satisfies $\Lambda_K = \Gamma$ and $\Lambda(x) = \widetilde{x}$. □

Example I.9.13. Choose $K = \widetilde{K} = \mathbb{Q}$, $L = \widetilde{L} = \mathbb{R}$, $x = \sqrt{2}$, $\Gamma = \mathrm{id}_{\mathbb{Q}}$ and $\widetilde{x} := -\sqrt{2}$. This yields $\Lambda \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$ with $\Lambda(\sqrt{2}) = -\sqrt{2}$.

Definition I.9.14. Let $\alpha \in K[X] \setminus K$. A field $L \supseteq K$ is called a *splitting field* of α if

$$\alpha = c \prod_{i=1}^{n} (X - x_i) \in L[X]$$

and $L = K(x_1, \ldots, x_n)$ with $c \in K$.

Example I.9.15. Because $X^2-2=(X-\sqrt{2})(X+\sqrt{2})\in\mathbb{Q}(\sqrt{2})[X]$, $\mathbb{Q}(\sqrt{2})=\mathbb{Q}(\pm\sqrt{2})$ is the splitting field of $X^2-2\in\mathbb{Q}[X]$. On the other hand, $\mathbb{R}$ is *not* a splitting field of X^2-2, because $\mathbb{Q}(\sqrt{2})\neq\mathbb{R}$ (countable vs. uncountable). It is by no means clear whether every polynomial possesses a splitting field. For example, one must introduce the symbol i as a root of $X^2+1\in\mathbb{R}[X]$, so that $\mathbb{C}$ becomes the splitting field of X^2+1. As is well known, $\mathbb{C}\cong\mathbb{R}[X]/(X^2+1)$ then holds. We will reverse this isomorphism to construct arbitrary splitting fields.

Theorem I.9.16 (Kronecker)**.** *Every $\alpha\in K[X]\setminus K$ possesses a splitting field L with $|L:K|\leq\deg(\alpha)!$.*

Proof. Induction on $d:=\deg\alpha$. In the case $d=1$, K is a splitting field. So let $d>1$. Let $\beta\in K[X]$ be an irreducible divisor of α and $M:=K[X]/(\beta)$. Through $a\mapsto a+(\beta)$, we can regard K as a subfield of M. We now consider the polynomial ring $M[Y]$ over M in a new indeterminate Y. Then $\alpha\in M[Y]$ has the root $y:=X+(\beta)$ in M, because

$$\alpha(X+(\beta))=\alpha(X)+(\beta)=0\in M.$$

Write $\alpha=(Y-y)\gamma$ with $\gamma\in M[Y]$. By induction, there exists a splitting field L of γ over M. Because $M=K(y)$, L is also a splitting field of α over K and

$$|L:K|\overset{\text{I.9.5}}{=}|L:M||M:K|\leq\deg(\gamma)!\deg\beta\leq(d-1)!d=d!.$$ □

Example I.9.17. According to Example I.8.23, $\alpha=X^2+X+1\in\mathbb{F}_2[X]$ is irreducible. The splitting field L of α is therefore larger than $\mathbb{F}_2$. Because $|L:\mathbb{F}_2|\leq\deg(\alpha)!=2$, it follows that $|L|=4$. In this way, we will later construct all finite fields.

Theorem I.9.18 (Steinitz)**.** *Let $\Gamma\colon K\to\widetilde{K}$ be a field isomorphism and $\alpha\in K[X]\setminus K$. Let L be a splitting field of α and let $\widetilde{L}$ be a splitting field of $\Gamma(\alpha)\in\widetilde{K}[X]$. Then there exists an isomorphism $\Lambda\colon L\to\widetilde{L}$ with $\Lambda_K=\Gamma$. In particular, L is unique up to K-isomorphism.*

$$\begin{array}{ccc} K & \xrightarrow{\ \Gamma\ } & \widetilde{K} \\ \downarrow & & \downarrow \\ L & \overset{\Lambda}{\dashrightarrow} & \widetilde{L} \end{array}$$

Proof. Induction on $d:=\deg\alpha$. In the case $d=1$, $\Lambda=\Gamma$. Let $d>1$ and $\beta\in K[X]$ be an irreducible divisor of α with root $x\in L$. Because $\Gamma(\beta)\mid\Gamma(\alpha)$, $\widetilde{L}$ has a root $\widetilde{x}$ of $\Gamma(\beta)$. According to the extension theorem, Γ can be extended to $\widehat{\Gamma}\colon K(x)\to\widetilde{K}(\widetilde{x})$. Let $\alpha=(X-x)\gamma$ with $\gamma\in K(x)[X]$. Then L is a splitting field of γ and $\widetilde{L}$ is a splitting field of $\widehat{\Gamma}(\gamma)$. By induction, $\widehat{\Gamma}$ can be extended to $\Lambda\colon L\to\widetilde{L}$. The second claim follows with $K=\widetilde{K}$ and $\Gamma=\mathrm{id}_K$. □

I.10 Galois Theory

Lemma I.10.1. *Let $K \subseteq L$ be a finite field extension with $L = \bigcup_{i=1}^{n} M_i$ for intermediate fields $K \subseteq M_i \subseteq L$. Then $L = M_i$ for some $i \in \{1, \ldots, n\}$.*

Proof. We can assume that n is minimal and $n > 1$ holds. Let $x_i \in M_i \setminus \bigcup_{j \neq i} M_j$ for $i = 1, 2$. If K is infinite, then there exist $\lambda, \mu \in K$ with $\lambda \neq \mu$ and $x_1 + \lambda x_2, x_1 + \mu x_2 \in M_i$ for some $i \in \{1, \ldots, n\}$ (pigeonhole principle). Then $x_2 = (\lambda - \mu)^{-1}((x_1 + \lambda x_2) - (x_1 + \mu x_2)) \in M_i$ and $i = 2$. This yields the contradiction $x_1 = (x_1 + \lambda x_2) - \lambda x_2 \in M_2$.

Now let K be finite. Then L is also finite and according to Theorem I.8.31 there exists an $x \in L$ with $L^\times = \langle x \rangle$. Let $x \in M_i$ for some $i \in \{1, \ldots, n\}$. Then $L = \{0\} \cup \langle x \rangle \subseteq M_i$ and the claim follows. □

Definition I.10.2. For a field extension $K \subseteq L$, let

$$\mathrm{Gal}(L|K) := \{\sigma \in \mathrm{Aut}(L) : \sigma_K = \mathrm{id}_K\} \leq \mathrm{Aut}(L)$$

be the *Galois group* of L over K. For $H \leq \mathrm{Gal}(L|K)$, let

$$L^H := \{x \in L : \sigma(x) = x \ \forall \sigma \in H\}$$

be the *fixed field* of H in L. For $\sigma \in \mathrm{Gal}(L|K)$, let $L^\sigma := L^{\langle \sigma \rangle}$.

Remark I.10.3. It is easy to show that $\mathrm{Gal}(L|K)$ is a subgroup of $\mathrm{Aut}(L)$ and L^H is a subfield of L.

Example I.10.4.

(i) The complex conjugation $\sigma \in \mathrm{Gal}(\mathbb{C}|\mathbb{R})$. Here $\mathbb{C}^\sigma = \mathbb{R}$ holds.

(ii) For every number field K, $\mathrm{Gal}(K|\mathbb{Q}) = \mathrm{Aut}(K)$ holds, because for $\sigma \in \mathrm{Aut}(K)$, $\sigma_\mathbb{Q} \in \mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}_\mathbb{Q}\}$ according to Exercise I.53.

Remark I.10.5. If $x \in L$ is algebraic over K with minimal polynomial $\mu \in K[X]$ and $\sigma \in \mathrm{Gal}(L|K)$, then $\sigma(\mu) = \mu$ and

$$\mu(\sigma(x)) = \sigma(\mu)(\sigma(x)) \overset{\text{I.8.44}}{=} \sigma(\mu(x)) = \sigma(0) = 0.$$

Conclusion: $\mathrm{Gal}(L|K)$ acts on the set of roots of μ. If L is the splitting field of μ, then this action is faithful, because in this case L is generated by the roots. One then obtains a monomorphism $\mathrm{Gal}(L|K) \to S_{\deg \mu}$ (Theorem I.8.29).

Theorem I.10.6. *For every field extension $K \subseteq L$, $|\mathrm{Gal}(L|K)| \leq |L : K|$ holds.*

Proof. We can assume $|L : K| < \infty$. Let $L = K(x_1, \ldots, x_n)$ and $\sigma \in \mathrm{Gal}(L|K) =: G$. Then $\sigma(x_i)$ is a root of the minimal polynomial of x_i. In particular, there are only finitely many possibilities for $\sigma(x_i)$. Because $L = K(x_1, \ldots, x_n)$, σ is already uniquely determined by $\{\sigma(x_i) : i = 1, \ldots, n\}$. This shows $|G| < \infty$.

For $\sigma \in G \setminus \{1\}$, $L^\sigma \neq L$ holds. According to Lemma I.10.1, there exists an $x \in L \setminus \bigcup_{1 \neq \sigma \in G} L^\sigma$. The minimal polynomial $\mu \in K[X]$ of x then has pairwise distinct roots $\sigma(x)$ for $\sigma \in G$. This shows

$$|G| \overset{\text{I.8.29}}{\leq} \deg \mu \overset{\text{I.9.8}}{=} |K(x) : K| \leq |L : K|. \qquad \square$$

Definition I.10.7. A field extension $K \subseteq L$ is called a *Galois extension*, if

$$|\mathrm{Gal}(L|K)| = |L : K| < \infty.$$

Example I.10.8.

(i) Because of $\mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}, \sigma\}$ with the complex conjugation σ, $\mathbb{R} \subseteq \mathbb{C}$ is a Galois extension. According to Example I.9.13, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is also a Galois extension.

(ii) Obviously, $\mu := X^3 - 2$ is the minimal polynomial of $x := \sqrt[3]{2} \in \mathbb{R}$ over $\mathbb{Q}$. Every $\sigma \in \mathrm{Gal}(\mathbb{Q}(x)|\mathbb{Q})$ must map x to a root of μ. In this case, $\sigma(x) \in \mathbb{Q}(x) \subseteq \mathbb{R}$ holds. Since x is the only real root of μ (the others are $x\zeta$ and $x\bar{\zeta}$ with $\zeta = e^{2\pi \mathrm{i}/3} = \frac{1}{2}(-1 + \sqrt{3}\mathrm{i})$), it follows that $\sigma(x) = x$ and $\sigma = \mathrm{id}$. Therefore, $|\mathrm{Gal}(\mathbb{Q}(x)|\mathbb{Q})| = 1 < 3 = |\mathbb{Q}(x) : \mathbb{Q}|$ and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ is *not* a Galois extension.

Theorem I.10.9 (Artin)**.** *For every finite field extension $K \subseteq L$ with $G := \mathrm{Gal}(L|K)$, the following are equivalent:*

(1) $K \subseteq L$ is a Galois extension.

(2) $L^G = K$.

(3) L is the splitting field of a polynomial $\alpha \in K[X]$ with pairwise distinct roots.

(4) There exists an $x \in L$ with $L = K(x)$ and minimal polynomial μ, such that μ splits into pairwise distinct linear factors over L.

Proof.

(1) $\Rightarrow$ (2): It holds that $K \subseteq L^G$ and $|L : K| \overset{(1)}{=} |G| \leq |\mathrm{Gal}(L|L^G)| \overset{\text{I.10.6}}{\leq} |L : L^G| \leq |L : K|$. Thus $L^G = K$.

(2) $\Rightarrow$ (3): Let $L = K(x_1, \ldots, x_n)$, $S := \{\sigma(x_i) : \sigma \in G,\ i = 1, \ldots, n\} \subseteq L$ and

$$\alpha := \prod_{s \in S} (X - s) \in L[X].$$

Then

$$\sigma(\alpha) = \prod_{s \in S} (X - \sigma(s)) = \prod_{s \in S} (X - s) = \alpha$$

for all $\sigma \in G$. From (2) it follows that $\alpha \in L^G[X] = K[X]$. By construction, L is the splitting field of α and the roots $s \in S$ are pairwise distinct.

(3) $\Rightarrow$ (1): Let α be as in (3) with pairwise distinct roots $x_1, \ldots, x_n \in L$. We argue by induction on $|L : K|$ and can assume $|L : K| > 1$. Let $\beta \in K[X]$ be an irreducible divisor of α with roots $x_1, \ldots, x_s$ (wlog.). By the extension theorem, there are pairwise distinct K-isomorphisms $\sigma_i \colon K(x_1) \to K(x_i)$ for $i = 1, \ldots, s$. Since L is also the splitting field of α over $K(x_1)$, each σ_i can be extended to L (Steinitz). Each of these extensions can be composed with $\gamma \in \mathrm{Gal}(L|K(x_1))$. By induction, $|\mathrm{Gal}(L|K(x_1))| = |L : K(x_1)|$. Thus, one obtains

$$|L : K(x_1)|s = |L : K(x_1)| \deg \beta = |L : K(x_1)||K(x_1) : K| = |L : K|$$

distinct elements of G. According to Theorem I.10.6, there cannot be more.

(1) $\Rightarrow$ (4): Let $x \in L \setminus \bigcup_{1 \neq \sigma \in G} L^\sigma$ (Lemma I.10.1) be as in the proof of Theorem I.10.6. Then the minimal polynomial $\mu \in K[X]$ of x has pairwise distinct roots $\sigma(x)$ ($\sigma \in G$). It follows that

$$|L : K| \overset{(1)}{=} |G| \leq \deg \mu = |K(x) : K| \leq |L : K|.$$

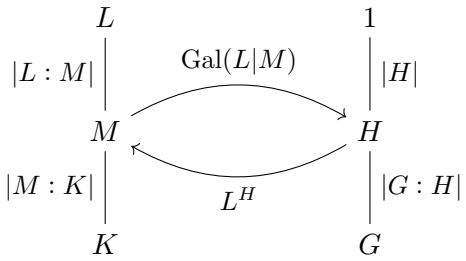
Thus $L = K(x)$ and μ has exactly the roots $\sigma(x)$ ($\sigma \in G$).

(4) $\Rightarrow$ (3): Choose $\alpha = \mu$. □

Example I.10.10. The splitting field $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi \mathrm{i}/3})$ of $X^3 - 2$ is a Galois extension over $\mathbb{Q}$, because the roots of $X^3 - 2$ are pairwise distinct.

Theorem I.10.11 (Fundamental Theorem of Galois Theory[1])**.** *Let $K \subseteq L$ be a Galois extension, $G := \mathrm{Gal}(L|K)$, $\mathcal{M} := \{M \text{ field} : K \subseteq M \subseteq L\}$ and $\mathcal{H} := \{H : H \leq G\}$. Then:*

(i) The maps $M \mapsto \mathrm{Gal}(L|M)$ and $H \mapsto L^H$ are mutually inverse, inclusion-reversing bijections between $\mathcal{M}$ and $\mathcal{H}$. In this context, $\boxed{|L : L^H| = |H|}$ *and* $\boxed{|L^H : K| = |G : H|}$ *hold.*



(ii) For $M \in \mathcal{M}$, $M \subseteq L$ is a Galois extension.

(iii) $K \subseteq M \in \mathcal{M}$ is a Galois extension if and only if $\mathrm{Gal}(L|M) \trianglelefteq G$. In this case,

$$\boxed{\mathrm{Gal}(M|K) \cong \mathrm{Gal}(L|K)/\mathrm{Gal}(L|M).}$$

Proof.

(ii) According to Artin, L is the splitting field of a polynomial $\alpha \in K[X]$ with pairwise distinct roots. Then L is certainly also the splitting field of $\alpha \in M[X]$ and again according to Artin, $M \subseteq L$ is a Galois extension.

[1] On Galois' life see [T. Rothman, *Genius and biographers: the fictionalization of Évariste Galois*, Amer. Math. Monthly 89 (1982), 84–106]

(i) For $M \in \mathcal{M}$, $M \subseteq L$ is a Galois extension according to (ii). By Artin, it follows that $L^{\mathrm{Gal}(L|M)} = M$. Conversely, let $H \in \mathcal{H}$. Then $H \leq \mathrm{Gal}(L|L^H)$. According to Artin, there exists an $x \in L$ with $L = K(x)$. It holds that $\alpha := \prod_{\sigma \in H}(X - \sigma(x)) \in L^H[X]$. For $\sigma \in \mathrm{Gal}(L|L^H)$, $\sigma(x)$ is a root of $\sigma(\alpha) = \alpha$. Thus there exists a $\tau \in H$ with $\sigma(x) = \tau(x)$. Because of $K(x) = L$, it follows that $\sigma = \tau \in H$. In total, $H = \mathrm{Gal}(L|L^H)$. Therefore, the specified maps are inverse bijections to each other. Because of

$$H_1 \subseteq H_2 \Longrightarrow L^{H_2} \subseteq L^{H_1}$$

the maps are inclusion-reversing. Furthermore, $|L : L^H| = |\mathrm{Gal}(L|L^H)| = |H|$ and $|L^H : K| = |L : K|/|L : L^H| = |G : H|$.

(iii) Let us first assume that $K \subseteq M$ is a Galois extension. According to Artin, M is the splitting field of an $\alpha \in K[X]$. Since every $\sigma \in G$ permutes the roots of $\alpha = \sigma(\alpha)$, it follows that $\sigma(M) = M$. With $H := \mathrm{Gal}(L|M)$, it holds that

$$\begin{aligned} L^H &\overset{\text{(i)}}{=} M = \sigma(M) = \sigma(L^H) = \big\{\sigma(x) \in \sigma(L) : \forall \gamma \in H : \gamma(x) = x\big\} \\ &= \big\{x \in L : \forall \gamma \in H : \gamma(\sigma^{-1}(x)) = \sigma^{-1}(x)\big\} \\ &= \big\{x \in L : \forall \gamma \in H : (\sigma\gamma\sigma^{-1})(x) = x\big\} = L^{\sigma H \sigma^{-1}} \end{aligned}$$

and $\sigma H \sigma^{-1} = H$ according to (i). This shows $H \trianglelefteq G$.

Conversely, let $H := \mathrm{Gal}(L|M) \trianglelefteq G$. For $\sigma \in G$, it then holds that $\sigma(M) = \sigma(L^H) = L^{\sigma H \sigma^{-1}} = L^H = M$. Therefore, the restriction $\Gamma\colon G \to \mathrm{Gal}(M|K)$ is well-defined with $\mathrm{Ker}(\Gamma) = H$. It follows that

$$|M : K| \overset{\text{(i)}}{=} |G : H| = |G/\mathrm{Ker}(\Gamma)| \overset{\text{I.3.29}}{\leq} |\mathrm{Gal}(M|K)| \overset{\text{I.10.6}}{\leq} |M : K|.$$

Thus $K \subseteq M$ is a Galois extension and $\mathrm{Gal}(M|K) = \Gamma(G) \cong G/H$. □

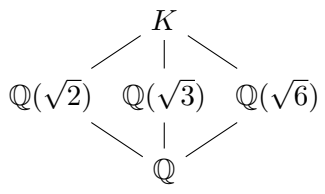
Example I.10.12. We already know that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is a Galois extension of degree 2. Assumption: $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then there exist $a, b \in \mathbb{Q}$ with $\sqrt{3} = a + \sqrt{2}b$. It follows that $3 = a^2 + 2b^2 + 2\sqrt{2}ab$. Since $1, \sqrt{2}$ are linearly independent over $\mathbb{Q}$, it holds that $ab = 0$. Because $\sqrt{3} \notin \mathbb{Q}$, we have $a = 0$ and $3 = 2b^2$. By multiplying with the denominator of b, one obtains $3c^2 = 2d^2$ with $c, d \in \mathbb{N}$. This contradicts the unique prime factorization. Thus $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ and $X^2 - 3$ is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. For $K := \mathbb{Q}(\sqrt{2}, \sqrt{3})$, it therefore holds that

$$|K : \mathbb{Q}| \overset{\text{I.9.5}}{=} |K : \mathbb{Q}(\sqrt{2})||\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 4.$$

The extension theorem yields $G := \mathrm{Gal}(K|\mathbb{Q}) = \{\mathrm{id}, \alpha, \beta, \gamma\}$ with

$$\begin{aligned} &\alpha(\sqrt{2}) = \sqrt{2}, && \beta(\sqrt{2}) = -\sqrt{2}, && \gamma(\sqrt{2}) = -\sqrt{2}, \\ &\alpha(\sqrt{3}) = -\sqrt{3}, && \beta(\sqrt{3}) = \sqrt{3}, && \gamma(\sqrt{3}) = -\sqrt{3}. \end{aligned}$$

In particular, $\mathbb{Q} \subseteq K$ is a Galois extension. Because of $\alpha^2 = \beta^2 = \gamma^2 = \mathrm{id}_K$, we have $G \cong C_2 \times C_2$ according to the fundamental theorem of finite abelian groups. The subgroups of G are 1, $\langle\alpha\rangle$, $\langle\beta\rangle$, $\langle\gamma\rangle$ and G. Obviously $\mathbb{Q}(\sqrt{2}) \subseteq K^\alpha$. Because of $|K^\alpha : \mathbb{Q}| = |G : \langle\alpha\rangle| = 2$, it holds that $K^\alpha = \mathbb{Q}(\sqrt{2})$. Analogously, one obtains the remaining intermediate fields $K^\beta = \mathbb{Q}(\sqrt{3})$ and $K^\gamma = \mathbb{Q}(\sqrt{6})$. Since G is abelian, all these intermediate fields form Galois extensions over $\mathbb{Q}$.



Remark I.10.13. The intermediate fields of an arbitrary Galois extension $K \subseteq L$ can in general be determined by a system of linear equations. For $H \leq \mathrm{Gal}(L|K)$, we have $x \in L^H$ if and only if x lies in the kernel of the K-linear maps $\sigma - \mathrm{id}_L$ for $\sigma \in H$. Often it is easier to choose a "random" element $x \in L$ and consider the *trace* $\mathrm{tr}(x) := \sum_{\sigma \in H} \sigma(x)$. For $\tau \in H$, it holds that

$$\tau(\mathrm{tr}(x)) = \sum_{\sigma \in H} \tau(\sigma(x)) = \sum_{\gamma \in H} \gamma(x) = \mathrm{tr}(x) \in L^H.$$

It can of course happen that $\mathrm{tr}(x)$ lies in K, so that one obtains no information about L^H. With $x := \sqrt{2} + \sqrt{3}$ and $H := \langle \beta \rangle$ in Example I.10.12, one gets $\mathrm{tr}(x) = 2\sqrt{3}$.

Definition I.10.14. For $i = 1, 2$ let $K \subseteq M_i \subseteq L$ be field extensions. One calls

$$M_1 M_2 := M_1(M_2) = M_2(M_1)$$

the *compositum* of M_1 and M_2 (the "smallest" subfield of L containing M_1 and M_2).

Theorem I.10.15. *For finite field extensions $K \subseteq M_i \subseteq L$ with $i = 1, 2$, the following holds:*

(i)
$$\mathrm{lcm}\big(|M_1 : K|, |M_2 : K|\big) \;\big|\; |M_1 M_2 : K| \leq |M_1 : K||M_2 : K|.$$

(ii) (*Translation Theorem*) *If $K \subseteq M_1$ is a Galois extension, then so is $M_2 \subseteq M_1 M_2$ and it holds that*

$$\boxed{\mathrm{Gal}(M_1 M_2|M_2) \cong \mathrm{Gal}(M_1|M_1 \cap M_2).}$$

(iii) If $K \subseteq M_1$ and $K \subseteq M_2$ are Galois extensions, then so is $K \subseteq M_1 M_2$. In this case, $\mathrm{Gal}(M_1 M_2|K)$ is isomorphic to a subgroup of $\mathrm{Gal}(M_1|K) \times \mathrm{Gal}(M_2|K)$. Equality holds if and only if $M_1 \cap M_2 = K$.

(iv) If $K \subseteq L$ is a Galois extension with $G := \mathrm{Gal}(L|K)$ and $H_1, H_2 \leq G$, then $\boxed{L^{H_1} L^{H_2} = L^{H_1 \cap H_2}}$ and $\boxed{L^{H_1} \cap L^{H_2} = L^{\langle H_1, H_2 \rangle}.}$

Proof.

(i) The degree theorem implies $|M_i : K| \;\big|\; |M_1 M_2 : K|$ for $i = 1, 2$. For the second assertion, it suffices to show $|M_1 M_2 : M_2| \leq |M_1 : K|$. Let $b_1, \ldots, b_n$ be a K-basis of M_1. Then

$$M_1 \cup M_2 \subseteq S := M_2 b_1 + \ldots + M_2 b_n \subseteq M_1 M_2$$

and it suffices to show that S is a field. Certainly $(S, +)$ is an abelian group. For $i, j \in \{1, \ldots, n\}$, we have $b_i b_j \in M_1 \subseteq S$. This shows $xy \in S$ for $x, y \in S$. For $x \neq 0$, the map $\sigma \colon S \to S$, $y \mapsto xy$ is injective. Since S is a finite-dimensional M_2-vector space, σ is even M_2-linear and thus bijective. In particular, there exists a $y \in L$ with $xy = 1$, i. e. $x^{-1} = y \in S$.

(ii) According to Artin, M_1 is the splitting field of an $\alpha \in K[X]$ with pairwise distinct roots $x_1, \ldots, x_d \in M_1$. Obviously $M_1 M_2 = M_2(M_1) = M_2(x_1, \ldots, x_d)$ is the splitting field of $\alpha \in M_2[X]$. According to Artin, $M_2 \subseteq M_1 M_2$ is a Galois extension. For $\sigma \in G := \mathrm{Gal}(M_1 M_2|M_2)$, we have $\sigma(M_1) = K(\sigma(x_1), \ldots, \sigma(x_d)) = M_1$ because of $\sigma(\alpha) = \alpha$. As in the Fundamental Theorem of Galois Theory, the restriction $\Gamma \colon G \to H := \mathrm{Gal}(M_1|M_1 \cap M_2)$ is a well-defined monomorphism. For $x \in M_1 \setminus M_2$, there exists a $\sigma \in G$ with $\sigma(x) \neq x$ because of $(M_1 M_2)^G = M_2$. This shows $M_1^{\Gamma(G)} = M_1 \cap M_2$ and $\Gamma(G) = H$ according to the Fundamental Theorem of Galois Theory.

(iii) Let M_i be the splitting field of $\alpha_i \in K[X]$ with pairwise distinct roots. Then M_1M_2 is the splitting field of $\frac{\alpha_1\alpha_2}{\gcd(\alpha_1,\alpha_2)} \in K[X]$ with pairwise distinct roots. According to Artin, $K \subseteq M_1M_2$ is a Galois extension. Obviously the map

$$\begin{aligned}\Gamma\colon \mathrm{Gal}(M_1M_2|K) &\to \mathrm{Gal}(M_1|K) \times \mathrm{Gal}(M_2|K),\\ \sigma &\mapsto (\sigma_{|M_1}, \sigma_{|M_2})\end{aligned}$$

is a well-defined monomorphism. From (ii) it follows

$$|\mathrm{Gal}(M_1M_2|K)| = |M_1M_2 : K| = |M_1M_2 : M_2||M_2 : K| = |M_1 : M_1 \cap M_2||M_2 : K|.$$

Thus Γ is surjective if and only if $M_1 \cap M_2 = K$.

(iv) Since $\langle H_1, H_2\rangle$ consists of products of elements from $H_1 \cup H_2$, we have $L^{H_1} \cap L^{H_2} = L^{\langle H_1,H_2\rangle}$. Finally, $L^{H_i} \subseteq L^{H_1}L^{H_2} \subseteq L^{H_1\cap H_2}$ and $H_1 \cap H_2 \subseteq \mathrm{Gal}(L|L^{H_1}L^{H_2}) \subseteq H_1 \cap H_2$. This shows $L^{H_1}L^{H_2} = L^{H_1\cap H_2}$. □

Example I.10.16. If one replaces K by $M_1 \cap M_2$ in Theorem I.10.15(i),(ii), one obtains $|M_1M_2 : M_2| \leq |M_1 : M_1 \cap M_2|$ and

$$\boxed{\mathrm{Gal}(M_1M_2|M_1 \cap M_2) \cong \mathrm{Gal}(M_1|M_1 \cap M_2) \times \mathrm{Gal}(M_2|M_1 \cap M_2).}$$

If neither M_1 nor M_2 is a Galois extension over K, then the inequality can be strict as in the case $M_1 = \mathbb{Q}(\sqrt[3]{2})$ and $M_2 = \mathbb{Q}(\sqrt[3]{2}e^{2\pi\mathrm{i}/3})$.

I.11 Finite Fields

Definition I.11.1.

(i) Obviously, there exists exactly one ring homomorphism $\Phi\colon \mathbb{Z} \to K$ (since $\Phi(1) = 1$, $\Phi(2) = \Phi(1+1) = 1+1$, etc.). According to Example I.7.9(vii), there exists exactly one $c \in \mathbb{N}_0$ with $\operatorname{Ker}(\Phi) = c\mathbb{Z}$. One calls $\operatorname{char} K := c$ the *characteristic* of K. In the following, we will identify $z \in \mathbb{Z}$ with $\Phi(z) \in K$.

(ii) The *prime field* $P(K)$ of K is the intersection of all subfields of K. Obviously, $P(K)$ is then the "smallest" subfield of K.

Example I.11.2.

(i) Since the embedding $\Phi\colon \mathbb{Z} \to \mathbb{Q}$ is injective, $\operatorname{char} \mathbb{Q} = 0$ holds. This also holds for every extension of $\mathbb{Q}$.

(ii) For $p \in \mathbb{P}$, $\underbrace{1 + \ldots + 1}_{p\text{-times}} = 0$ holds in $\mathbb{F}_p$. This shows $\operatorname{char} \mathbb{F}_p = p$.

Theorem I.11.3. *It holds that* $\operatorname{char} K \in \mathbb{P} \cup \{0\}$ *and*

$$P(K) \cong \begin{cases} \mathbb{Q} & \text{if } \operatorname{char} K = 0, \\ \mathbb{F}_p & \text{if } \operatorname{char} K = p > 0. \end{cases}$$

Proof. In the case $\operatorname{char} K = 0$, the ring monomorphism $\Phi\colon \mathbb{Z} \to P(K)$ can be extended to a field homomorphism $\widehat{\Phi}\colon \mathbb{Q} \to P(K)$ according to Exercise I.40. Thus, $\widehat{\Phi}(\mathbb{Q})$ is a subfield of $P(K)$ and it follows that $P(K) = \widehat{\Phi}(\mathbb{Q}) \cong \mathbb{Q}$.

Now let $c := \operatorname{char} K > 0$. The homomorphism theorem yields an isomorphism $\widehat{\Phi}\colon \mathbb{Z}/c\mathbb{Z} \to \Phi(\mathbb{Z}) \subseteq P(K)$. As a subring of $P(K)$, $\Phi(\mathbb{Z}) \cong \mathbb{Z}/c\mathbb{Z}$ is a finite integral domain. According to Exercise I.36, $\mathbb{Z}/c\mathbb{Z}$ is a field and it follows that $\widehat{\Phi}(\mathbb{Z}) = P(K)$. According to Corollary I.7.13, $c \in \mathbb{P}$ and the claim follows. □

Example I.11.4. If K is finite, then $P(K) \cong \mathbb{F}_p$ holds for some $p \in \mathbb{P}$. Since K is a finite-dimensional vector space over $P(K)$, $|K| = p^n$ holds for some $n \in \mathbb{N}$. In particular, there is no field with six elements. Conversely, we will show that for every prime power $p^n \neq 1$, there is essentially exactly one field with p^n elements.

Definition I.11.5. For $\alpha = \sum_{n=0}^{\infty} a_n X^n \in K[X]$, $\alpha' := \sum_{n=1}^{\infty} n a_n X^{n-1} \in K[X]$ is the (formal) *derivative* of α.

Example I.11.6. In $\mathbb{F}_2[X]$, $(X^2)' = 2X = 0$ holds.

Lemma I.11.7. *For $a, b \in K$ and $\alpha, \beta \in K[X]$, it holds that*

$$(a\alpha + b\beta)' = a\alpha' + b\beta' \qquad \text{(sum rule)},$$
$$(\alpha\beta)' = \alpha'\beta + \alpha\beta' \qquad \text{(product rule)}.$$

Proof. For $\alpha = \sum a_n X^n$ and $\beta = \sum b_n X^n$ we have

$$\begin{aligned}(a\alpha + b\beta)' &= \Big(\sum (aa_n + bb_n)X^n\Big)' = \sum n(aa_n + bb_n)X^{n-1} \\ &= a\sum na_n X^{n-1} + b\sum nb_n X^{n-1} = a\alpha' + b\beta'\end{aligned}$$

and therefore

$$\begin{aligned}(\alpha\beta)' &= \Big(\sum_{i,j} a_i b_j X^{i+j}\Big)' = \sum_{i,j} a_i b_j \big(X^{i+j}\big)' = \sum_{i,j} (i+j) a_i b_j X^{i+j-1} \\ &= \sum_{i,j} i a_i b_j X^{i-1+j} + \sum_{i,j} j a_i b_j X^{j-1+i} = \alpha'\beta + \alpha\beta'.\end{aligned}$$

□

Lemma I.11.8. *A root $x \in K$ of $\alpha \in K[X]$ is a multiple root if and only if $\alpha'(x) = 0$.*

Proof. Let $\beta \in K[X]$ with $\alpha = (X - x)\beta$. By the product rule, we have

$$\alpha' = \beta + (X - x)\beta'.$$

Therefore, $\beta(x) = 0$ if and only if $\alpha'(x) = 0$. □

Remark I.11.9. In Lemma I.11.8 one can assume that K is a splitting field of α.

Lemma I.11.10. *For* $\operatorname{char} K = p > 0$*, the map $F\colon K \to K$, $x \mapsto x^p$ is a field homomorphism, which is called the* Frobenius homomorphism.

Proof. Certainly $F(1) = 1^p = 1$. For $x, y \in K$ we also have $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$ and

$$F(x + y) = (x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p = F(x) + F(y),$$

since $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{1\cdot 2\cdot \ldots \cdot k} \equiv 0 \pmod{p}$ for $0 < k < p$. □

Example I.11.11. In $\mathbb{F}_p$, the "false" binomial formula $(a+b)^p = a^p + b^p$ therefore holds.[1] For $a \in \mathbb{N}$ we also have $a^p = (1 + \ldots + 1)^p \equiv 1^p + \ldots + 1^p \equiv a \pmod{p}$ (cf. Euler-Fermat). For $\alpha = \sum a_n X^n \in \mathbb{F}_p[X]$ we have

$$\alpha(X^p) = \sum a_n X^{pn} = \sum a_n^p X^{pn} = \Big(\sum a_n X^n\Big)^p = \alpha^p.$$

Theorem I.11.12. *For every prime power $q \neq 1$, there exists, up to isomorphism, exactly one field $\mathbb{F}_q$ with q elements. Conversely, every finite field is isomorphic to some $\mathbb{F}_q$.*

[1] also called *Freshman's Dream*

Proof. Let $\mathbb{F}_q$ be a splitting field of $X^q - X$ over $\mathbb{F}_p$, where $q = p^n$. Because $(X^q - X)' = qX^{q-1} - 1 = -1$, $X^q - X$ has pairwise distinct roots $x_1, \ldots, x_q$ in $\mathbb{F}_q = \mathbb{F}_p(x_1, \ldots, x_q)$ according to Lemma I.11.8. We show that these roots themselves form a field. For $1 \leq i, j \leq q$, it holds that $(x_i x_j)^q = x_i^q x_j^q = x_i x_j$ and

$$(x_i - x_j)^q = F^n(x_i - x_j) = F^n(x_i) - F^n(x_j) = x_i^q - x_j^q = x_i - x_j,$$

where F is the Frobenius homomorphism. For $x_i \neq 0$, we additionally have $(x_i^{-1})^q = (x_i^q)^{-1} = x_i^{-1}$. Thus $\{x_1, \ldots, x_q\}$ is a subfield of $\mathbb{F}_q$, which must contain the prime field $\mathbb{F}_p$. This shows $\mathbb{F}_q = \mathbb{F}_p(x_1, \ldots, x_q) = \{x_1, \ldots, x_q\}$ and $|\mathbb{F}_q| = q$.

Now let K be another field with $|K| = q$. Then $P(K) \cong \mathbb{F}_p$ and according to Remark I.3.12(ii) it holds that $x^{q-1} = 1$ for all $x \in K^\times$. Thus K is also a splitting field of $X^q - X$ and $K \cong \mathbb{F}_q$ follows by Steinitz. According to Example I.11.4, every finite field is therefore isomorphic to some $\mathbb{F}_q$. □

Example I.11.13. According to Example I.9.17, $\mathbb{F}_4 = \{0, 1, a, b\}$ is (also) the splitting field of $X^2 + X + 1 \in \mathbb{F}_2[X]$. It therefore holds that $a^2 + a + 1 = 0 = b^2 + b + 1$ and one obtains:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Theorem I.11.14. *For every prime power $q = p^n \neq 1$, $\mathbb{F}_p \subseteq \mathbb{F}_q$ is a Galois extension and*

$$\boxed{\mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p) = \mathrm{Aut}(\mathbb{F}_q) = \langle F \rangle \cong C_n}$$

with the Frobenius homomorphism F. The subfields of $\mathbb{F}_q$ are

$$\{x \in \mathbb{F}_q : x^{p^d} = x\} \cong \mathbb{F}_{p^d}$$

with $d \mid n$.

Proof. By construction, $\mathbb{F}_q$ is the splitting field of $X^q - X \in \mathbb{F}_p[X]$ with pairwise distinct roots. According to Artin, $\mathbb{F}_p \subseteq \mathbb{F}_q$ is a Galois extension. According to Lemma I.9.11, $F \in \mathrm{Aut}(\mathbb{F}_q)$. An arbitrary automorphism $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ must fix the prime field $\mathbb{F}_p$ elementwise (since $\sigma(1) = 1$, $\sigma(1+1) = \sigma(1) + \sigma(1) = 1 + 1$, etc.). Thus $\mathrm{Aut}(\mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p)$. For $k \geq 1$, the fixed points of F^k are roots of $X^{p^k} - X$. According to Theorem I.8.29, there are at most p^k such fixed points. In particular, $F^k \neq \mathrm{id}$ for $k < n$. This shows

$$n \leq |\langle F \rangle| \leq |\mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p)| = |\mathbb{F}_q : \mathbb{F}_p| = n$$

and the second claim follows. According to Theorem I.3.34, the subgroups of $\langle F \rangle$ have the form $\langle F^d \rangle$ for $d \mid n$. The last statement therefore follows from the Fundamental Theorem of Galois Theory. □

Example I.11.15. The subfields of $\mathbb{F}_8$ are $\mathbb{F}_2$ and $\mathbb{F}_8$ and not, for instance, $\mathbb{F}_4$.

Remark I.11.16. Note: For $n > 1$, $\mathbb{F}_{p^n} \ncong \mathbb{Z}/p^n\mathbb{Z}$. According to Artin and Theorem I.9.8, there exists an irreducible polynomial $\alpha \in \mathbb{F}_p[X]$ of degree n with $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/(\alpha)$. In this way, one can construct $\mathbb{F}_{p^n}$ explicitly. The following lemma shows how to find suitable α.

Lemma I.11.17. *For every prime power $q = p^n \neq 1$,*

$$X^q - X = \prod_{\substack{\varphi \in \mathbb{F}_p[X] \text{ irreducible} \\ \deg(\varphi) \mid n}} \varphi.$$

Proof. Let $\varphi \in \mathbb{F}_p[X]$ be an irreducible divisor of $X^q - X$. Then φ has a root $x \in \mathbb{F}_q$, because $\mathbb{F}_q$ is the splitting field of $X^q - X$. According to the degree theorem, $\deg \varphi = |\mathbb{F}_p(x) : \mathbb{F}_p|$ is a divisor of $|\mathbb{F}_q : \mathbb{F}_p| = n$.

Conversely, let $\varphi \in \mathbb{F}_p[X]$ be irreducible with $d := \deg \varphi \mid n$. Then $K := \mathbb{F}_p[X]/(\varphi)$ is a field with p^d elements. For $a := X + (\varphi) \in K$, it thus holds that $a^{p^d} = a$ and $a^{p^n} = a^{p^d \cdots p^d} = a$. This shows $X^q - X \equiv 0 \pmod{\varphi}$ and $\varphi \mid X^q - X$. In the case $\varphi^2 \mid X^q - X$, it would follow that $\varphi \mid (X^q - X)' = -1$ by the product rule. The claim now follows from the unique factorization in $\mathbb{F}_p[X]$ (Theorem I.8.24). □

Example I.11.18. In $\mathbb{F}_2[X]$, it holds that

$$\frac{X^8 - X}{X(X+1)} = \frac{X^7 - 1}{X - 1} = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = (X^3 + X + 1)(X^3 + X^2 + 1).$$

On the right are the irreducible polynomials of degree 3.

Definition I.11.19. A field K is called *perfect*, if $\operatorname{char} K = 0$ or the Frobenius homomorphism is surjective (cf. Exercise I.63).

Theorem I.11.20. *For every field K, the following statements are equivalent:*

(1) K is perfect.

(2) For every irreducible polynomial $\alpha \in K[X]$, $\gcd(\alpha, \alpha') = 1$.

(3) For every irreducible polynomial $\alpha \in K[X]$, $\alpha' \neq 0$.

(4) Every irreducible polynomial in $K[X]$ has only simple roots in its splitting field.

Proof. We first show the equivalence of (2), (3) and (4). For every irreducible polynomial $\alpha \in K[X]$, it holds that $\gcd(\alpha, \alpha') \in \{1, \alpha\}$. Due to $\deg \alpha' < \deg \alpha$, (2) is equivalent to (3). For every root x of α in a splitting field, α is the minimal polynomial of x. Therefore, $\alpha'(x) = 0$ if and only if $\alpha' = 0$. With Lemma I.11.8, it follows that (3)⇔(4).

Now let K be perfect. In the case $\operatorname{char} K = 0$, certainly $\alpha' \neq 0$. So let $\operatorname{char} K = p > 0$ and the Frobenius homomorphism F be surjective. In the case $\alpha' = 0$, α has the form $\alpha = \sum_{i=0}^{n} a_i X^{ip}$ with $a_0, \ldots, a_n \in K$. Since F is surjective, there exist $b_0, \ldots, b_n \in K$ with $b_i^p = F(b_i) = a_i$ for $i = 0, \ldots, n$. It follows that

$$\alpha = \sum b_i^p X^{ip} = \sum (b_i X^i)^p \overset{\text{I.11.11}}{=} \left(\sum b_i X^i \right)^p$$

in contradiction to the irreducibility of α. This shows (1)⇒(3).

Finally, let us assume (4). To show (1), we can assume $\operatorname{char} K = p > 0$. Let $a \in K$ and x be a root of $X^p - a$ in a splitting field. Then $(X - x)^p = X^p - x^p = X^p - a$ holds. Thus every irreducible divisor $\alpha \in K[X]$ of $X^p - a$ has the form $\alpha = (X - x)^n$. According to (4), $n = 1$ holds, i. e. $x \in K$. This shows $a = x^p = F(x)$ and F is surjective. □

Remark I.11.21.

(i) According to Theorem I.8.31, $\mathbb{F}_{p^n}^\times$ is cyclic. We investigate the structure of the abelian group $(\mathbb{F}_{p^n}, +)$. Because of $\operatorname{char} \mathbb{F}_{p^n} = p$, it holds that $\underbrace{a + \ldots + a}_{p\text{-times}} = 0$ for all $a \in \mathbb{F}_{p^n}$. From the fundamental theorem of finite abelian groups, it follows that

$$(\mathbb{F}_{p^n}, +) \cong C_p \times \ldots \times C_p = C_p^n.$$

Groups of this type are generally called *elementary abelian* p-groups. A prominent example is V_4.

(ii) As is well known, computers calculate with bits, i.e., elements of $\mathbb{F}_2$. A byte consists of eight bits and can therefore be understood as an element of $\mathbb{F}_{2^8}$. This is of practical relevance for CD players and QR codes (see chapter III.12).

I.12 Cyclotomic Fields

Remark I.12.1. Obviously, $\mathbb{F}_q$ is the splitting field of $X^{q-1}-1$ over $\mathbb{F}_p$. In this section, we investigate the corresponding fields in characteristic 0.

Theorem I.12.2. *Let* $\operatorname{char} K = 0$.

(i) For every splitting field L of $\alpha \in K[X] \setminus K$, $K \subseteq L$ is a Galois extension.

(ii) Every finite field extension $K \subseteq L$ lies in a Galois extension $K \subseteq M$, i. e. $L \subseteq M$.

Proof.

(i) Let $\alpha = \alpha_1^{n_1} \dots \alpha_k^{n_k}$ be the decomposition into pairwise distinct irreducible polynomials $\alpha_1, \dots, \alpha_k \in K[X]$. According to Theorem I.11.20, each α_i has only simple roots. Because $\gcd(\alpha_i, \alpha_j) = 1$ for $i \neq j$, $\beta := \alpha_1 \dots \alpha_k$ has pairwise distinct roots in L. Obviously, L is also the splitting field of β and the assertion follows by Artin.

(ii) Let $x_1, \dots, x_n$ be a K-basis of L. Let $\mu_1, \dots, \mu_n \in K[X]$ be the minimal polynomials of $x_1, \dots, x_n$ and let M be a splitting field of $\mu_1 \dots \mu_n$. According to (i), $K \subseteq M$ is a Galois extension and $L = K(x_1, \dots, x_n) \subseteq M$. □

Theorem I.12.3 (Primitive Element Theorem)**.** *For every finite field extension $K \subseteq L$ with* $\operatorname{char} K = 0$*, there exists an $x \in L$ with $L = K(x)$. One calls x a* primitive element.

Proof. According to Theorem I.12.2, there exists a Galois extension $K \subseteq M$ with $L \subseteq M$. According to the Fundamental Theorem of Galois Theory, there are only finitely many fields between K and M. Therefore, there are also only finitely many fields $M_1, \dots, M_n$ with $K \subseteq M_i \subsetneq L$. According to Lemma I.10.1, there exists an $x \in L \setminus \bigcup M_i$. Then $K(x) \neq M_i$ for $i = 1, \dots, n$ and it follows that $K(x) = L$. □

Remark I.12.4. According to Theorem I.8.31, the Primitive Element Theorem also holds for finite fields, but not for arbitrary fields of positive characteristic.

Example I.12.5. Let $K := \mathbb{Q}(\sqrt{2}, \sqrt{3})$. According to Example I.10.12, $\sqrt{2} + \sqrt{3}$ is changed by all non-trivial Galois automorphisms in $\operatorname{Gal}(K|\mathbb{Q})$. This shows $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = K$ and $\sqrt{2}+\sqrt{3}$ is a primitive element.

Definition I.12.6. Let $n \in \mathbb{N}$. One calls $\zeta \in K$ an *n-th root of unity*, if $\zeta^n = 1$. In the case $|\langle \zeta \rangle| = n$, ζ is called *primitive*. The splitting field $\mathbb{Q}_n$ of $X^n - 1$ over $\mathbb{Q}$ is called the *n-th cyclotomic field*.

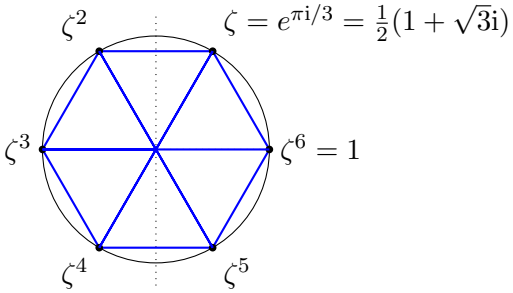
Remark I.12.7.

(i) Because of $(X^n-1)' = nX^{n-1} \neq 0$, X^n-1 has only simple roots in $\mathbb{Q}_n$ (Lemma I.11.8), i. e. there are exactly n n-th roots of unity. These obviously form a group $G \leq \mathbb{Q}_n^\times$, which is cyclic according to Theorem I.8.31, say $G = \langle\zeta\rangle$. The primitive n-th roots of unity have the form ζ^k with $\gcd(n,k) = 1$ according to Lemma I.3.7. The polynomial

$$\Phi_n := \prod_{\substack{1\leq k\leq n,\\ \gcd(n,k)=1}} (X-\zeta^k) \in \mathbb{Q}_n[X]$$

is called the *n-th cyclotomic polynomial*. It holds that $\deg \Phi_n = \varphi(n)$ with Euler's φ-function.

(ii) As is well known, $e^{2\pi \mathrm{i}/n} \in \mathbb{C}$ is a primitive n-th root of unity. One can therefore identify $\mathbb{Q}_n$ with $\mathbb{Q}(e^{2\pi\mathrm{i}/n}) \subseteq \mathbb{C}$ (Steinitz). The numbers $e^{2\pi\mathrm{i}k/n}$ with $k = 1,\dots,n$ divide the unit circle in the complex plane into n equal parts, i. e. they form a regular n-gon. Example $n = 6$:



(iii) In characteristic $p > 0$, 1 is the only p-th root of unity, because $X^p - 1 = (X-1)^p$.

Example I.12.8. It holds that $\mathbb{Q}_1 = \mathbb{Q}_2 = \mathbb{Q}$ and $\Phi_1 = X-1$, $\Phi_2 = X+1$ as well as

$$\Phi_3 = (X - e^{2\pi\mathrm{i}/3})(X - e^{-2\pi\mathrm{i}/3}) = X^2 + X + 1.$$

For $n \mid m$, it holds more generally that $\mathbb{Q}_n \subseteq \mathbb{Q}_m$, because every n-th root of unity is also an m-th root of unity.

Lemma I.12.9. *For $n \in \mathbb{N}$, $X^n - 1 = \prod_{d\mid n} \Phi_d$. In particular, $\Phi_n \in \mathbb{Z}[X]$ holds.*

Proof. Let $\zeta \in \mathbb{Q}_n$ be a primitive n-th root of unity. For $d \mid n$, then ζ^d is a primitive n/d-th root of unity (Lemma I.3.7). This shows

$$X^n - 1 = \prod_{i=1}^{n} (X-\zeta^i) = \prod_{d\mid n} \prod_{\substack{1\leq k\leq n/d\\ \gcd(k,n/d)=1}} (X-\zeta^{dk}) = \prod_{d\mid n} \Phi_{n/d} = \prod_{d\mid n} \Phi_d.$$

For the second assertion, we argue by induction on n. For $n = 1$, $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Now let $n > 1$ and assume the assertion is proven for $d < n$. Then

$$\alpha := \prod_{\substack{d\mid n\\ d\neq n}} \Phi_d \in \mathbb{Z}[X]$$

is monic. Since the polynomial division $\Phi_n = (X^n-1)/\alpha$ is exact in $\mathbb{Q}_n[X]$, it is also exact in $\mathbb{Q}[X]$ (the uniquely determined remainder of the division does not depend on the field), i. e. $\Phi_n \in \mathbb{Q}[X]$. Since α and Φ_n are monic, it follows that $\Phi_n \in \mathbb{Z}[X]$ from Corollary I.8.51. □

Example I.12.10. With Lemma I.12.9, cyclotomic polynomials can be calculated recursively. For $p \in \mathbb{P}$ and $n \in \mathbb{N}$, it holds that

$$\Phi_{p^n} = \frac{X^{p^n} - 1}{\prod_{0 \le d < n} \Phi_{p^d}} = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \ldots + X^{p^{n-1}} + 1.$$

In the case $n = 1$, $\Phi_p = X^{p-1} + X^{p-2} + \ldots + X + 1$ is irreducible according to Example I.8.55. We show that this also holds in general.

Theorem I.12.11 (Gauss)**.** *Cyclotomic polynomials are irreducible in* $\mathbb{Q}[X]$.

Proof. Let $\Phi_n = \alpha\beta$ with $\alpha, \beta \in \mathbb{Q}[X]$ and α irreducible. Since Φ_n and α are monic, β is also monic. From Lemma I.12.9 and Corollary I.8.51 it follows that $\alpha, \beta \in \mathbb{Z}[X]$. We must show $\alpha = \Phi_n$. Let $\zeta \in \mathbb{Q}_n$ be a root of α. Then ζ is also a root of Φ_n and thus a primitive n-th root of unity. Since every root of Φ_n has the form ζ^k with $\gcd(n, k) = 1$, it suffices to show $\alpha(\zeta^k) = 0$. By induction on the number of prime factors of k, we may assume that $k = p$ itself is a prime number (which does not divide n).

Assume $\alpha(\zeta^p) \neq 0$. Then $\beta(\zeta^p) = 0$ and $\beta(X^p) \in \mathbb{Z}[X]$ has the root ζ. Since α is the minimal polynomial of ζ over $\mathbb{Q}$, it follows that $\alpha \mid \beta(X^p)$ in $\mathbb{Q}[X]$. Thus, let $\beta(X^p) = \alpha\gamma$ with $\gamma \in \mathbb{Q}[X]$. Since α is monic, it even holds that $\gamma \in \mathbb{Z}[X]$ by Corollary I.8.51. For the reduction modulo p (Lemma I.8.56), we have

$$\overline{\alpha} \cdot \overline{\gamma} = \overline{\alpha\gamma} = \overline{\beta(X^p)} \overset{\text{I.11.11}}{=} \overline{\beta}^p.$$

For an irreducible divisor $\overline{\delta}$ of $\overline{\alpha}$, it then follows that $\overline{\delta} \mid \overline{\beta}$ (Theorem I.8.24) and

$$\overline{\delta}^2 \mid \overline{\alpha\beta} = \overline{\Phi_n} \mid X^n - \overline{1}.$$

By the product rule, it follows that $\overline{\delta} \mid (X^n - \overline{1})' = \overline{n}X^{n-1} \neq 0$ because $p \nmid n$. Thus $\overline{\delta} = X$ and one obtains the contradiction $\overline{\delta} \nmid X^n - \overline{1}$. □

Theorem I.12.12. *For* $n \in \mathbb{N}$, $\mathbb{Q} \subseteq \mathbb{Q}_n$ *is a Galois extension with* $\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. *For every subfield* $L \subseteq \mathbb{Q}_n$, $\mathbb{Q} \subseteq L$ *is a Galois extension with an abelian Galois group.*

Proof. According to Theorem I.12.2, $\mathbb{Q} \subseteq \mathbb{Q}_n$ is a Galois extension. Let $\zeta \in \mathbb{Q}_n$ be a primitive n-th root of unity and $\sigma \in G := \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$. Then $\sigma(\zeta)$ is also a root of $X^n - 1$, i.e., $\sigma(\zeta) \in \langle\zeta\rangle$. Because $\mathbb{Q}_n = \mathbb{Q}(\zeta)$, σ is uniquely determined by $\sigma(\zeta)$. By restriction, one obtains a monomorphism

$$\Gamma\colon G \to \mathrm{Aut}(\langle\zeta\rangle) \overset{\text{I.7.27}}{\cong} (\mathbb{Z}/n\mathbb{Z})^\times.$$

According to Gauss, Φ_n is the minimal polynomial of ζ over $\mathbb{Q}$. This shows

$$|G| = |\mathbb{Q}_n : \mathbb{Q}| = \deg \Phi_n = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

Thus Γ is an isomorphism.

Now let $L \subseteq \mathbb{Q}_n$ be a subfield. Then certainly $\mathbb{Q} = P(\mathbb{Q}_n) \subseteq L$. According to the first part of the proof, G is abelian. In particular, every subgroup of G is normal. The second assertion therefore follows from the Fundamental Theorem of Galois Theory. □

Example I.12.13. With Theorems I.7.24 and I.8.34, the structure of $G = \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ can be determined. This yields the subgroups of G and the subfields of $\mathbb{Q}_n$ (cf. Example I.5.14). For example,

$$\mathrm{Gal}(\mathbb{Q}_{12}|\mathbb{Q}) \cong (\mathbb{Z}/12\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \cong C_2 \times C_2.$$

The subgroups of order 2 of $(\mathbb{Z}/12\mathbb{Z})^\times$ are $\langle -1 + 12\mathbb{Z}\rangle$, $\langle 5 + 12\mathbb{Z}\rangle$ and $\langle -5 + 12\mathbb{Z}\rangle$. The corresponding subfields of $\mathbb{Q}_{12}$ are

$$\mathbb{Q}(\zeta + \bar{\zeta}) = \mathbb{Q}(\sqrt{3}), \qquad \mathbb{Q}(\zeta^3) = \mathbb{Q}_4 = \mathbb{Q}(\mathrm{i}), \qquad \mathbb{Q}(\zeta^2) = \mathbb{Q}_6 = \mathbb{Q}(\sqrt{3}\mathrm{i}) = \mathbb{Q}_3$$

(cf. Remark I.10.13).

Theorem I.12.14. *For $n, m \in \mathbb{N}$, $\mathbb{Q}_n \cap \mathbb{Q}_m = \mathbb{Q}_{\gcd(n,m)}$ and $\mathbb{Q}_n\mathbb{Q}_m = \mathbb{Q}_{\mathrm{lcm}(n,m)}$.*

Proof. We consider $\mathbb{Q}_n$ and $\mathbb{Q}_m$ as subfields of $\mathbb{Q}_k$ with $k := \mathrm{lcm}(n, m)$. In this way, the compositum $\mathbb{Q}_n\mathbb{Q}_m \subseteq \mathbb{Q}_k$ is well-defined. Let $G_1 := (\mathbb{Z}/k\mathbb{Z})^\times$ and $G_d := \{l + k\mathbb{Z} \in G_1 : l \equiv 1 \pmod d\} \leq G_1$ for $d \mid k$. According to Theorem I.12.12, $\mathbb{Q}_d = \mathbb{Q}_k^{G_d}$ for $d \mid k$. Obviously, $G_n \cap G_m = G_k = 1$ and

$$\mathbb{Q}_n\mathbb{Q}_m = \mathbb{Q}_k^{G_n}\mathbb{Q}_k^{G_m} \overset{\text{I.10.15}}{=} \mathbb{Q}_k^{G_n \cap G_m} = \mathbb{Q}_k$$

With $g := \gcd(n, m)$, we have $\langle G_n, G_m\rangle = G_nG_m \leq G_g$. For $l + k\mathbb{Z} \in G_g$, conversely, there exist $a, b \in \mathbb{Z}$ such that $l + k\mathbb{Z} = 1 + an + bm + k\mathbb{Z} = (1 + an + k\mathbb{Z})(1 + bm + k\mathbb{Z}) \in G_nG_m$. Thus

$$\mathbb{Q}_n \cap \mathbb{Q}_m = \mathbb{Q}_k^{G_n} \cap \mathbb{Q}_k^{G_m} \overset{\text{I.10.15}}{=} \mathbb{Q}_k^{G_nG_m} = \mathbb{Q}_k^{G_g} = \mathbb{Q}_g. \qquad \square$$

Lemma I.12.15. *Let $n, a \in \mathbb{N}$ and p be a prime divisor of $\Phi_n(a)$. Then $p \mid n$ or $n \mid p - 1$.*

Proof. Because of $\Phi_n(a + p) \equiv \Phi_n(a) \pmod p$, we may assume $a > 1$. According to Lemma I.12.9, $p \mid \Phi_n(a) \mid (a^n - 1)$, so $a^n \equiv 1 \pmod p$. The order k of $a + p\mathbb{Z} \in \mathbb{F}_p^\times$ therefore divides n (Lemma I.3.7). In the case $k = n$, $n \mid p - 1$ follows from Lagrange. So let $k < n$ and $b := a^k \equiv 1 \pmod p$. Because of $a^k > 1$, it holds that

$$\frac{n}{k} \equiv 1 + b + \ldots + b^{n/k-1} = \frac{b^{n/k} - 1}{b - 1} = \frac{a^n - 1}{a^k - 1} = \prod_{\substack{d \mid n \\ d \nmid k}} \Phi_d(a) \equiv 0 \pmod p.$$

It follows that $p \mid \frac{n}{k} \mid n$. $\square$

Remark I.12.16. The following result is a special case of Dirichlet's prime number theorem: For $\gcd(a, n) = 1$, there are infinitely many prime numbers in $a + n\mathbb{Z}$ (some special cases are discussed in Exercise I.5 and in the appendix; a general proof can be found in my Number Theory notes).[1]

Theorem I.12.17. *For $n \in \mathbb{N}$, there are infinitely many prime numbers $p \equiv 1 \pmod n$.*

Proof. Let $p_1, \ldots, p_s$ be prime numbers with $p_i \equiv 1 \pmod n$ for $i = 1, \ldots, s$ (the case $s = 0$ is allowed). For $m := np_1 \ldots p_s$, there exists a $k \in \mathbb{N}$ with $\Phi_m(km) > 1$, because Φ_m, as a monic polynomial, induces an unbounded function $\mathbb{R} \to \mathbb{R}$. Let p be a prime divisor of $\Phi_m(km)$. Because of $p \mid ((km)^m - 1)$, we have $p \nmid m$ and Lemma I.12.15 shows $p \equiv 1 \pmod m$. Then also $p \equiv 1 \pmod n$. Because of $p \nmid m$, we have found a new prime number of the desired form. $\square$

[1] The prime numbers are even distributed uniformly among the primitive residue classes modulo n. A randomly chosen prime number therefore ends with equal probability on one of the digits 1, 3, 7 or 9.

Remark I.12.18. One can show that for every finite group G, there exists a number field K with $\mathrm{Gal}(K|\mathbb{Q}) \cong G$ (Theorem A.6.4). The so far unsolved *inverse Galois problem* asks whether there always exists a Galois extension $\mathbb{Q} \subseteq K$ with this property. SHAFAREVICH proved this for solvable groups. We treat abelian groups and later symmetric groups (Theorem II.11.48).

Theorem I.12.19. *For every finite abelian group G, there exists a Galois extension $\mathbb{Q} \subseteq K$ with $\mathrm{Gal}(K|\mathbb{Q}) \cong G$.*

Proof. According to the fundamental theorem of finite abelian groups, there exist $d_1, \ldots, d_n \in \mathbb{N}$ with $G \cong C_{d_1} \times \ldots \times C_{d_n}$. According to Theorem I.12.17, there exist pairwise distinct $p_1, \ldots, p_n \in \mathbb{P}$ with $p_i \equiv 1 \pmod{d_i}$ for $i = 1, \ldots, n$. Because of $d_i \mid p_i - 1 = \varphi(p_i)$, the group $(\mathbb{Z}/p_i\mathbb{Z})^\times$ has a factor group of order d_i (Theorem I.3.34), i. e. there is an epimorphism $f_i \colon (\mathbb{Z}/p_i\mathbb{Z})^\times \to C_{d_i}$. Then also

$$\begin{aligned}(\mathbb{Z}/p_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_n\mathbb{Z})^\times &\to C_{d_1} \times \ldots \times C_{d_n},\\ (x_1, \ldots, x_n) &\mapsto (f_1(x_1), \ldots, f_n(x_n))\end{aligned}$$

is an epimorphism. With Theorem I.12.12 and Theorem I.7.24, one obtains an epimorphism

$$\Gamma \colon \mathrm{Gal}(\mathbb{Q}_{p_1 \ldots p_n}|\mathbb{Q}) \cong (\mathbb{Z}/p_1 \ldots p_n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_n\mathbb{Z})^\times \to C_{d_1} \times \ldots \times C_{d_n} \cong G.$$

Let $N := \mathrm{Ker}(\Gamma)$ and $K := \mathbb{Q}^N_{p_1 \ldots p_n}$. According to the fundamental theorem of Galois theory, it then follows that

$$\mathrm{Gal}(K|\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}_{p_1 \ldots p_n}|\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}_{p_1 \ldots p_n}|K) \cong \mathrm{Gal}(\mathbb{Q}_{p_1 \ldots p_n}|\mathbb{Q})/N \cong \Gamma(\mathrm{Gal}(\mathbb{Q}_{p_1 \ldots p_n}|\mathbb{Q})) \cong G. \qquad \square$$

Example I.12.20. The proof yields $\mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^{-1})|\mathbb{Q}) \cong C_3$ with $\zeta := e^{2\pi \mathrm{i}/7}$ (choose $p_1 = 7$).

Theorem I.12.21 (KRONECKER-WEBER)**.** *Let $\mathbb{Q} \subseteq K$ be a Galois extension with abelian Galois group. Then $K \subseteq \mathbb{Q}_n$ for some $n \geq 1$.*

Proof. Number theory.[2] $\square$

Remark I.12.22. We consider the smallest special case with the help of a *Gauss sum* (see Definition A.1.5).

Theorem I.12.23. *Let K be a quadratic number field, i. e. $|K : \mathbb{Q}| = 2$. Then $K \subseteq \mathbb{Q}_n$ for some $n \in \mathbb{N}$.*

Proof. Let $x \in K \setminus \mathbb{Q}$ with minimal polynomial $\mu \in \mathbb{Q}[X]$. Then $K = \mathbb{Q}(x)$ and $\mu = X^2 + aX + b$ with $a, b \in \mathbb{Q}$. For $d := a^2/4 - b \in \mathbb{Q}$, we have $x = -a/2 \pm \sqrt{d}$ according to the p-q-formula. This shows

$$K = \mathbb{Q}\Big(x + \frac{a}{2}\Big) = \mathbb{Q}(\sqrt{d}).$$

Because of $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(e\sqrt{d}) = \mathbb{Q}(\sqrt{e^2 d})$ for all $e \in \mathbb{N}$, we can assume $d \in \mathbb{Z}$. We must show $\sqrt{d} \in \mathbb{Q}_{n_d}$ for some $n_d \in \mathbb{N}$. If this is already shown for $d > 0$, then

$$\mathbb{Q}(\sqrt{-d}) \subseteq \mathbb{Q}(\mathrm{i}, \sqrt{d}) \subseteq \mathbb{Q}_{4n_d}$$

[2] See for example Section 17.5 in [A. Leutbecher, *Zahlentheorie*, Springer, Berlin, 1996]

holds because of $\mathrm{i} \in \mathbb{Q}_4 \subseteq \mathbb{Q}_{4n_d}$. We can therefore assume $d > 0$. If the assertion holds for $e, f \in \mathbb{N}$, then it also holds for $d = ef$, since $\mathbb{Q}(\sqrt{ef}) \subseteq \mathbb{Q}(\sqrt{e}, \sqrt{f}) \subseteq \mathbb{Q}_{n_e n_f}$. We can therefore assume $p := d \in \mathbb{P}$.

First let $p > 2$ and let $\zeta \in \mathbb{Q}_p$ be a primitive p-th root of unity. For $1 \leq k, l \leq q := \frac{p-1}{2}$ we have

$$2k \equiv \pm 2l \pmod{p} \overset{\text{I.2.26}}{\iff} k \equiv \pm l \pmod{p} \iff k = l.$$

With Example I.12.10 it follows

$$p = \Phi_p(1) = \prod_{k=1}^{p-1}(1-\zeta^k) = \prod_{k=1}^{q}(1-\zeta^{2k})(1-\zeta^{-2k}) = \prod_{k=1}^{q}(\zeta^{-k}-\zeta^k)(\zeta^k-\zeta^{-k}) = (-1)^q \prod_{k=1}^{q}(\zeta^k-\zeta^{-k})^2.$$

With $\epsilon := (-1)^q$ it follows

$$\sqrt{p} = \sqrt{\epsilon}\sqrt{\epsilon p} = \pm\sqrt{\epsilon}\prod_{k=1}^{q}(\zeta^k-\zeta^{-k}) \in \mathbb{Q}_{4p}.$$

Finally, let $p = 2$ and $\zeta \in \mathbb{Q}_8$ be a primitive 8-th root of unity. Then $\zeta^2 = \pm\mathrm{i}$, $(\zeta+\zeta^{-1})^2 = \zeta^2+\zeta^{-2}+2 = 2$ and $\sqrt{2} = \pm(\zeta+\zeta^{-1}) \in \mathbb{Q}_8$. □

I.13 Algebraic Closure

Remark I.13.1. By adding an identity element, the *semigroup* $\mathbb{N}$ becomes the *monoid* $\mathbb{N}_0$. If one adds inverse elements, one arrives at the group $\mathbb{Z}$, which is simultaneously an integral domain. Formation of the quotient field turns $\mathbb{Z}$ into the field $\mathbb{Q}$. In analysis, one *completes* $\mathbb{Q}$ with respect to the Euclidean metric and obtains $\mathbb{R}$ from it. In this section, we construct (among other things) the *algebraic closure* $\mathbb{C}$ of $\mathbb{R}$. In doing so, however, one loses the *ordering* of $\mathbb{R}$.[1] By giving up the commutativity of multiplication, one can extend $\mathbb{C}$ to the *quaternion skew field* $\mathbb{H}$ (Exercise I.50). Finally, one arrives from $\mathbb{H}$ at the *octonions* $\mathbb{O}$, for which multiplication is no longer associative.

$$\mathbb{N}_0 \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H} \subseteq \mathbb{O}$$

Lemma I.13.2. *If $K \subseteq L \subseteq M$ are algebraic field extensions, then $K \subseteq M$ is also algebraic.*

Proof. Let $x \in M$ be arbitrary. Since x is algebraic over L, there exist $y_0, \ldots, y_n \in L$ (not all 0) with $\sum y_i x^i = 0$. By assumption, $y_0, \ldots, y_n$ are algebraic over K. Thus, it holds that

$$|K(y_0, \ldots, y_n) : K| = |K(y_0, \ldots, y_n) : K(y_0, \ldots, y_{n-1})| \ldots |K(y_0) : K| < \infty.$$

Now x is algebraic over $\widehat{K} := K(y_0, \ldots, y_n)$ and it follows that

$$|K(x) : K| \leq |\widehat{K}(x) : K| = |\widehat{K}(x) : \widehat{K}||\widehat{K} : K| < \infty.$$

Thus x is algebraic over K (Theorem I.9.6). □

Remark I.13.3. The corresponding statement of Lemma I.13.2 does not hold for Galois extensions: According to Exercise I.57, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ are Galois extensions, but not $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$, because $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ (cf. Example I.10.8).

Theorem I.13.4. *Let $K \subseteq L$ be a field extension. Then the algebraic elements of L over K form a field M with $K \subseteq M \subseteq L$.*

Proof. Since the inclusion $K \subseteq M \subseteq L$ is trivial, it only remains to show that M is a field. For $x, y \in M$, we have $x - y \in K(x, y)$ as well as $xy^{-1} \in K(x, y)$ if $y \neq 0$. Because of

$$|K(x, y) : K| = |K(x, y) : K(x)||K(x) : K| < \infty$$

it follows that $x - y, xy^{-1} \in M$ (Theorem I.9.6). This shows the claim. □

Definition I.13.5.

(i) K is called *algebraically closed*, if every $\alpha \in K[X] \setminus K$ has a root in K. According to Lemma I.8.27, α then even splits into linear factors, i. e. α has exactly $\deg \alpha$ roots in K counted with multiplicities.

[1] The relation $\leq$ cannot be extended to $\mathbb{C}$ such that $z > 0 \Rightarrow z^2 > 0$ holds for all $z \in \mathbb{C}$.

(ii) An algebraically closed field $\overline{K} \supseteq K$ is called an *algebraic closure* of K, if the field extension $K \subseteq \overline{K}$ is algebraic.

Remark I.13.6. If K is finite, then the polynomial $1 + \prod_{x \in K}(X - x) \in K[X]$ has no root in K. An algebraically closed field must therefore be infinite.

Theorem I.13.7 (Fundamental Theorem of Algebra)**.** *The field $\mathbb{C}$ is algebraically closed.*

Proof. Let $\alpha \in \mathbb{C}[X] \setminus \mathbb{C}$ and $\beta := \alpha\overline{\alpha} \in \mathbb{R}[X]$, where $\overline{\alpha}$ denotes the complex conjugate polynomial. If β has a root $z \in \mathbb{C}$, then $\alpha(z) = 0$ or $\alpha(\overline{z}) = \overline{\alpha}(z) = 0$. We can therefore assume $\alpha \in \mathbb{R}[X]$.

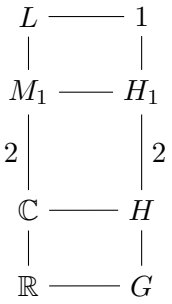
Let L be a splitting field of α over $\mathbb{C}$. We assume indirectly that $L \neq \mathbb{C}$. Obviously, L is also a splitting field of $(X^2+1)\alpha$ over $\mathbb{R}$. According to Theorem I.12.2, $\mathbb{R} \subseteq L$ is a Galois extension because $\operatorname{char} \mathbb{R} = 0$. Let $G := \operatorname{Gal}(L|\mathbb{R})$, $S \in \operatorname{Syl}_2(G)$ and $M := L^S$. By the primitive element theorem, there exists an $x \in M$ with $M = \mathbb{R}(x)$. For the minimal polynomial μ of x over $\mathbb{R}$, it then holds that

$$\deg \mu = |M : \mathbb{R}| = |L^S : \mathbb{R}| = |G : S| \equiv 1 \pmod 2$$

according to the fundamental theorem of Galois theory. The continuous function $\mu\colon \mathbb{R} \to \mathbb{R}$ therefore satisfies $\lim_{r \to \pm\infty} \mu(r) = \pm\infty$. By the intermediate value theorem of analysis, μ has a root in $\mathbb{R}$, i. e. $\deg \mu = 1$ and $G = S$.

Let $H := \operatorname{Gal}(L|\mathbb{C}) \leq G$. Because $L \neq \mathbb{C}$, $H \neq 1$. As a 2-group, H has a subgroup H_1 of index 2 (Sylow). For $M_1 := L^{H_1}$, we then have $\mathbb{C} \subseteq M_1$ and

$$|M_1 : \mathbb{C}| = |H : H_1| = 2.$$



For $z \in M_1 \setminus \mathbb{C}$, we have $M_1 = \mathbb{C}(z)$. Thus, the minimal polynomial of z has the form $X^2 + aX + b \in \mathbb{C}[X]$ (cf. Theorem I.12.23). If we can show that $w := a^2/4 - b \in \mathbb{C}$ has a square root $\sqrt{w} \in \mathbb{C}$, then the contradiction $z \in \mathbb{C}$ follows (p-q-formula). Let $w = x + y\mathrm{i}$ with $x, y \in \mathbb{R}$ and wlog. $y \neq 0$. Then

$$\sqrt{\frac{1}{2}\big(x + \sqrt{x^2+y^2}\big)} + \frac{y}{|y|}\sqrt{\frac{1}{2}\big(-x + \sqrt{x^2+y^2}\big)}\mathrm{i} \in \mathbb{C}$$

is a root of w (verify by calculation). □

Remark I.13.8.

(i) A shorter proof with a bit more analysis can be found in Theorem A.4.2.

(ii) (Partial fraction decomposition) According to Theorem I.13.7, every irreducible polynomial in $\mathbb{C}[X]$ has degree 1. The prime factorization of a monic polynomial $\alpha \in \mathbb{C}[X]$ therefore has the form $\alpha = (X - x_1)^{a_1} \ldots (X - x_n)^{a_n}$ with pairwise distinct roots $x_1, \ldots, x_n \in \mathbb{C}$. Since $\alpha/(X - x_i)^{a_1}, \ldots, \alpha/(X - x_n)^{a_n}$ are coprime, there exist $\beta_1, \ldots, \beta_n \in \mathbb{C}[X]$ with $\beta_1\alpha/(X - x_i)^{a_1} + \ldots + \beta_n\alpha/(X - x_n)^{a_n} = 1$. Euclidean division yields $\beta_i = \gamma_i(X - x_i)^{a_i} + \rho_i$ with $\deg \rho_i < a_i$ for $i = 1, \ldots, n$. A comparison of degrees of

$$(\gamma_1 + \ldots + \gamma_n)\alpha + \rho_1\frac{\alpha}{(X - x_1)^{a_1}} + \ldots + \rho_n\frac{\alpha}{(X - x_n)^{a_n}} = 1$$

shows $\gamma_1 + \ldots + \gamma_n = 0$, i. e.

$$\frac{1}{\alpha} = \frac{\rho_1}{(X-x_1)^{a_1}} + \ldots + \frac{\rho_n}{(X-x_n)^{a_n}} \in \mathbb{C}(X).$$

Since $1, (X-x_i), (X-x_i)^2, \ldots$ is a $\mathbb{C}$-basis of $\mathbb{C}[X]$, there exist $c_{i1}, \ldots, c_{ia_i} \in \mathbb{C}$ with $\rho_i = c_{i1}(X-x_i)^{a_i-1} + \ldots + c_{ia_i}$. Altogether one obtains the *partial fraction decomposition*

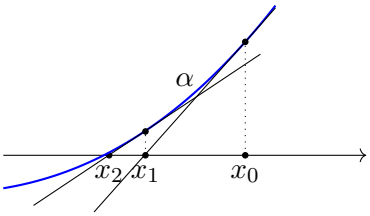
$$\frac{1}{\alpha} = \sum_{i=1}^{n} \sum_{j=1}^{a_i} \frac{c_{ij}}{(X-x_i)^j}.$$

This is useful for the integration of rational functions.

(iii) We will show later that the roots of a polynomial cannot, in general, be calculated exactly. In practice, there are approximation methods such as that of Newton:

Given: $\alpha \in \mathbb{R}[X]$, x_0 = estimate of a root of α.
Iterate:

$$x_{n+1} := x_n - \frac{\alpha(x_n)}{\alpha'(x_n)} \qquad (n \geq 0).$$



Example I.13.9. Let $\alpha := X^5 - 4X + 2$ and $x_0 := 0{,}5$. With $\alpha' = 5X^4 - 4$ one obtains $x_1 = 0{,}50847\ldots$ and $x_2 = 0{,}50849948\ldots$ (all given decimal places are correct).

Theorem I.13.10. *The field $\mathbb{Q}$ possesses an algebraic closure $\overline{\mathbb{Q}} \subseteq \mathbb{C}$.*

Proof. Let $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ be the field of algebraic elements in $\mathbb{C}$ over $\mathbb{Q}$ (Theorem I.13.4). Then $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ is certainly an algebraic field extension. According to the fundamental theorem of algebra, every polynomial $\alpha \in \overline{\mathbb{Q}}[X] \setminus \overline{\mathbb{Q}}$ has a root $x \in \mathbb{C}$. Obviously x is algebraic over $\overline{\mathbb{Q}}$ and according to Lemma I.13.2, x is also algebraic over $\mathbb{Q}$. This shows $x \in \overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}}$ is algebraically closed. □

Remark I.13.11. As already mentioned in Example I.9.2, $\overline{\mathbb{Q}}$ is countable and the set of transcendental numbers $\mathbb{C} \setminus \overline{\mathbb{Q}}$ is uncountable. We now construct a transcendental number.

Theorem I.13.12 (Liouville)**.** *The real number $\xi := \sum_{k=1}^{\infty} 10^{-k!} = 0{,}1100010\ldots$ is transcendental.*

Proof. [2] Certainly ξ is real as the limit of a Cauchy sequence. Suppose indirectly $\xi \in \overline{\mathbb{Q}}$ with minimal polynomial $\mu \in \mathbb{Q}[X]$. Let $a \in \mathbb{N}$ with $\alpha := a\mu = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$. Choose $m \in \mathbb{N}$ with

$$\sum_{i=1}^{n} |a_i| \leq 10^{(m-n)m!}.$$

Let $t := 10^{m!}$ and $s \in \mathbb{N}$ with $s/t = \sum_{k=1}^{m} 10^{-k!}$. Then

$$\xi - \frac{s}{t} = \sum_{k>m} 10^{-k!} \leq \frac{2}{10^{(m+1)!}} = \frac{2}{t^{m+1}} < \frac{1}{t^m}. \tag{I.13.1}$$

[2] The calculations can be simplified using the mean value theorem of analysis.

Since μ is irreducible, $\alpha(s/t) \neq 0$ holds and it follows

$$|\alpha(s/t)| = \Big|\sum_{i=0}^{n} a_i (s/t)^i\Big| \geq \frac{1}{t^n}. \tag{I.13.2}$$

For $i \geq 0$, $X^i - \xi^i = (X - \xi) \sum_{k=0}^{i-1} \xi^k X^{i-1-k}$. Because of $s/t \leq \xi \leq 1/2$, this leads to the contradiction

$$\begin{aligned} |\alpha(s/t)| = |\alpha(s/t) - \alpha(\xi)| &= \Big|\sum_{i=0}^{n} a_i ((s/t)^i - \xi^i)\Big| = (s/t - \xi)\Big|\sum_{i=1}^{n} a_i \sum_{k=0}^{i-1} \xi^k (s/t)^{i-1-k}\Big| \\ &\leq (s/t - \xi) \sum_{i=1}^{n} |a_i| i \xi^{i-1} \leq (s/t - \xi) \sum_{i=1}^{n} |a_i| < \frac{10^{(m-n)m!}}{t^m} = \frac{1}{t^n}. \end{aligned}$$

□

Theorem I.13.13 (Lindemann)**.** *The circle number $\pi = 3{,}14\ldots$ is transcendental.*

Proof. The proof is based on Euler's formula $e^{\pi \mathrm{i}} + 1 = 0$. See Example A.10.6. □

Theorem I.13.14. *Every (countable) field K possesses exactly one algebraic closure up to K-isomorphism.*

Proof. We restrict ourselves to the case where K is countable. The general case requires Zorn's Lemma (equivalent to the axiom of choice, see Theorem II.2.9). If K is countable, then all polynomials can also be counted, i. e. $K[X] = \{\alpha_1, \alpha_2, \ldots\}$. Let $K_0 := K$ and inductively K_n be the splitting field of α_n over K_{n-1} for $n = 1, 2, \ldots$. Obviously, $\overline{K} := \bigcup K_n$ is then a field and the extension $K \subseteq \overline{K}$ is algebraic according to Lemma I.13.2. If $\alpha \in \overline{K}[X] \setminus \overline{K}$, then every root x of α (in a splitting field) is algebraic over $\overline{K}$ and thus also algebraic over K. In particular, x is a root of a polynomial in $K[X]$. This shows $x \in \overline{K}$ and $\overline{K}$ is indeed an algebraic closure of K.

If $\widetilde{K}$ is another algebraic closure of K, then $\widetilde{K}$ contains a splitting field $\widetilde{K}_n$ of $\alpha_1 \ldots \alpha_n$ for $n \geq 1$. Since the extension $K \subseteq \widetilde{K}$ is algebraic, $\widetilde{K} = \bigcup \widetilde{K}_n$ also holds. Let $\sigma_0 := \mathrm{id}_K$. According to Steinitz, there exist K-isomorphisms $\sigma_n \colon K_n \to \widetilde{K}_n$ with $(\sigma_n)_{K_{n-1}} = \sigma_{n-1}$ for $n \geq 1$. We consider the map $\sigma \colon \overline{K} \to \widetilde{K}$ with $\sigma(x) := \sigma_n(x)$ for $x \in K_n$. If $x \in K_n \cup K_m$ with $n \leq m$, then $\sigma_n(x) = \sigma_m(x)$ holds. Therefore, σ is a well-defined bijection. For $x, y \in \overline{K}$ there exists an $n \in \mathbb{N}$ with $x, y \in K_n$. It then holds that

$$\sigma(x \dot{+} y) = \sigma_n(x \dot{+} y) = \sigma_n(x) \dot{+} \sigma_n(y) = \sigma(x) \dot{+} \sigma(y).$$

Thus σ is a K-isomorphism. □

Example I.13.15. For $p \in \mathbb{P}$ it holds that

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^{2!}} \subseteq \mathbb{F}_{p^{3!}} \subseteq \ldots$$

according to Theorem I.11.14. Obviously, $\overline{\mathbb{F}_p} := \bigcup_{n \geq 1} \mathbb{F}_{p^{n!}}$ is an algebraic field extension over $\mathbb{F}_p$. By construction, the polynomials $X^{p^{n!}} - X \in \overline{\mathbb{F}_p}[X]$ for all $n \in \mathbb{N}$ split completely into linear factors. According to Lemma I.11.17, all (irreducible) polynomials from $\mathbb{F}_p[X]$ split into linear factors over $\overline{\mathbb{F}_p}$. Now if $\alpha \in \overline{\mathbb{F}_p}[X] \setminus \overline{\mathbb{F}_p}$ with root x in a splitting field of α, then x is algebraic over $\overline{\mathbb{F}_p}$ and also over $\mathbb{F}_p$. This shows $x \in \overline{\mathbb{F}_p}$ and $\overline{\mathbb{F}_p}$ is an algebraic closure of $\mathbb{F}_p$.

I.14 Solvability of Equations

Lemma I.14.1 (Dedekind)**.** *For fields K and L, the set of homomorphisms $K \to L$ is linearly independent in the L-vector space of all maps $K \to L$.*

Proof. Suppose there exist homomorphisms $\sigma_1, \ldots, \sigma_n \colon K \to L$ and $a_1, \ldots, a_n \in L^\times$ with $\sum a_i \sigma_i = 0$. Let n be as small as possible. Certainly $n \geq 2$ and there exists a $y \in K$ with $\sigma_1(y) \neq \sigma_n(y)$. For all $x \in K$ it then holds that

$$\sum_{i=1}^{n-1} a_i\big(\sigma_i(y) - \sigma_n(y)\big)\sigma_i(x) = \sum_{i=1}^{n} a_i \sigma_i(yx) - \sigma_n(y) \sum_{i=1}^{n} a_i \sigma_i(x) = 0.$$

This shows $\sum_{i=1}^{n-1} a_i(\sigma_i(y) - \sigma_n(y))\sigma_i = 0$ in contradiction to the choice of n. □

Lemma I.14.2 (Kummer)**.** *Let* $\operatorname{char} K = 0$ *and $n \in \mathbb{N}$, such that K contains a primitive n-th root of unity. Let $K \subseteq L$ be a Galois extension.* $\mathrm{Gal}(L|K)$ *is cyclic of order $d \mid n$ if and only if L is the splitting field of $X^n - x$ for some $x \in K$.*

Proof. Let $\zeta \in K$ be a primitive n-th root of unity. First, let $G := \mathrm{Gal}(L|K) = \langle \Gamma \rangle \cong C_d$ with $d \mid n$. Then $\gamma := \zeta^{n/d} \in K$ is a primitive d-th root of unity. By Dedekind, there exists a $b \in L$ with

$$a := \gamma\Gamma(b) + \ldots + \gamma^d \Gamma^d(b) \neq 0.$$

Then $\Gamma^i(a) = \gamma^{-i} a \in K(a)$ for $i = 1, \ldots, d$ and the restrictions of $\Gamma, \ldots, \Gamma^d$ to $K(a)$ are pairwise distinct. By Theorem I.10.6 it follows that $L = K(a)$. Furthermore,

$$x := a^n = \gamma^{-n} a^n = \Gamma(a^n) \in L^\Gamma = K.$$

The roots of $X^n - x$ are precisely $a\zeta^i$ with $i = 1, \ldots, n$. Thus L is the splitting field of $X^n - x$.

Conversely, let L be the splitting field of $X^n - x \in K[X]$. Let $a \in L$ with $a^n = x$. The roots of $X^n - x$ are then $a\zeta^i$ with $i = 1, \ldots, n$. This shows $L = K(a)$. Each $\Gamma \in \mathrm{Gal}(L|K) =: G$ is already uniquely determined by $\Gamma(a) = a\zeta^i$. Therefore the map

$$\begin{aligned} F \colon G &\to \mathbb{Z}/n\mathbb{Z}, \\ \Gamma &\mapsto i + n\mathbb{Z} \end{aligned}$$

is injective. For $\Lambda \in G$ with $\Lambda(a) = a\zeta^j$ it holds that

$$(\Gamma \circ \Lambda)(a) = \Gamma(a\zeta^j) = \Gamma(a)\zeta^j = a\zeta^{i+j}.$$

Thus F is a monomorphism and G is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$ by the homomorphism theorem. The claim now follows from Theorem I.3.34. □

Remark I.14.3. In *Artin-Schreier theory* one considers the analogous situation for $\operatorname{char} K > 0$ (see Theorem A.7.7).

Example I.14.4. The splitting field of X^4-2 over $K := \mathbb{Q}_4 = \mathbb{Q}(\mathrm{i})$ is $L := \mathbb{Q}(\mathrm{i}, \sqrt[4]{2})$. Because $\sqrt{2} \notin K$, X^4-2 is irreducible over K. Therefore $\mathrm{Gal}(L|K)$ is cyclic of order $|L:K| = 4$.

Definition I.14.5.

(i) A field extension $K \subseteq L$ is called a *radical extension*, if intermediate fields $K = K_0 \subseteq \ldots \subseteq K_n = L$ and elements $a_i \in K_i$, $k_i \in \mathbb{N}$ with $K_i = K_{i-1}(a_i)$ and $a_i^{k_i} \in K_{i-1}$ for $i = 1, \ldots, n$ exist.

(ii) A polynomial $\alpha \in \mathbb{Q}[X] \setminus \mathbb{Q}$ is called *solvable*, if it splits into linear factors in a radical extension over $\mathbb{Q}$. This means that one can express the solutions of the equation $\alpha(X) = 0$ by rational numbers, basic arithmetic operations and taking roots (for example p-q-formula for $\deg \alpha = 2$).

(iii) If K is a splitting field of $\alpha \in \mathbb{Q}[X] \setminus \mathbb{Q}$, then $\mathrm{Gal}(\alpha) := \mathrm{Gal}(K|\mathbb{Q})$ is called the *Galois group* of α. Since K is uniquely determined up to $\mathbb{Q}$-isomorphism (Steinitz), $\mathrm{Gal}(\alpha)$ is uniquely determined up to isomorphism. With the fundamental theorem of algebra, one can also uniquely choose K as a subfield of $\mathbb{C}$.

Example I.14.6.

(i) Let $n \in \mathbb{N}$ and $\alpha := X^n - 2 \in \mathbb{Q}[X]$. The splitting field of α is obviously $L = \mathbb{Q}_n(\sqrt[n]{2})$ (cf. Exercise I.55). Because of $\mathbb{Q}_n = \mathbb{Q}(e^{2\pi \mathrm{i}/n})$, $\mathbb{Q} \subseteq L$ is a radical extension and α is solvable. Let $G := \mathrm{Gal}(\alpha) = \mathrm{Gal}(L|\mathbb{Q})$. According to Kummer, $N := \mathrm{Gal}(L|\mathbb{Q}_n)$ is a cyclic subgroup of G. Since $\mathbb{Q} \subseteq \mathbb{Q}_n$ is also a Galois extension (Theorem I.12.12), $N \trianglelefteq G$ holds according to the main theorem of Galois theory. Furthermore, $G/N \cong \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian. Therefore, G is solvable according to Theorem I.6.5.

(ii) Attention: A polynomial α can be solvable even though its splitting field does *not* form a radical extension. A concrete example is given in Example I.14.26(ii).

Remark I.14.7. One can sense that the main theorem of Galois theory transforms radical extensions into solvable groups via Kummer. For this, however, one must first obtain a Galois extension.

Lemma I.14.8. *Every radical extension $K \subseteq L$ with $\mathrm{char}\, K = 0$ lies in a radical extension that is also a Galois extension.*

Proof. Let $K = K_0 \subseteq \ldots \subseteq K_n = L$ and $K_i = K_{i-1}(a_i)$ with $a_i^{k_i} \in K_{i-1}$ for $i = 1, \ldots, n$. According to Theorem I.12.2, there exists a Galois extension $K \subseteq M$ with $L \subseteq M$. Let $\mathrm{Gal}(M|K) = \{\mathrm{id}_M = \sigma_1, \ldots, \sigma_k\}$ and

$$K_{ij} := K(\sigma_1(a_1), \ldots, \sigma_k(a_1), \ldots, \sigma_1(a_{i-1}), \ldots, \sigma_k(a_{i-1}), \sigma_1(a_i), \ldots, \sigma_j(a_i))$$

for $i = 1, \ldots, n$ and $j = 1, \ldots, k$. Because of $\sigma_i(K_{nk}) = K_{nk}$ for $i = 1, \ldots, k$, $K_{nk}^{\mathrm{Gal}(K_{nk}|K)} \subseteq M^{\mathrm{Gal}(M|K)} = K$, i. e. $K \subseteq K_{nk}$ is a Galois extension according to Artin. Furthermore, $L = K(a_1, \ldots, a_n) \subseteq K_{nk}$ holds.

Certainly $K_{11} = K(a_1)$ with $a_1^{k_1} \in K_0 = K$. For $i = 1, \ldots, n$ and $j = 2, \ldots, k$, $K_{ij} = K_{i,j-1}(\sigma_j(a_i))$ holds and

$$\sigma_j(a_i)^{k_i} = \sigma_j(a_i^{k_i}) \in \sigma_j(K_{i-1}) = \sigma_j(K(a_1, \ldots, a_{i-1})) \subseteq K_{i-1,j} \subseteq K_{i,j-1}.$$

For $i = 2, \ldots, n$, finally $K_{i1} = K_{i-1,k}(a_i)$ with $a_i^{k_i} \in K_{i-1} \subseteq K_{i-1,k}$ also holds. Thus $K \subseteq K_{11} \subseteq K_{12} \subseteq \ldots \subseteq K_{nk}$ is a radical extension. □

Theorem I.14.9 (Galois). *An $\alpha \in \mathbb{Q}[X] \setminus \mathbb{Q}$ is solvable if and only if* $\mathrm{Gal}(\alpha)$ *is solvable.*

Proof.
Step 1: $\Longrightarrow$
According to Lemma I.14.8 there exists a radical and Galois extension $\mathbb{Q} = K_0 \subseteq \ldots \subseteq K_n$, such that a splitting field L of α lies in K_n. Let $a_i \in K_i$ and $k_i \in \mathbb{N}$ with $K_i = K_{i-1}(a_i)$ and $a_i^{k_i} \in K_{i-1}$ for $i = 1, \ldots, n$. Let $k := k_1 \ldots k_n$ and $\zeta \in \mathbb{Q}_k$ be a primitive k-th root of unity. According to Artin, K_n is the splitting field of some $\gamma \in K_0[X]$. Therefore $K_n(\zeta)$ is the splitting field of $(X^k - 1)\gamma \in K_0[X]$. In particular, $K_0 \subseteq K_n(\zeta)$ is a Galois extension (Theorem I.12.2). According to Theorem I.12.12, $\mathbb{Q} = K_0 \subseteq K_0(\zeta) = \mathbb{Q}_k$ is a Galois extension with an abelian Galois group. The fundamental theorem of Galois theory shows

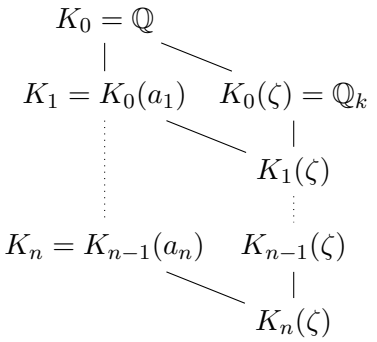
$$G_n := \mathrm{Gal}(K_n(\zeta)|K_0(\zeta)) \trianglelefteq \mathrm{Gal}(K_n(\zeta)|K_0) =: G$$

and $G/G_n \cong \mathrm{Gal}(K_0(\zeta)/K_0)$ is abelian.

We now consider the Galois extension $K_{i-1}(\zeta) \subseteq K_n(\zeta)$ for $i = 1, \ldots, n$ (Theorem I.10.11). Obviously $K_i(\zeta) = K_{i-1}(\zeta, a_i)$ is the splitting field of $X^{k_i} - a_i^{k_i} \in K_{i-1}(\zeta)[X]$. According to Theorem I.12.2 and Kummer, $K_{i-1}(\zeta) \subseteq K_i(\zeta)$ is a Galois extension with a cyclic Galois group. Thus $G_{n-i} := \mathrm{Gal}(K_n(\zeta)|K_i(\zeta)) \trianglelefteq G_{n-i+1}$ and $G_{n-i+1}/G_{n-i} \cong \mathrm{Gal}(K_i(\zeta)|K_{i-1}(\zeta))$ is cyclic. Overall, one has a series

$$1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n \trianglelefteq G$$

with abelian factors, i. e. G is solvable. Since $\mathbb{Q} \subseteq L$ is a Galois extension, $\mathrm{Gal}(\alpha) \cong \mathrm{Gal}(L|\mathbb{Q}) \cong G/\mathrm{Gal}(K_n(\zeta)|L)$ is also solvable (Theorem I.6.5).



Step 2: $\Longleftarrow$
Let $\mathrm{Gal}(\alpha)$ be solvable of order n. Let K be a splitting field of α and let $\zeta \in \mathbb{Q}_n$ be a primitive n-th root of unity. It suffices to show that $\mathbb{Q}_n \subseteq K(\zeta)$ is a radical extension, because then $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) = \mathbb{Q}_n \subseteq K(\zeta)$ is also a radical extension. As a splitting field of α over $\mathbb{Q}_n$, $\mathbb{Q}_n \subseteq K(\zeta)$ is a Galois extension (Theorem I.12.2). For $\Gamma \in G := \mathrm{Gal}(K(\zeta)|\mathbb{Q}_n)$, we have $\Gamma(\alpha) = \alpha$ and $\Gamma(K) = K$. The restriction map

$$G \to \mathrm{Gal}(K|\mathbb{Q}) \cong \mathrm{Gal}(\alpha)$$

is thus a well-defined homomorphism with kernel $\mathrm{Gal}(K(\zeta)|\mathbb{Q}_n(K)) = 1$. By the isomorphism theorem, we can consider G as a subgroup of $\mathrm{Gal}(\alpha)$. In particular, G is solvable (Theorem I.6.5). Let $1 = G_0 \trianglelefteq \ldots \trianglelefteq G_m = G$ with cyclic factors (Theorem I.6.4). For $K_i := K(\zeta)^{G_{m-i}}$, it then holds that $\mathbb{Q}_n = K_0 \subseteq \ldots \subseteq K_m = K(\zeta)$. For $i = 1, \ldots, m$, $K_{i-1} \subseteq K_m$ is a Galois extension and because of

$$\mathrm{Gal}(K_m|K_i) = \mathrm{Gal}(K_m|K_m^{G_{m-i}}) = G_{m-i} \trianglelefteq G_{m-i+1} = \mathrm{Gal}(K_m|K_{i-1})$$

$K_{i-1} \subseteq K_i$ is also a Galois extension with $\mathrm{Gal}(K_i|K_{i-1}) \cong G_{m-i+1}/G_{m-i}$ (Theorem I.10.11). By Lagrange, $|G_{m-i+1}/G_{m-i}|$ is a divisor of $|G|$ and thus a divisor of $|\mathrm{Gal}(\alpha)| = n$ because $G \leq \mathrm{Gal}(\alpha)$. By Kummer, there exists an $a_i \in K_i$ with $K_i = K_{i-1}(a_i)$ and $a_i^n \in K_{i-1}$. Thus $\mathbb{Q}_n \subseteq K(\zeta)$ is a radical extension and α is solvable. □

Theorem I.14.10 (Cardano, del Ferro, Tartaglia, Ferrari). *Polynomials of degree ≤ 4 are solvable.*

Proof. Let $\alpha \in \mathbb{Q}[X] \setminus \mathbb{Q}$ with $d := \deg \alpha \leq 4$. Remark I.10.5 yields a monomorphism $\mathrm{Gal}(\alpha) \to S_d \leq S_4$. According to Example I.6.6, S_4 is solvable and therefore so is $\mathrm{Gal}(\alpha)$. The claim now follows by Galois. □

Lemma I.14.11. *If $\sigma \in S_5$ is a 5-cycle and $\tau \in S_5$ is a transposition, then $S_5 = \langle \sigma, \tau \rangle$ holds.*

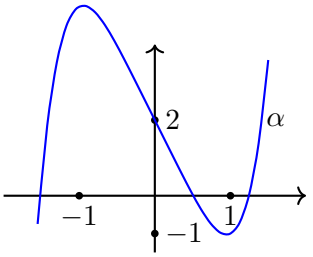
Proof. Let $\sigma = (a_1, \ldots, a_5)$, $\tau = (b_1, b_2)$ and $G := \langle \sigma, \tau \rangle$. Because of $\sigma = (a_2, a_3, a_4, a_5, a_1) = \ldots$ we can assume $a_1 = b_1$. Because of $\sigma^i = (a_1, a_{i+1}, \ldots)$ for $1 \leq i \leq 4$ we can assume $a_2 = b_2$ by replacing σ with a suitable σ^i. Then $\tau\sigma\tau^{-1} = (a_1, a_3, a_4, a_5, a_2) \notin \langle \sigma \rangle$ holds. Thus G contains at least the two 5-Sylow groups $\langle \sigma \rangle$ and $\langle \tau\sigma\tau^{-1} \rangle$. According to Sylow, G possesses at least six 5-Sylow groups. These all lie in $G \cap A_5 \trianglelefteq G$. In particular, $|G \cap A_5| \geq 6 \cdot 4 = 24$. According to Theorem I.6.13, A_5 is simple and, according to Example I.3.17(iii), cannot contain a subgroup of index 2. Therefore $A_5 = G \cap A_5 \leq G$ holds. Because of $\tau \notin A_5$, it finally follows that $G = S_5$. □

Theorem I.14.12 (Abel, Ruffini[1]). *There are non-solvable polynomials of degree 5.*

Proof. By Eisenstein with $p = 2$, $\alpha := X^5 - 4X + 2 \in \mathbb{Q}[X]$ is irreducible. According to Theorem I.11.20, α has pairwise distinct roots $x_1, \ldots, x_5$ in a splitting field $K \subseteq \mathbb{C}$. Thus

$$5 = \deg \alpha = |\mathbb{Q}(x_1) : \mathbb{Q}| \;\big|\; |K : \mathbb{Q}| = |\mathrm{Gal}(\alpha)|.$$

By Cauchy, $\mathrm{Gal}(\alpha)$ possesses an element of order 5. Remark I.10.5 provides a monomorphism $\Gamma\colon \mathrm{Gal}(\alpha) \to \mathrm{Sym}(x_1, \ldots, x_5)$ whose image contains a 5-cycle σ. Because of $\alpha' = 5X^4 - 4$, the graph of $\alpha\colon \mathbb{R} \to \mathbb{R}$ has two extrema, namely at $\pm\sqrt[4]{4/5}$. From $\alpha(0) = 2$ and $\alpha(1) = -1$ it follows that α has exactly three real roots (cf. Example I.13.9). Complex conjugation on K then yields a transposition τ in the image of Γ. According to Lemma I.14.11, $\langle \sigma, \tau \rangle = \mathrm{Sym}(x_1, \ldots, x_5)$ and therefore $\mathrm{Gal}(\alpha) \cong \Gamma(\mathrm{Gal}(\alpha)) \cong S_5$. Since S_5 is not solvable (Theorem I.6.13), the claim follows by Galois. □



Remark I.14.13.

(i) The proof of Theorem I.14.12 shows that the estimate $|L : K| \leq \deg(\alpha)!$ in Kronecker's Theorem cannot be improved.

(ii) One must realize that $\sqrt[n]{z}$ for $z \in \mathbb{C}$ is merely a symbol for an unspecified root of $X^n - z$ (in analysis, one could specifically define $\sqrt[n]{z} := \exp(\log(z)/n)$ using the principal value of the complex logarithm). With equal justification, one could define a new symbol, say $q_n(z)$, for a root of $X^n + X - z$ and ask which equations can be solved using only basic arithmetic operations and q_n. In fact, Bring and Jerrard showed that every equation of fifth degree can be transformed into the reduced form $X^5 + X - z = 0$ using basic arithmetic operations and extraction of roots.

(iii) One can "solve" equations of fifth (and higher) degree using modular elliptic functions or hypergeometric series.[2]

(iv) In the following, we determine $\mathrm{Gal}(\alpha)$ as a permutation group on the roots of $\alpha \in \mathbb{Q}[X]$.

[1] For the history see [M. I. Rosen, *Nils Hendrik Abel and Equations of the Fifth Degree*, Amer. Math. Monthly 102 (1995), 495–505]

[2] See [King, *Beyond the quartic equation*, Birkhäuser, Boston, 1996]

Definition I.14.14.

(i) The polynomial ring with several unknowns $X_1, \ldots, X_n$ is defined inductively by $K[X_1, \ldots, X_n] := K[X_1, \ldots, X_{n-1}][X_n]$. Every element in $K[X_1, \ldots, X_n]$ then has the form

$$\alpha = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$$

with $a_{i_1,\ldots,i_n} \in K$. One sets $\deg \alpha := \sup\{i_1 + \ldots + i_n : a_{i_1,\ldots,i_n} \neq 0\}$. It holds (still) that $\deg(\alpha\beta) = \deg \alpha + \deg \beta$ and $\deg(\alpha + \beta) \leq \max\{\deg \alpha, \deg \beta\}$ with equality if $\deg \alpha \neq \deg \beta$.

(ii) A polynomial $\alpha \in K[X_1, \ldots, X_n]$ is called *symmetric*, if $\alpha = \alpha(X_{\pi(1)}, \ldots, X_{\pi(n)})$ holds for every $\pi \in S_n$. The *elementary symmetric* polynomials of order n are $\sigma_0 := 1$ and

$$\sigma_k := \sum_{1 \leq i_1 < \ldots < i_k \leq n} X_{i_1} \ldots X_{i_k} \in K[X_1, \ldots, X_n] \qquad (k = 1, \ldots, n).$$

Remark I.14.15. The symmetric polynomials form a subring of $K[X_1, \ldots, X_n]$ (cf. Remark I.8.11).

Example I.14.16.

(i) Obviously $XY^3 + X^3Y - X - Y + 2 \in K[X, Y]$ is symmetric of degree 4.

(ii) For $n = 3$ we have

$$\sigma_0 = 1, \qquad \sigma_1 = X_1 + X_2 + X_3, \qquad \sigma_2 = X_1X_2 + X_1X_3 + X_2X_3, \qquad \sigma_3 = X_1X_2X_3.$$

(iii) In general, $\deg \sigma_k = k$ for $k = 0, \ldots, n$.

Theorem I.14.17 (Vieta)**.** *For $\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Q}[X]$ with roots $x_1, \ldots, x_n \in \mathbb{C}$, it holds that*

$$a_{n-k} = (-1)^k \sigma_k(x_1, \ldots, x_n)$$

for $k = 1, \ldots, n$.

Proof.

$$\alpha = \prod_{i=1}^{n} (X - x_i) = \sum_{k=0}^{n} \Big((-1)^k \sum_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} \ldots x_{i_k} \Big) X^{n-k}. \qquad \square$$

Example I.14.18. For $\alpha = X^2 + aX + b$ with roots x_1 and x_2, it holds that $x_1 + x_2 = -a$ as well as $x_1x_2 = b$.

Theorem I.14.19 (Fundamental Theorem on Symmetric Polynomials)**.** *For every symmetric $\alpha \in K[X_1, \ldots, X_n]$ there exists exactly one $\gamma \in K[X_1, \ldots, X_n]$ with $\alpha = \gamma(\sigma_1, \ldots, \sigma_n)$.*

Proof.
Existence: Let wlog.

$$\alpha = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} \neq 0.$$

We order the tuples $(i_1, \ldots, i_n)$ lexicographically and argue by induction on

$$f(\alpha) := \max\big\{(i_1, \ldots, i_n) : a_{i_1,\ldots,i_n} \neq 0\big\}.$$

In the case $f(\alpha) = (0, \ldots, 0)$, then $\gamma := \alpha = a_{0,\ldots,0} \in K$. Now let $f(\alpha) = (d_1, \ldots, d_n) > (0, \ldots, 0)$. Because of $\alpha = \alpha(X_{\pi(1)}, \ldots, X_{\pi(n)})$ for all $\pi \in S_n$, it follows that $d_1 \geq \ldots \geq d_n$. Let

$$\beta := a_{d_1,\ldots,d_n} \sigma_1^{d_1-d_2} \sigma_2^{d_2-d_3} \ldots \sigma_{n-1}^{d_{n-1}-d_n} \sigma_n^{d_n}.$$

It holds that $f(\sigma_k^{d_k-d_{k+1}}) = (d_k - d_{k+1}) f(\sigma_k) = (d_k - d_{k+1}, \ldots, d_k - d_{k+1}, 0, \ldots, 0)$ and

$$f(\beta) = f(\sigma_1^{d_1-d_2}) + \ldots + f(\sigma_n^{d_n}) = (d_1, \ldots, d_n).$$

The symmetric polynomial $\alpha - \beta$ therefore satisfies $f(\alpha - \beta) < (d_1, \ldots, d_n)$ and the existence of γ follows by induction.

Uniqueness: Let $\gamma, \delta \in K[X_1, \ldots, X_n]$ with $\gamma(\sigma_1, \ldots, \sigma_n) = \delta(\sigma_1, \ldots, \sigma_n)$. For $\rho := \gamma - \delta$, then $\rho(\sigma_1, \ldots, \sigma_n) = 0$ and we must show $\rho = 0$. Suppose indirectly $\rho \neq 0$. Let $d_1 \geq \ldots \geq d_n$ be the lexicographically largest n-tuple such that the coefficient of $X_1^{d_1-d_2} X_2^{d_2-d_3} \ldots X_n^{d_n}$ in ρ does not vanish. As above, $f(\sigma_1^{d_1-d_2} \ldots \sigma_n^{d_n}) = (d_1, \ldots, d_n)$. For every other summand $X_1^{e_1-e_2} \ldots X_n^{e_n}$ of ρ, $f(\sigma_1^{e_1-e_2} \ldots \sigma_n^{e_n}) < (d_1, \ldots, d_n)$. This yields $f(\rho(\sigma_1, \ldots, \sigma_n)) = (d_1, \ldots, d_n)$ in contradiction to $\rho(\sigma_1, \ldots, \sigma_n) = 0$. □

Example I.14.20.

(i) We consider $\alpha = XY^3 + X^3Y - X - Y \in K[X, Y]$. With the notation from the proof, $f(\alpha) = (3, 1)$ and

$$\beta := \sigma_1^2 \sigma_2 = (X + Y)^2 XY = X^3Y + 2X^2Y^2 + XY^3.$$

It follows that $\alpha - \beta = -2X^2Y^2 - X - Y$. In the next step, $f(\alpha - \beta) = (2, 2)$ and

$$\beta_2 := -2\sigma_2^2 = -2X^2Y^2.$$

There remains $\alpha - \beta - \beta_2 = -X - Y = -\sigma_1$. Finally,

$$\alpha = \beta + \beta_2 - \sigma_1 = \sigma_1^2\sigma_2 - 2\sigma_2^2 - \sigma_1 = \gamma(\sigma_1, \sigma_2)$$

with $\gamma = X^2Y - 2Y^2 - X$.

(ii) For $k \in \mathbb{N}_0$, $\rho_k = X_1^k + \ldots + X_n^k \in K[X_1, \ldots, X_n]$ is symmetric. For $0 \leq l \leq n-1$, let

$$\alpha(k, l) := \sum_{i=1}^{n} X_i^k \sigma_l(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n).$$

Then

$$\sigma_i \rho_{k-i} = \begin{cases} \rho_k = \alpha(k, 0) & \text{if } i = 0, \\ \alpha(k-i, i) + \alpha(k-i+1, i-1) & \text{if } 1 \leq i \leq k < n, \\ \alpha(k-n+1, n-1) & \text{if } i = n \leq k. \end{cases}$$

As a telescoping sum, one obtains the GIRARD-NEWTON identities:

$$\boxed{\sum_{i=0}^{\min\{k,n\}} (-1)^i \sigma_i \rho_{k-i} = \begin{cases} 0 & \text{if } k \geq n, \\ (-1)^k (n-k)\sigma_k & \text{if } k < n \end{cases}}$$

(note $\alpha(0,l) = (n-l)\sigma_l$). Thus, one can express ρ_k recursively in terms of $\sigma_0, \ldots, \sigma_n$.

Definition I.14.21. Let $\alpha \in K[X]$ be monic with roots $x_1, \ldots, x_n$ (with multiplicities) in a splitting field L. Then

$$D_\alpha := \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in L$$

is called the *discriminant* of α (does not depend on the order of the x_i).

Lemma I.14.22. *Let $\alpha \in K[X]$ be monic with roots $x_1, \ldots, x_n$. Then*

$$D_\alpha = (-1)^{\binom{n}{2}} \alpha'(x_1) \ldots \alpha'(x_n).$$

Proof. For $i = 1, \ldots, n$, by the product rule, $\alpha' = \prod_{j \neq i}(X - x_j) + (X - x_i)\Big(\prod_{j \neq i}(X - x_j)\Big)'$ and $\alpha'(x_i) = \prod_{j \neq i}(x_i - x_j)$. This shows

$$\prod_{i=1}^{n} \alpha'(x_i) = \prod_{i<j} (x_i - x_j)(x_j - x_i) = (-1)^{\binom{n}{2}} \prod_{i<j} (x_i - x_j)^2 = (-1)^{\binom{n}{2}} D_\alpha. \qquad \square$$

Remark I.14.23.

(i) Obviously, α has only simple roots if and only if $D_\alpha \neq 0$. If applicable, $K \subseteq L$ is a Galois extension according to Artin and $D_\alpha \in L^{\mathrm{Gal}(L|K)} = K$.

(ii) One can regard D_α as a symmetric polynomial in $x_1, \ldots, x_n$. According to the main theorem above and Vieta, D_α can be expressed as a polynomial in the coefficients of α.

Example I.14.24. For $\alpha = X^2 + aX + b$ one obtains

$$\boxed{D_\alpha = (x_1 - x_2)^2 = \sigma_1^2 - 4\sigma_2 = a^2 - 4b.}$$

For $\alpha = X^3 + aX^2 + bX + c$, the TSCHIRNHAUS transformation $X \mapsto X - a/3$ leads to a reduced polynomial of the form $\alpha = X^3 + aX + b$ (in this process, neither D_α nor L change). According to Lemma I.14.22, it holds that

$$\begin{aligned} -D_\alpha = \alpha'(x_1)\alpha'(x_2)\alpha'(x_3) &= (3x_1^2 + a)(3x_2^2 + a)(3x_3^2 + a) = \\ &= 27(x_1x_2x_3)^2 + 9a\big((x_1x_2)^2 + (x_1x_3)^2 + (x_2x_3)^2\big) + 3a^2(x_1^2 + x_2^2 + x_3^2) + a^3. \end{aligned}$$

With

$$\begin{gathered} (x_1x_2x_3)^2 = \sigma_3^2 = b^2, \\ (x_1x_2)^2 + (x_1x_3)^2 + (x_2x_3)^2 = (x_1x_2 + x_1x_3 + x_2x_3)^2 - 2x_1x_2x_3(x_1 + x_2 + x_3) = \sigma_2^2 - 2\sigma_3\sigma_1 = a^2, \\ x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = \sigma_1^2 - 2\sigma_2 = -2a \end{gathered}$$

it follows that

$$\boxed{D_\alpha = -27b^2 - 9a^3 - 3a^2(-2a) - a^3 = -4a^3 - 27b^2.}$$

In general, the discriminant can be calculated via determinants (Example III.2.42).

Theorem I.14.25. *For every irreducible $\alpha \in \mathbb{Q}[X]$, it holds that* $\mathrm{Gal}(\alpha) \leq A_{\deg \alpha}$ *if and only if* $\sqrt{D_\alpha} \in \mathbb{Q}$.

Proof. Let $x_1, \ldots, x_n$ be the roots of α in a splitting field $L \subseteq \mathbb{C}$. As an irreducible polynomial, α has no multiple roots (Theorem I.11.20) and $D_\alpha \neq 0$ follows. For $\Gamma \in G := \mathrm{Gal}(\alpha) \leq S_n$, it holds that

$$\Gamma(\sqrt{D_\alpha}) = \prod_{i<j} (\Gamma(x_i) - \Gamma(x_j)) = \mathrm{sgn}(\Gamma)\sqrt{D_\alpha}.$$

Thus $G \leq A_n$ if and only if $\sqrt{D_\alpha} \in L^G = \mathbb{Q}$. □

Example I.14.26.

(i) Let $\alpha = X^3 + aX + b \in \mathbb{Q}[X]$ be irreducible with $a > 0$. According to Example I.14.24, $D_\alpha = -4a^3 - 27b^2 < 0$ and $\mathrm{Gal}(\alpha) \cong S_3$ follows from Theorem I.14.25. Because of $\alpha' = 3X^2 + a$, the graph of α has no extrema and therefore only one real root. Complex conjugation thus provides a transposition in $\mathrm{Gal}(\alpha)$.

(ii) According to Corollary I.8.51, $\alpha = X^3 - 3X + 1$ is irreducible with $D_\alpha = 4 \cdot 3^3 - 27 = 3^4 = 9^2$. Therefore,

$$G := \mathrm{Gal}(\alpha) \cong A_3 \cong C_3$$

holds according to Theorem I.14.25. Complex conjugation thus acts trivially on the roots of α, i. e. α possesses three real roots. In particular, the splitting field K of α lies in $\mathbb{R}$ and has degree 3 over $\mathbb{Q}$. If K were a radical extension, then there would exist a positive $x \in \mathbb{Q}$ with $K = \mathbb{Q}(\sqrt[3]{x})$. Now G must also permute the roots of $X^3 - x$. Since two of these are non-real, $\sqrt[3]{x}$ would have to remain fixed under G. This contradicts $K^G = \mathbb{Q}$. Thus K is not a radical extension, although α is solvable.

(iii) With a transformation as in Example I.14.24, one can convert a polynomial of degree 4 into the reduced form $\alpha = X^4 + aX^2 + bX + c \in \mathbb{Q}[X]$. Let α be irreducible with roots $x_1, \ldots, x_4$ in a splitting field $L \subseteq \mathbb{C}$. Then $G := \mathrm{Gal}(\alpha)$ permutes the numbers

$$y_1 := x_1x_2 + x_3x_4, \qquad y_2 := x_1x_3 + x_2x_4, \qquad y_3 := x_1x_4 + x_2x_3.$$

It holds that

$$\begin{aligned} y_1 + y_2 + y_3 &= \sigma_2 = a, \\ y_1y_2 + y_1y_3 + y_2y_3 &= \sigma_1\sigma_3 - 4\sigma_4 = -4c, \\ y_1y_2y_3 &= \sigma_1^2\sigma_4 + \sigma_3^2 - 4\sigma_2\sigma_4 = b^2 - 4ac. \end{aligned}$$

According to Vieta, y_1, y_2, y_3 are the solutions of the *cubic resolvent*

$$\beta := Y^3 - aY^2 - 4cY - b^2 + 4ac.$$

Because of $y_1 - y_2 = (x_1 - x_4)(x_2 - x_3)$ etc., $D_\alpha = D_\beta$ holds. If β splits into linear factors over $\mathbb{Q}$, then $G = \langle (1,2)(3,4), (1,3)(2,4) \rangle = V_4$. If β has exactly one rational root, say y_1, then

$$C_4 \cong \langle (1,3,2,4) \rangle \leq G \leq \langle (1,3,2,4), (1,2) \rangle \overset{\text{Exercise I.24}}{\cong} D_8$$

holds. Finally, if β is irreducible, one obtains

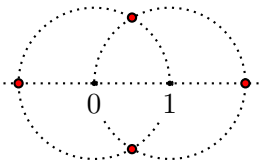
$$G = \begin{cases} A_4 & \text{if } \sqrt{D_\beta} \in \mathbb{Q}, \\ S_4 & \text{if } \sqrt{D_\beta} \notin \mathbb{Q}. \end{cases}$$

I.15 Construction with Compass and Straightedge

Remark I.15.1. In the following, we consider the set of complex numbers as a two-dimensional drawing surface.

Definition I.15.2. Let $\mathcal{M}_0 := \{0, 1\} \subseteq \mathbb{C}$ and inductively $\mathcal{M}_{i-1} \subseteq \mathbb{C}$ with $i \geq 1$. Let $\mathcal{G}$ be the set of all lines in $\mathbb{C}$ passing through two points in $\mathcal{M}_{i-1}$. Analogously, let $\mathcal{K}$ be the set of all circles in $\mathbb{C}$ whose center lies in $\mathcal{M}_{i-1}$ and whose radius is equal to the distance between two points in $\mathcal{M}_{i-1}$. Finally, let $\mathcal{M}_i$ be the set of intersection points of two distinct figures from $\mathcal{G} \cup \mathcal{K}$. A point $z \in \mathbb{C}$ is called (*with compass and straightedge*) *constructible*, if $z \in \mathcal{M} := \bigcup_{i \geq 0} \mathcal{M}_i$.

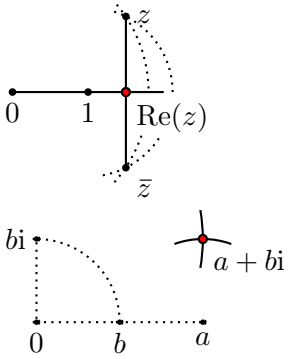
Example I.15.3. It holds that $\mathcal{M}_1 := \left\{-1, 0, 1, 2, \frac{1}{2}(1 \pm \sqrt{3}\mathrm{i})\right\}$.



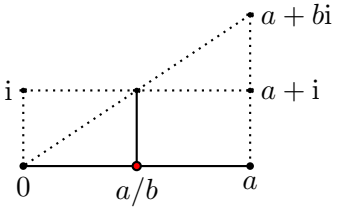
Lemma I.15.4. *The constructible points form a subfield of* $\mathbb{C}$ *that is closed under taking square roots and complex conjugation.*

Proof.
Step 1: $z \in \mathcal{M} \Longrightarrow |z| \in \mathcal{M}$.
Through the points $0, 1 \in \mathcal{M}$ one obtains all intersection points on the x-axis. Now $|z|$ is the intersection point of the x-axis with the circle with center 0 and radius $|z|$.

Step 2: $z \in \mathcal{M} \iff \mathrm{Re}(z), \mathrm{Im}(z) \in \mathcal{M}$.
By drawing circles around 1 and -1 with radius 2 and connecting the two intersection points, one obtains the y-axis. For an arbitrary $z \in \mathcal{M}$, one constructs $\mathrm{Re}(z), \mathrm{Im}(z)\mathrm{i} \in \mathcal{M}$ by dropping the perpendicular onto the x- and y-axis (see figure). With Step 1, it also follows that $\mathrm{Im}(z) \in \mathcal{M}$. Conversely, if $a, b \in \mathcal{M} \cap \mathbb{R}$ are given, then one first constructs $b\mathrm{i}$ and subsequently $a + b\mathrm{i}$ as the intersection point of two circles (see figure).

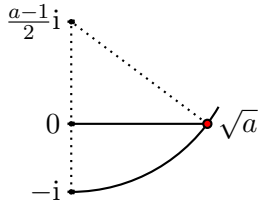


Step 3: $\mathcal{M} \cap \mathbb{R}$ is a field.
By definition $0, 1 \in \mathcal{M} \cap \mathbb{R}$. For $a, b \in \mathcal{M} \cap \mathbb{R}$ one obtains $a - b \in \mathcal{M} \cap \mathbb{R}$ as the intersection point of the x-axis with the circle with center a and radius b. For $a, b \in \mathcal{M} \cap \mathbb{R} \setminus \{0\}$ one obtains $a/b \in \mathcal{M}$ using the intercept theorem (wlog. $a, b > 0$, see figure).



Step 4: $a \in \mathcal{M} \cap \mathbb{R} \Longrightarrow \sqrt{a} \in \mathcal{M}$.
In the case $a < 0$, $\sqrt{a} = \sqrt{|a|}\mathrm{i}$. We can therefore assume $a > 0$. The claim now follows from the PYTHAGOREAN theorem (see figure):

$$\left(\frac{a-1}{2}\right)^2 + \sqrt{a}^2 = \left(\frac{a+1}{2}\right)^2.$$



Step 5: $\mathcal{M}$ is a field.
For $z, w \in \mathcal{M}$, $z + w = \mathrm{Re}(z) + \mathrm{Re}(w) + \mathrm{Im}(z)\mathrm{i} + \mathrm{Im}(w)\mathrm{i} \in \mathcal{M}$ according to the previous steps. For $z, w \in \mathcal{M} \setminus \{0\}$, analogously

$$\frac{z}{w} = \frac{z\overline{w}}{|w|^2} = \frac{\mathrm{Re}(z)\mathrm{Re}(w) + \mathrm{Im}(z)\mathrm{Im}(w)}{|w|^2} + \frac{\mathrm{Im}(z)\mathrm{Re}(w) - \mathrm{Re}(z)\mathrm{Im}(w)}{|w|^2}\mathrm{i} \in \mathcal{M}.$$

Step 6: $z \in \mathcal{M} \Longrightarrow \overline{z}, \sqrt{z} \in \mathcal{M}$.
The claim $\overline{z} = \mathrm{Re}(z) - \mathrm{Im}(z)\mathrm{i} \in \mathcal{M}$ follows immediately from the previous steps. Because of $\sqrt{-z} = \sqrt{z}\mathrm{i}$, we can assume $\mathrm{Im}(z) \geq 0$. Then it holds that

$$\sqrt{z} = \sqrt{\frac{1}{2}\big(\mathrm{Re}(z) + \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2}\big)} + \sqrt{\frac{1}{2}\big(-\mathrm{Re}(z) + \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2}\big)}\mathrm{i} \in \mathcal{M}$$

according to Step 4. □

Theorem I.15.5. *$z \in \mathbb{C}$ is constructible if and only if there exist fields $\mathbb{Q} = K_0 \subseteq \ldots \subseteq K_n$ with $|K_i : K_{i-1}| = 2$ for $i = 1, \ldots, n$ and $z \in K_n$.*

Proof. Suppose first that $\mathbb{Q} = K_0 \subseteq \ldots \subseteq K_n$ with $|K_i : K_{i-1}| = 2$ for $i = 1, \ldots, n$ and $z \in K_n$. Then there exist $a_i \in K_{i-1}$ with $K_i = K_{i-1}(\sqrt{a_i})$ for $i = 1, \ldots, n$ (see proof of Theorem I.12.23). By Lemma I.15.4, $a_1 \in K_0 = \mathbb{Q} = P(\mathcal{M}) \subseteq \mathcal{M}$, $K_1 = K_0(\sqrt{a_1}) \subseteq \mathcal{M}$ and inductively $z \in K_n \subseteq \mathcal{M}$.

Conversely, suppose z is constructible, i. e. $z \in \mathcal{M}_k$ for some $k \geq 0$. We argue by induction on k. In the case $k = 0$, $\mathbb{Q}(z) = \mathbb{Q}$ and the claim holds for $n = 0$. So let $k \geq 1$. Then z results from a construction using $a_1, \ldots, a_l \in \mathcal{M}_{k-1}$. By induction, there exist fields $\mathbb{Q} = K_{i,0} \subseteq \ldots \subseteq K_{i,m_i}$ with $a_i \in K_{i,m_i}$ and $|K_{i,j} : K_{i,j-1}| = 2$ for $j = 1, \ldots, m_i$ and $i = 1, \ldots, l$. Complex conjugation yields an analogous chain of extensions for $\overline{a_i}$. As above, all these extensions result from iterative adjunction of square roots. Adjoining all these square roots one after another, one obtains

$$\mathbb{Q} = K_0 \subseteq \ldots \subseteq K_n$$

with $a_1, \ldots, a_l, \overline{a_1}, \ldots, \overline{a_l} \in K_n$ and $|K_i : K_{i-1}| = 2$ for $i = 1, \ldots, n$. We now distinguish the three construction principles.

Case 1: z is the intersection point of two distinct lines.
Then there exist $a, b, c, d \in K_n$ and $r, s \in \mathbb{R}$ with $z = a + rb = c + sd$. Thus (r, s) is the unique solution of the system of equations

$$\begin{pmatrix} \mathrm{Re}(b) & -\mathrm{Re}(d) \\ \mathrm{Im}(b) & -\mathrm{Im}(d) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \mathrm{Re}(c-a) \\ \mathrm{Im}(c-a) \end{pmatrix}.$$

Because $\mathrm{Re}(a) = (a + \bar{a})/2 \in K_n$ etc., it follows that $r \in K_n$ and $z = a + rb \in K_n$ by Lemma I.15.4.

Case 2: z is the intersection point of a line and a circle.
Then there exist $a, b, c \in K_n$, $r \in K_n \cap \mathbb{R}$ and $s \in \mathbb{R}$ with $z = a + sb$ and

$$\mathrm{Re}(a + sb - c)^2 + \mathrm{Im}(a + sb - c)^2 = r^2.$$

This is a quadratic equation for s with coefficients in K_n. Thus s and z lie in a quadratic extension of K_n. The claim follows by Lemma I.15.4.

Case 3: z is the intersection point of two distinct circles.
Then there exist $a_i \in K_n$ and $r_i \in K_n \cap \mathbb{R}$ with $\mathrm{Re}(z - a_i)^2 + \mathrm{Im}(z - a_i)^2 = r_i^2$ for $i = 1, 2$. Subtraction yields

$$\mathrm{Re}(a_1 - a_2)\mathrm{Re}(z) + \mathrm{Im}(a_1 - a_2)\mathrm{Im}(z) \in K_n \cap \mathbb{R}. \tag{I.15.1}$$

Since the centers a_1 and a_2 of the circles are distinct, (I.15.1) describes a line on which at least two points from K_n lie. The claim now follows from Case 2. □

Corollary I.15.6. *If $z \in \mathbb{C}$ is constructible, then $|\mathbb{Q}(z) : \mathbb{Q}|$ is a power of 2. In particular, z is algebraic over $\mathbb{Q}$.*

Proof. With the notation from Theorem I.15.5, it holds that $|\mathbb{Q}(z) : \mathbb{Q}| \mid |K_n : K_0| = 2^n$. □

Remark I.15.7.

(i) Theorem I.15.5 shows that $\mathcal{M}$ is the "smallest" subfield of $\mathbb{C}$ that is closed under taking square roots.

(ii) The converse of Corollary I.15.6 is false: According to Eisenstein with $p = 2$, $\alpha = X^4 + 2X - 2 \in \mathbb{Q}[X]$ is irreducible with cubic resolvent $\beta = Y^3 + 8Y - 4$ (see Example I.14.26). Since β has no integer root, β is irreducible according to Corollary I.8.51. Because $D_\alpha = D_\beta < 0$, $G := \mathrm{Gal}(\alpha) \cong S_4$. For a root z of α in a splitting field L, $|\mathbb{Q}(z) : \mathbb{Q}| = 4$ and $H := \mathrm{Gal}(L|\mathbb{Q}(z)) \leq G$ has order 6. According to Sylow, G possesses exactly four 3-Sylow subgroups, of which exactly one, say P, lies in H. It follows that $H = \mathrm{N}_G(P)$. If a subgroup $H < K < G$ existed, one would have the contradiction

$$|\mathrm{Syl}_3(K)| = |K : \mathrm{N}_K(P)| = |K : H| = 2 \not\equiv 1 \pmod 3.$$

The fundamental theorem of Galois theory implies that $\mathbb{Q}(z)$ has no subfields of degree 2 over $\mathbb{Q}$. Thus z is not constructible, but $|\mathbb{Q}(z) : \mathbb{Q}| = 4$.

Theorem I.15.8 (Problems of Antiquity)**.**

(i) (*Squaring the circle*) *With compass and straightedge, no square can be constructed that has the same area as the unit circle.*

(ii) (*Angle trisection*) *Not every angle can be divided into three equal angles with compass and straightedge.*

(iii) (*Delian problem*) *With compass and straightedge, no cube can be constructed that is twice as large as the unit cube.*

Proof.

(i) Since the unit circle has area π, the side length of the corresponding square is $\sqrt{\pi}$. According to Lindemann, π and $\sqrt{\pi}$ are transcendental. The claim follows from Corollary I.15.6.

(ii) Let us assume that one can trisect 120°. Then one can construct 40° and thus a primitive 9-th root of unity ζ. According to Theorem I.12.12, $|\mathbb{Q}(\zeta) : \mathbb{Q}| = \varphi(9) = 6$ is not a power of 2. The claim follows from Corollary I.15.6.

(iii) The edge length of the corresponding cube is $z := \sqrt[3]{2}$. As is well known, $X^3 - 2$ is the minimal polynomial of z and $|\mathbb{Q}(z) : \mathbb{Q}| = 3$ is not a power of 2. Again, the claim follows from Corollary I.15.6. □

Lemma I.15.9. *If $2^n + 1$ is a prime number with $n \in \mathbb{N}$, then n is a power of 2.*

Proof. If n has an odd divisor $q > 1$, then

$$2^n + 1 = (2^{n/q} + 1) \sum_{i=0}^{q-1} (-2^{n/q})^i \qquad \text{(geometric series)}$$

is not a prime number. □

Remark I.15.10. The prime numbers of the form $F_n := 2^{2^n} + 1$ are called FERMAT-*primes* (cf. Exercise I.4). The only known ones are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$. It holds that

$$\begin{aligned} &641 = 5^4 + 2^4 \mid 2^{28}(5^4 + 2^4) = 5^4 \cdot 2^{28} + 2^{32}, \\ &641 = 5 \cdot 2^7 + 1 \mid (5 \cdot 2^7 + 1)(5 \cdot 2^7 - 1)(5^2 \cdot 2^{14} + 1) = 5^4 \cdot 2^{28} - 1, \\ &641 \,\Big|\, (5^4 \cdot 2^{28} + 2^{32}) - (5^4 \cdot 2^{28} - 1) = 2^{32} + 1 = F_5 \notin \mathbb{P}. \end{aligned}$$

More generally, it is known that $F_n \notin \mathbb{P}$ for $n = 5, \ldots, 32$ (`https://www.fermatsearch.org`).

Theorem I.15.11 (GAUSS[1])**.** *The regular n-gon can be constructed with compass and straightedge if and only if n is the product of a power of 2 and pairwise distinct Fermat primes.*

Proof. The regular n-gon is constructible if and only if one can construct a primitive n-th root of unity $\zeta \in \mathbb{C}$. Let $n = p_1^{a_1} \ldots p_k^{a_k}$ be the prime factorization of n. Then

$$|\mathbb{Q}(\zeta) : \mathbb{Q}| \overset{\text{I.12.12}}{=} \varphi(n) \overset{\text{I.2.38}}{=} p_1^{a_1 - 1}(p_1 - 1) \ldots p_k^{a_k - 1}(p_k - 1).$$

[1] Gauss wrote about this: "Through intense reflection on the connection of all roots with each other according to arithmetic reasons, I succeeded, during a holiday stay in Braunschweig on the morning of the day in question (before I had gotten out of bed), in seeing this connection most clearly, so that I could make the special application to the 17-gon and the numerical confirmation on the spot."

If ζ is constructible, then $\varphi(n)$ is a power of 2 according to Corollary I.15.6. This shows $p_i = 2$ or $p_i^{a_i}$ is a Fermat prime according to Lemma I.15.9 for each $i \in \{1, \ldots, k\}$.

Conversely, if n is the product of a power of 2 and pairwise distinct Fermat primes, then $\varphi(n)$ is a power of 2. According to Theorem I.12.12, $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ is a Galois extension and $G := \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ is a 2-group. By Sylow, there exist $1 = G_0 < \ldots < G_m = G$ with $|G_i : G_{i-1}| = 2$ for $i = 1, \ldots, m$. For $K_i := \mathbb{Q}(\zeta)^{G_{m-i}}$, it then holds that $\mathbb{Q} = K_0 \subseteq \ldots \subseteq K_m = \mathbb{Q}(\zeta)$ with $|K_i : K_{i-1}| = 2$ for $i = 1, \ldots, m$ according to the Fundamental Theorem of Galois Theory. According to Theorem I.15.5, ζ is constructible. □

Example I.15.12.

(i) The regular n-gon can be constructed for $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, \ldots$.

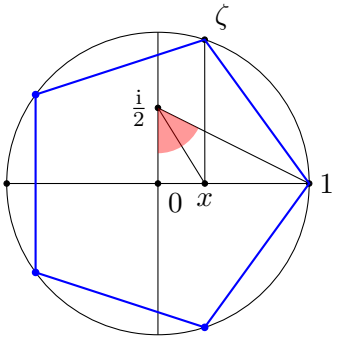
(ii) (Construction of the regular 5-gon) For $\zeta := e^{2\pi \mathrm{i}/5}$ and $\omega := \zeta + \zeta^{-1} = 2\mathrm{Re}(\zeta)$ we have

$$0 = \Phi_5(\zeta) = \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = \zeta^2 + 2 + \zeta^{-2} + \zeta + \zeta^{-1} - 1 = \omega^2 + \omega - 1.$$

This shows $\mathrm{Re}(\zeta) = \frac{\omega}{2} = \frac{1}{4}(\sqrt{5} - 1) \in \mathcal{M}$ (note: $\mathrm{Re}(\zeta) > 0$).

(1) Construct $\frac{\mathrm{i}}{2}$. By Pythagoras, the segment $(\frac{\mathrm{i}}{2}, 1)$ has length $\frac{\sqrt{5}}{2}$.
(2) Bisect the angle $(0, \frac{i}{2}, 1)$. The angle bisector divides the segment $(0, 1)$ in the ratio of the adjacent sides (angle bisector theorem). For the intersection point $x \in \mathbb{R}$ of the angle bisector with the x-axis, it therefore holds that $\frac{x}{1-x} = \frac{1}{\sqrt{5}}$ and

$$x = \frac{1}{\sqrt{5}+1} = \frac{\sqrt{5}-1}{4} = \mathrm{Re}(\zeta).$$



(3) Drop the perpendicular at x. The intersection point of the perpendicular with the unit circle is ζ.
(4) Mark off the segment $(1, \zeta)$ three times on the unit circle.
(5) Connect the resulting points.

Remark I.15.13. According to Gauss, $\zeta := e^{2\pi \mathrm{i}/17}$ can be constructed. Indeed,

$$\mathrm{Re}(\zeta) = \frac{1}{16}\left(2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}} + \sqrt{34 - 2\sqrt{17}} + \sqrt{17} - 1\right)$$

(without proof).

Theorem I.15.14 (Mohr, Mascheroni)**.** *Every constructible point can also be constructed using only a compass.*

Proof. See for example [N. Hungerbühler, *A short elementary proof of the Mohr-Mascheroni Theorem*, Amer. Math. Monthly 101 (1994), 784–787]. □

Exercises

Number Theory

Exercise I.1 (3 points)**.** Solve the equation

$$x^3 - 3x^2 + x - 1 = 0$$

in $\mathbb{C}$.

Exercise I.2 (3 points)**.** Calculate $\gcd(813, 1329)$ and find $a, b \in \mathbb{Z}$ with

$$813a + 1329b = \gcd(813, 1329).$$

Exercise I.3 (2 points)**.** Let $2 \leq b \in \mathbb{N}$. Show that every $n \in \mathbb{N}_0$ can be uniquely written in the form

$$n = \sum_{i=0}^{\infty} n_i b^i \qquad (b\text{-adic expansion})$$

with $0 \leq n_i \leq b - 1$ for $i \geq 0$.

Exercise I.4 $(2 + 2 + 2$ points)**.** For $n \in \mathbb{N}_0$ let $F_n := 2^{2^n} + 1$. Show:

(a) $\prod_{k=0}^{n-1} F_k = F_n - 2$ for $n \in \mathbb{N}_0$.

(b) $\gcd(F_n, F_m) = 1$ for $n \neq m$.

(c) Using (b), give a new proof for $|\mathbb{P}| = \infty$.

Exercise I.5 $(2 + 2$ points)**.**

(a) Show that there are infinitely many prime numbers of the form $4n - 1$.
Hint: Examine the prime divisors of $4p_1 \dots p_k - 1$ with $p_1, \dots, p_k \in \mathbb{P}$.

(b) Show that there are infinitely many prime numbers of the form $6n - 1$.

Exercise I.6 (2 points)**.** Determine the smallest natural number n with the property

$$\forall p \in \mathbb{P} : p \mid n \iff (p - 1) \mid n.$$

Hint: The solution is related to Jena.

Exercise I.7 $(2 + 2 + 2$ points)**.**

(a) Calculate $\operatorname{lcm}(10.403, 10.807)$.

(b) Solve the equation $47x \equiv 27 \pmod{89}$ in $\mathbb{Z}$.

(c) Solve the system

$$\begin{aligned} x &\equiv 11 \pmod{37}, \\ 2x &\equiv 13 \pmod{41}. \end{aligned}$$

Exercise I.8 (2 + 2 + 2 points)**.** Let $n \in \mathbb{N}$. Show:

(a) n is divisible by 3 (resp. 9) if and only if the sum of digits of n is divisible by 3 (resp. 9). (The sum of digits is the sum of the decimal digits.)

(b) n is divisible by 11 if and only if the alternating sum of the decimal digits of n is divisible by 11. (It does not matter whether one starts the sum from the left or right.)

(c) We now group the decimal digits into blocks of 3 starting from the right. n is divisible by 7 if and only if the alternating sum of these blocks is divisible by 7 (Example: $12.345.678 \to 678 - 345 + 12 = 345 = 7 \cdot 50 - 5 \equiv 2 \pmod{7}$).

Exercise I.9 (3 points)**.** (Wilson) Let $2 \leq n \in \mathbb{N}$. Show that n is a prime number if and only if

$$(n-1)! \equiv -1 \pmod{n}$$

holds.

Exercise I.10 (3 points)**.** (Lamé) How large must $a, b \in \mathbb{N}$ at least be so that the Euclidean algorithm for calculating $\gcd(a, b)$ goes through exactly $k \in \mathbb{N}$ iterations?
Hint: The solution leads to a well-known sequence of numbers.

Exercise I.11 (3 points)**.** Five pirates and a monkey are stranded on a desert island. On the first day, they collect n coconuts. During the following night, one pirate wakes up to secure his share. He divides the pile of coconuts into five equal parts, with one coconut left over, which he gives to the monkey. Then he takes one of the five parts to a secret hiding place and goes back to sleep. A short time later, the second pirate also wakes up to perform the same procedure (again, one nut remains for the monkey). During the rest of the night, the remaining three pirates also perform this procedure. The next morning, the remaining pile is distributed in equal parts among the five pirates, and this time no nut is left over. What was the minimum value of n?

Exercise I.12 (2 + 2 points)**.**

(a) Determine all $n \in \mathbb{N}$ with $\varphi(n) = 14$.

(b) Determine the prime factorization of 626.257.
Hint: Does it help to know that $\varphi(626.257) = 624.640$?

Exercise I.13 (3 points)**.** Show that there are 48 consecutive natural numbers that all have a square divisor.
Hint: Use the Chinese Remainder Theorem.

Exercise I.14 (3 points)**.** Show $\gcd(a^n - 1, a^m - 1) = a^{\gcd(n,m)} - 1$ for $a, n, m \in \mathbb{N}$.

Group Theory

Exercise I.15 $(1+1+1+1$ points$)$**.** Determine the cycle types of the elements in S_5. How many elements are there of each type? What order and what sign do these elements have?

Exercise I.16 (3 points)**.** Show:

$$V_4 := \big\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\big\} = \big\langle (1,2)(3,4), (1,3)(2,4)\big\rangle \trianglelefteq S_4.$$

One calls V_4 the *Klein four-group*.

Exercise I.17 $(2+2$ points$)$**.** Let $H \leq G$ be groups. Show:

(a) $H_G := \bigcap_{g\in G} gHg^{-1}$ is the "largest" normal subgroup of G contained in H, i. e. for $N \trianglelefteq G$ with $N \subseteq H$, it holds that $N \subseteq H_G$.

(b) $H^G := \langle \bigcup_{g\in G} gHg^{-1}\rangle$ is the "smallest" normal subgroup of G containing H, i. e. for $N \trianglelefteq G$ with $H \subseteq N$, it holds that $H^G \subseteq N$.

Exercise I.18 $(3+2$ points$)$**.** Show that for every group G the following statements are equivalent:

(1) G is abelian.

(2) $G \to G$, $g \mapsto g^{-1}$ is an automorphism.

(3) $G \to G$, $g \mapsto g^2$ is an endomorphism.

When is $G \to G$, $g \mapsto g^2$ an automorphism (assume $|G| < \infty$ for this)?

Exercise I.19 $(2+2+2+2+2+2$ points$)$**.** Let G be a group and $U, V, W \leq G$. Show:

(a) $U \subseteq V \Longrightarrow |G:U| = |G:V||V:U|$.

(b) $U \cup V \leq G \iff U \cup V \in \{U, V\}$.

(c) $UV \leq G \iff UV = VU$.

(d) $|UV| = |U : U \cap V||V| = |V : U \cap V||U|$.

(e) $U \subseteq W \Longrightarrow UV \cap W = U(V \cap W)$.

(f) If $|G:U|$ and $|G:V|$ are finite and coprime, then $|G : U \cap V| = |G:U||G:V|$ and $G = UV$.

Exercise I.20 $(2+2$ points$)$**.** For $3 \leq n \in \mathbb{N}$ let

$$D_{2n} := \langle \sigma, \tau\rangle \leq \mathrm{Sym}(\mathbb{C})$$

with $\sigma(z) := e^{\frac{2\pi \mathrm{i}}{n}} z$ and $\tau(z) := \bar{z}$ (complex conjugation) for $z \in \mathbb{C}$. Show:

(a) $\langle\sigma\rangle \trianglelefteq D_{2n}$ and $|D_{2n}| = 2n$.

(b) If $\Delta \subseteq \mathbb{C}$ is the regular n-gon in the complex plane with center 0 and vertex 1 (i. e. the convex hull of the n-th roots of unity), then

$$D_{2n} = \{\alpha \colon \mathbb{C} \to \mathbb{C} : \alpha(\Delta) = \Delta,\ |\alpha(x) - \alpha(y)| = |x - y|\ \forall x, y \in \mathbb{C}\},$$

i. e. D_{2n} is the *symmetry group* of the regular n-gon.

One calls D_{2n} the *dihedral group* of order $2n$.

Exercise I.21 $(1 + 1 + 1 + 1$ points$)$**.**

(a) Construct groups $U, V \leq G$ with $UV \not\leq G$.

(b) Construct a group homomorphism $f \colon G \to H$ with $f(G) \not\trianglelefteq H$.

(c) Construct groups $N \trianglelefteq M \trianglelefteq G$ with $N \not\trianglelefteq G$.

(d) Show that A_4 has no subgroup of order 6.

Exercise I.22 $(2 + 2 + 2 + 2 + 2 + 2$ points$)$**.** Let G be a group and $g \in G$. Show:

(a) The map $\alpha_g \colon G \to G,\ x \mapsto gxg^{-1}$ is an automorphism. One calls α_g the *inner automorphism* induced by g.

(b) The map $\alpha \colon G \to \mathrm{Aut}(G),\ g \mapsto \alpha_g$ is a homomorphism. One calls $\mathrm{Inn}(G) := \alpha(G) \leq \mathrm{Aut}(G)$ the *inner automorphism group* of G.

(c) It holds that $G/\mathrm{Z}(G) \cong \mathrm{Inn}(G)$.

(d) If $G/\mathrm{Z}(G)$ is cyclic, then G is abelian (i. e. $G/\mathrm{Z}(G) = 1$).

(e) It holds that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. One calls $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ the *outer automorphism group*.

(f) For $H \leq G$, $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Exercise I.23 (2 points)**.** Show that every group of order 220 has a normal subgroup of order 55.
Hint: First construct a smaller normal subgroup and then use the second isomorphism theorem.

Exercise I.24 (2 points)**.** Show that the 2-Sylow subgroups of S_4 are isomorphic to D_8.
Note: Examine the action of D_8 on the set of fourth roots of unity (see Exercise I.20).

Exercise I.25 $(2 + 2$ points$)$**.** Let $H \leq G$ be groups with $n := |G : H| < \infty$. Show:

(a) $|G : H_G| \leq n!$ with the notation from Exercise I.17.

(b) If G is finite and n is the smallest prime divisor of $|G|$, then $H \trianglelefteq G$ (this generalizes Example I.3.17(iii)).

Note: Examine the action of G on G/H (Remark I.4.6(i)).

Exercise I.26 $(2+2+2+2+2+2$ points**).** Let G be a non-abelian group of order 8. Show:

(a) G possesses an element x of order 4.
Note: Exercise I.18.

(b) For $y \in G \setminus \langle x \rangle$, it holds that $y^4 = 1$ and $yx = x^{-1}y$.

(c) The multiplication table of G is uniquely determined by the order of y.

(d) In the case $y^2 = 1$, $G \cong D_8$.

(e) In the case $y^2 \neq 1$,

$$G \cong Q_8 := \left\langle \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle \leq \mathrm{GL}(2, \mathbb{C})$$

with $\mathrm{i} = \sqrt{-1}$. Q_8 is called the *quaternion group* of order 8.
Note: It suffices to show that Q_8 has the desired properties.

(f) Construct all groups of order 8 up to isomorphism.
Note: Show $D_8 \ncong Q_8$ by counting elements of order 2.

Exercise I.27 (3 points)**.** How many cubes with monochromatic faces exist if five colors are available?
Note: Note that mirrored cubes can be distinguished.

Exercise I.28 (2 points)**.** Determine all abelian groups of order 720 up to isomorphism.

Exercise I.29 $(2+2$ points**).**

(a) Let G be a finite abelian group. Show that there exist uniquely determined numbers $d_1, \ldots, d_n \in \mathbb{N} \setminus \{1\}$ with $G \cong C_{d_1} \times \ldots \times C_{d_n}$ and $d_1 \mid d_2 \mid \ldots \mid d_n$.

(b) Let $N \trianglelefteq G \cong C_{q_1} \times \ldots \times C_{q_n}$ with prime powers $q_1, \ldots, q_n$. Show that there exist divisors $r_i \mid q_i$ for $i = 1, \ldots, n$ with $G/N \cong C_{r_1} \times \ldots \times C_{r_n}$.

Exercise I.30 $(1+1+1+1$ points**).** Show that all groups of orders $40, 42, 45, 56$ are solvable.

Exercise I.31 $(2+2+2$ points**).** For a group G and $x, y \in G$, one calls $[x, y] := xyx^{-1}y^{-1}$ the *commutator* of x and y. Furthermore,

$$G' := \langle [x, y] : x, y \in G \rangle$$

is the *derived subgroup* of G. With $G^{(0)} := G$, let $G^{(n+1)} := (G^{(n)})'$ for $n \geq 0$. Show that:

(a) From $G' \subseteq H \leq G$ it follows that $H \trianglelefteq G$ and G/H is abelian.
Hint: First consider the case $G' = H$ and use the second isomorphism theorem for the general case.

(b) If $N \trianglelefteq G$ with abelian quotient group G/N, then $G' \leq N$ holds. (Therefore G' is the "smallest" normal subgroup with an abelian quotient group.)

(c) Now let $|G| < \infty$. G is solvable if and only if there exists an $n \in \mathbb{N}$ with $G^{(n)} = 1$.
Hint: Argue by induction on $|G|$.

Exercise I.32 (2 + 2 points)**.** For a finite group G and a prime divisor p of $|G|$, let

$$\Omega := \{(x_1, \ldots, x_p) \in G^p : x_1 \ldots x_p = 1\}.$$

(a) Show that $\mathbb{Z}/p\mathbb{Z}$ acts on Ω by

$$^{k+p\mathbb{Z}}(x_1, \ldots, x_p) := (x_{1+k}, \ldots, x_{p+k}),$$

where the indices are to be read modulo p.

(b) (McKay) Use the class equation to derive Cauchy's theorem.

Exercise I.33 (2 points)**.** Show that $\mathrm{Aut}(S_3) \cong S_3$.

Exercise I.34 (2 points)**.** (Landau) Let $n \in \mathbb{N}$. Show that there are only finitely many finite groups G with $k(G) = n$.
Hint: Show that the class equation in the form $1 = \frac{1}{|\mathrm{C}_G(x_1)|} + \ldots + \frac{1}{|\mathrm{C}_G(x_n)|}$ has only finitely many solutions.

Exercise I.35 (3 points)**.** Show that the power set $\mathcal{P}(\Omega)$ of a finite set Ω with the *symmetric difference*

$$A \ominus B := (A \cup B) \setminus (A \cap B) \qquad (A, B \subseteq \Omega)$$

becomes a group and determine its isomorphism type.

Ring Theory

Exercise I.36 (2 points)**.** Show that every finite integral domain is a field.

Exercise I.37 (2 + 2 + 2 + 2 points)**.** Let R be a ring and $I, J \trianglelefteq R$. Show that:

(a) $I \cap J \trianglelefteq R$.

(b) $I + J := \{x + y : x \in I,\, y \in J\} \trianglelefteq R$.

(c) $IJ := \left\{\sum_{i=1}^{k} x_i y_i : k \in \mathbb{N},\, x_i \in I,\, y_i \in J\right\} \trianglelefteq R$.

(d) $IJ \subseteq I \cap J \subseteq I + J$.

Exercise I.38 (2 + 2 points)**.** Let R be a ring with subring $S \subseteq R$ and $I, J \trianglelefteq R$ with $I \subseteq J$. Prove:

(a) $S + I$ is a subring of R, $I \trianglelefteq S + I$, $S \cap I \trianglelefteq S$ and $S/(S \cap I) \cong (S + I)/I$.

(b) $J/I \trianglelefteq R/I$ and $(R/I)/(J/I) \cong R/J$.

Hint: Use the isomorphism theorem.

Exercise I.39 (2 + 2 + 2 points)**.** Let K be a field and $n \in \mathbb{N}$. Show:

(a) The upper triangular matrices form a subring R of $K^{n \times n}$.

(b) The upper triangular matrices with zeros on the main diagonal form an ideal I of R.

(c) There exists a ring isomorphism $R/I \cong K^n$.

Exercise I.40 $(2+2+2+2$ points$)$**.** Let R be an integral domain.

(a) Show that

$$(x,y) \sim (x',y') :\Longleftrightarrow xy' = x'y$$

defines an equivalence relation on $R \times (R \setminus \{0\})$. Let $[x,y]$ be the equivalence class of (x,y).

(b) Show that $Q(R) := \{[x,y] : x,y \in R,\ y \neq 0\}$ with the operations

$$[a,b] + [c,d] := [ad+bc, bd],$$
$$[a,b] \cdot [c,d] := [ac, bd]$$

becomes a field. $Q(R)$ is called the *field of fractions* of R.

(c) Show that the map $R \to Q(R)$, $x \mapsto [x,1]$ is a ring monomorphism. In this way, R can be regarded as a subring of $Q(R)$.

(d) (Universal property) For every field K and every ring monomorphism $f\colon R \to K$ there exists exactly one field homomorphism $g\colon Q(R) \to K$ with $g([x,1]) = \alpha(x)$ for $x \in R$, i. e. g extends f. Therefore $Q(R)$ is the "smallest" field containing R.

Remark: This generalizes the construction of $\mathbb{Q}$ from $\mathbb{Z}$.

Exercise I.41 $(2+2$ points$)$**.**

(a) Write $(\mathbb{Z}/2200\mathbb{Z})^\times$ as a direct product of cyclic groups of prime power order.

(b) Determine all generators of $(\mathbb{Z}/22\mathbb{Z})^\times$.

Exercise I.42 $(1+3$ points$)$**.**

(a) Determine the period length in the decimal expansion of $1/22$ and $1/23$.

(b) Let $n \in \mathbb{N}$ with $\gcd(n,10) = 1$. Show that the period length $\rho(n)$ in the decimal expansion of $1/n$ is exactly the order of $10 + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. Conclude $\rho(n) \mid \varphi(n)$.

Remark: An open conjecture of Gauss states that there are infinitely many prime numbers p with $\rho(p) = p-1$.

Exercise I.43 $(2+2+2+2$ points$)$**.** Let $1 \neq n \in \mathbb{N} \setminus \mathbb{P}$ with $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}$ with $\gcd(a,n) = 1$. Show:

(a) (Korselt) For every prime divisor p of n, $n \equiv 1 \pmod{p-1}$ holds.
Hint: The equation $a^{n-1} \equiv 1 \pmod{n}$ restricts the order of the elements in $(\mathbb{Z}/n\mathbb{Z})^\times$.

(b) n is odd and square-free.

(c) n has at least three prime divisors.

(d) There exists such an n. Such n are called Carmichael numbers.

Remark: The converse of "Fermat's Little Theorem" (Corollary I.7.18) is therefore false. Nevertheless, this is a useful primality test.

Exercise I.44 (2 points)**.** Prove that the automorphism group of $(\mathbb{Z}, +)$ is isomorphic to C_2.

Exercise I.45 (2 points)**.** (*Universal property* of the polynomial ring) Let $\varphi\colon R \to S$ be a homomorphism of commutative rings R, S and $s \in S$. Show that φ has exactly one extension $\hat{\varphi}\colon R[X] \to S[X]$ with $\hat{\varphi}(X) = s$.

Exercise I.46 $(2 + 2$ points)**.** Let K be a field and $\alpha \in K[X]$.

(a) Describe $(K[X]/(\alpha))^\times$.

(b) Calculate $(X^3 + X + 1 + (\alpha))^{-1}$ in $\mathbb{F}_2[X]/(\alpha)$ for $\alpha = X^4 + X^2 + 1 \in \mathbb{F}_2[X]$ (if the inverse exists).

Exercise I.47 $(2 + 2 + 2 + 2$ points)**.** Investigate which of the following polynomials are irreducible in $\mathbb{Q}[X]$:

(a) $X^3 - 2X^2 - 18X + 15$

(b) $X^3 + \frac{2}{3}X^2 + \frac{1}{3}X + 1$

(c) $X^4 + 4X^2 + X + 6$

(d) $X^5 + 20X + 16$
Hint: Eisenstein.

Exercise I.48 $(2 + 3$ points)**.**

(a) Show that $(2, X)$ is not a principal ideal in $\mathbb{Z}[X]$ and determine $\mathbb{Z}[X]/(2, X)$.

(b) Prove or disprove: $\mathbb{Z}[X]/(X^2 - 1) \cong \mathbb{Z}^2$.

Exercise I.49 $(2 + 2$ points)**.** Show that

$$R := \left\{ a + b\frac{1 + \sqrt{-3}}{2} : a, b \in \mathbb{Z} \right\}$$

is a subring of $\mathbb{C}$ and determine $R^\times$.
Remark: The elements of R are called *Eisenstein integers*.

Exercise I.50 (2 points)**.** Show that

$$\mathbb{H} := \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$$

as a subring of $\mathbb{C}^{2\times 2}$ is a non-commutative division ring. $\mathbb{H}$ is called, after HAMILTON, the *quaternion division ring* (cf. Exercise I.26).

Exercise I.51 (2 points)**.** Let $n \in \mathbb{N}$ and $d \mid n$. Show that $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$, $k + n\mathbb{Z} \mapsto k + d\mathbb{Z}$ is a well-defined group epimorphism.

Exercise I.52 (2 points)**.** Let $2 < p \in \mathbb{P}$ and $a \in \mathbb{Z}$ with $(\mathbb{Z}/p^2\mathbb{Z})^\times = \langle a + p^2\mathbb{Z}\rangle$. Show that $(\mathbb{Z}/p^n\mathbb{Z})^\times = \langle a + p^n\mathbb{Z}\rangle$ for all $n \geq 2$.

Field Theory

Exercise I.53 ($2 + 2$ points)**.** Show that $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}_\mathbb{Q}\}$ and $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}_\mathbb{R}\}$.
Hint: The second statement follows from the first if you can show that every automorphism is continuous. For this, use the fact that every positive real number has a real square root.

Exercise I.54 (4 points)**.** Decide which of the following numbers are algebraic over $\mathbb{Q}$

$$\sqrt[5]{1+\sqrt{2}},\ e^{3\pi i/5},\ \sqrt{2}+\sqrt[3]{5},\ \pi^2\mathrm{i}.$$

Hint: You may use the transcendence of π.

Christmas puzzle (+3 extra points)**.** Determine without a computer the 42nd decimal place of

$$\left(\sqrt{2}+\sqrt{3}\right)^{666}.$$

Hint: One can use Example I.10.12, but it can also be done elementarily.

Exercise I.55 ($2 + 2 + 2 + 2 + 2 + 2$ points)**.** According to Example I.10.10, the splitting field K of $X^3 - 2$ forms a Galois extension over $\mathbb{Q}$.

(a) Determine $|K : \mathbb{Q}|$.

(b) Determine $G := \mathrm{Gal}(K|\mathbb{Q})$.

(c) Determine all subgroups of G.

(d) Determine all subfields of K.

(e) Which subfields of K form Galois extensions over $\mathbb{Q}$?

(f) Find an $x \in K$ with $K = \mathbb{Q}(x)$.

Remark: This is the algebraic version of a curve sketching.

Exercise I.56 (2 points)**.** Show that the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

Exercise I.57 (2 points)**.** Let K be a field with $\mathrm{char}\, K \neq 2$ or $|K| < \infty$. Show that every field extension of degree 2 over K is a Galois extension.

Exercise I.58 (2 + 2 points)**.** Let K be a field and $\alpha \in K[X]$. The *k-th derivative* $\alpha^{(k)}$ is defined inductively by $\alpha^{(0)} := \alpha$ and $\alpha^{(k)} := (\alpha^{(k-1)})'$. Show for $\alpha, \beta \in K[X]$ and $x \in K$:

(a) $(\alpha(\beta))' = \alpha'(\beta)\beta'$ (chain rule).

(b) $\alpha = \sum_{k=0}^{\infty} \frac{\alpha^{(k)}(x)}{k!}(X - x)^k$, if $\operatorname{char} K = 0$ (Taylor series).

Exercise I.59 (4 points)**.** Construct $\mathbb{F}_9$ and provide the corresponding operation tables.

Exercise I.60 (2 + 2 + 2 points)**.** Let $p \in \mathbb{P}$, $k, n \in \mathbb{N}$ and $q := p^k$.

(a) Determine the orders of $\mathrm{GL}(n, \mathbb{F}_q)$ and $\mathrm{SL}(n, \mathbb{F}_q)$.
Hint: A square matrix is invertible if and only if its rows are linearly independent.

(b) Show that the upper triangular matrices with ones on the main diagonal form a Sylow p-subgroup P_n of $\mathrm{SL}(n, \mathbb{F}_q)$. Is $P_n \in \mathrm{Syl}_p(\mathrm{GL}(n, \mathbb{F}_q))$ as well?

(c) Show that $|\mathrm{Syl}_p(\mathrm{SL}(2, \mathbb{F}_p))| = p + 1$.
Hint: The normalizer of P_2 contains diagonal matrices.

Exercise I.61 (2 + 2 points)**.** Let $I_d(p)$ be the number of irreducible polynomials of degree d over $\mathbb{F}_p$. Derive a formula for $I_d(p)$ by applying Möbius inversion (Theorem I.2.42) to Lemma I.11.17. Use this to calculate $I_{12}(2)$.

Exercise I.62 (4 points)**.** Show that every ring with exactly four elements is isomorphic to exactly one of the following rings:

$$\mathbb{Z}/4\mathbb{Z}, \qquad \mathbb{F}_4, \qquad \mathbb{F}_2^2, \qquad \mathbb{F}_2[X]/(X^2).$$

Exercise I.63 (2 + 2 + 2 points)**.** Let $K := \mathbb{F}_2(X)$ be the field of rational functions over $\mathbb{F}_2$. Let L be a splitting field of $Y^2 - X$ over $K[Y]$. Show:

(a) The Frobenius homomorphism on K is not surjective.

(b) $|L : K| = 2$.

(c) $K \subseteq L$ is not a Galois extension.

Exercise I.64 (2 + 2 + 2 points)**.**

(a) Show that every irreducible polynomial in $\mathbb{R}[X]$ has degree 1 or 2.

(b) Calculate the cyclotomic polynomial Φ_{15}.

(c) Show that $\Phi_{2n}(X) = \Phi_n(-X)$ for every odd number $n > 1$.

Exercise I.65 (3 points)**.** Determine all subfields of $\mathbb{Q}_{15}$ with degree 2 over $\mathbb{Q}$.

Exercise I.66 (3 points)**.** Construct a Galois extension $\mathbb{Q} \subseteq K$ with $\mathrm{Gal}(K|\mathbb{Q}) \cong C_7$.
Hint: It suffices to specify a primitive element. Use the proof of Theorem 12.18 for this.

Exercise I.67 (3 points)**.** Let K be a field with algebraic closure $\overline{K}$. Let $K \subseteq L$ and $K \subseteq M$ be Galois extensions with $L, M \subseteq \overline{K}$. Show that L and M are K-isomorphic if and only if $L = M$.
Remark: In the case $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{F}_p\}$, one can replace "$K$-isomorphic" with "isomorphic", because $\mathrm{Aut}(K) = 1$.

Solvability of Equations

Exercise I.68 (2 points)**.** Write the symmetric polynomial

$$X^2Y^2 + X^2Z^2 + Y^2Z^2 + 1$$

as a polynomial of elementary symmetric polynomials.

Exercise I.69 (3 points)**.** Let $\alpha \in \mathbb{Z}[X]$ be monic. Show that D_α is congruent to 0 or 1 modulo 4.
Hint: For the roots $x_1, \ldots, x_n \in \mathbb{C}$ of α, it holds that $D_\alpha = \prod_{i<j}\big((x_i + x_j)^2 - 4x_ix_j\big)$.

Exercise I.70 (3 points)**.** Let $x, y, z \in \mathbb{C}$ be the roots of $X^3 + 2X^2 - 3X + 1 \in \mathbb{Q}[X]$. Calculate $x^3 + y^3 + z^3$.
Note: One does not need to calculate x, y, z for this.

Exercise I.71 (3 points)**.** Solve the non-linear system of equations

$$\begin{aligned} x + y + z &= 3, \\ x^2 + y^2 + z^2 &= 15, \\ x^3 + y^3 + z^3 &= 45. \end{aligned}$$

Exercise I.72 (2 + 2 points)**.** Let K be a field and $G \leq K^\times$ with $n := |G| < \infty$. Let $d \mid n$.

(a) Show with the help of Theorem I.8.29 that G has at most $\varphi(d)$ elements of order d.

(b) Conclude with the help of Example I.2.43 that G is cyclic.

Remark: This is an elementary proof of Theorem I.8.31.

Exercise I.73 (2 + 2 points)**.**

(a) Determine the Galois group of $X^4 - X^3 + 1$.

(b) Construct a polynomial $\alpha \in \mathbb{Q}[X]$ with $\mathrm{Gal}(\alpha) \cong A_4$.

Exercise I.74 (2 + 2 + 2 + 2 points)**.**

(a) Show that every constructible point $z \in \mathbb{C}$ is a root of a solvable polynomial in $\mathbb{Q}[X]$.

(b) Let $n, m \in \mathbb{N}$ be coprime, such that the regular n- and m-gons are constructible. Show without using Theorem I.15.11 that the mn-gon is constructible.

(c) Express $\cos(\frac{2\pi}{2^n})$ for $n \in \mathbb{N}$ using rational numbers, basic arithmetic operations, and square roots.
Note: This is possible because the regular 2^n-gon is constructible.

(d) Justify why $\cos(2\pi/7)$ can be expressed using rational numbers, basic arithmetic operations, square roots, and cubic roots.

Algebra II

II.1 Set Theory

Remark II.1.1. In linear algebra, one proves the existence of bases for finitely generated vector spaces. In Theorem I.13.14, we constructed the algebraic closure for countable fields. To be able to prove these and other statements without finiteness conditions, one needs variants of the axiom of choice from set theory.

Theorem II.1.2 (Cantor-Bernstein[1])**.** *Let A and B be sets with injective maps $f\colon A \to B$ and $g\colon B \to A$. Then A and B have the same cardinality.*

Proof. We define $C_0 := A \setminus g(B)$ and $C_n := g(f(C_{n-1}))$ for $n \geq 1$. Furthermore, let $C := \bigcup_{n=0}^{\infty} C_n$ and $h\colon A \to B$ with

$$h(x) := \begin{cases} f(x) & \text{if } x \in C, \\ g^{-1}(x) & \text{if } x \notin C. \end{cases}$$

In the case $x \notin C$, then $x \notin C_0$, i. e. $x \in g(B)$. Consequently, $g^{-1}(x)$ is uniquely determined by the injectivity of g and h is well-defined. Now let $x, y \in A$ with $h(x) = h(y)$. Assume $x \in C$ and $y \notin C$. Then $f(x) = g^{-1}(y)$ and $g(f(x)) = y$. Let $x \in C_n$ for some $n \geq 0$. Then the contradiction $y = g(f(x)) \in g(f(C_n)) = C_{n+1} \subseteq C$ follows. Thus $x, y \in C$ or $x, y \notin C$ holds and one obtains $x = y$. Therefore h is injective.

Now let $y \in B$ be arbitrary. In the case $g(y) \notin C$, then $h(g(y)) = g^{-1}(g(y)) = y$. So let $g(y) \in C_n$ for some $n \geq 1$. Then there exists an $x \in C_{n-1}$ with $g(f(x)) = g(y)$. From the injectivity of g it follows that $h(x) = f(x) = y$. Thus h is also surjective and bijective. □

Definition II.1.3. Let $\leq$ be an order relation (reflexive, transitive and antisymmetric) on a set A and $B \subseteq A$.

(i) As usual, we use the notations $a \geq a'$ (if $a' \leq a$), $a < a'$ (if $a \leq a' \neq a$) and $a > a'$ (if $a' \leq a \neq a'$) for $a, a' \in A$.

(ii) An element $b \in B$ is called

- *greatest element* of B, if $\forall b' \in B : b' \leq b$.
- *maximal element* of B, if $\nexists b' \in B : b < b'$.

(iii) An element $a \in A$ is called an *upper bound* of B, if $\forall b \in B : b \leq a$. Analogously, one defines *least element*, *minimal element* and *lower bound*.

(iv) A is called *totally ordered* (or a *chain*), if $\forall a, a' \in A : (a \leq a' \vee a' \leq a)$.[2]

(v) A is called *well-ordered*, if every non-empty subset of A contains a least element.

[1] also called the Schröder-Bernstein theorem, see [A. Hinkis, *Proofs of the Cantor-Bernstein Theorem*, Springer, Heidelberg, 2013]

[2] If A is finite, then the elements can be arranged in a "chain" $A = \{a_1 < \ldots < a_n\}$.

Example II.1.4. The divisibility relation | on $A := \{1, \dots, 10\}$ is an order relation. Because $\operatorname{lcm}(A) > 10$, A has no greatest element. On the other hand, $6, \dots, 10$ are the maximal elements of A. Finally, 6 is the only upper bound of $B := \{2, 3\}$. Because $2 \nmid 3 \nmid 2$, A is not totally ordered. Since B has no least element, A is also not well-ordered.

Remark II.1.5.

(i) In general, neither greatest elements, nor maximal elements, nor upper bounds exist. Greatest elements are maximal and unique, if they exist. Well-ordered sets are always totally ordered. Finite totally ordered sets are well-ordered.

(ii) In the following, we use the *Axiom of Choice*: If $(M_i)_{i \in I}$ is a family of non-empty sets, then the Cartesian product $\bigtimes_{i \in I} M_i$ is also non-empty.

Theorem II.1.6 (Zorns Lemma)**.** *Let M be an ordered set in which every totally ordered subset has an upper bound. Then M contains a maximal element.*

Proof (Weston). Since the empty subset has an upper bound, M itself is not empty. By the axiom of choice, there exists a function f that assigns an element $f(N) \in N$ to every non-empty subset $N \subseteq M$. For every totally ordered subset $N \subseteq M$, let $\hat{N}$ be the set of upper bounds of N in $M \setminus N$ ($\hat{N} = \varnothing$ is possible). Such an N is called *special* if for all $A \subseteq N$ it holds that

$$f(\hat{A}) \text{ is minimal in } \hat{A} \cap N \text{ or } \hat{A} \cap N = \varnothing.$$

We show that the union N_0 of all special subsets is totally ordered. For $x, y \in N_0$, there exist special subsets $N_1, N_2 \subseteq M$ with $x \in N_1$ and $y \in N_2$. In the case $x \in N_2$, it holds that $x \leq y$ or $y \leq x$, since N_2 is totally ordered. So let $x \notin N_2$ and

$$A := \{a \in N_1 \cap N_2 : a < x\}.$$

Since N_1 is special and $x \in \hat{A} \cap N_1$, $f(\hat{A}) \in N_1$ and $f(\hat{A}) \leq x$. In the case $\hat{A} \cap N_2 \neq \varnothing$, analogously $f(\hat{A}) \in N_2$ and one would have the contradiction $f(\hat{A}) \in A \cap \hat{A} = \varnothing$. Therefore $y \notin \hat{A}$ and there exists an $a \in A$ with $y < a < x$, since N_2 is totally ordered.

Now we prove that N_0 is special. For this, let $A \subseteq N_0$ with $\hat{A} \cap N_0 \neq \varnothing$. Then there exists a special subset $N \subseteq N_0$ with $f(\hat{A})$ minimal in $\hat{A} \cap N$. If $f(\hat{A})$ were not minimal in $\hat{A} \cap N_0$, then there exists $x \in \hat{A} \cap N_0$ with $x < f(\hat{A})$. But one could choose N with $x \in N$ and in this way obtain a contradiction. Thus N_0 is special. Now we assume $\hat{N_0} \neq \varnothing$ and consider the totally ordered set

$$N_1 := N_0 \cup \{f(\hat{N_0})\}.$$

Let $A \subseteq N_1$ with $\hat{A} \cap N_1 \neq \varnothing$. In the case $\hat{A} \cap N_0 \neq \varnothing$, $f(\hat{A})$ is minimal in $\hat{A} \cap N_0$ and also in $\hat{A} \cap N_1$. Therefore let $\hat{A} \cap N_0 = \varnothing$, $f(\hat{N_0}) \in \hat{A}$ and $A \subseteq N_0$. Then for every $x \in N_0$ there exists an $a \in A$ with $x < a$, since N_0 is totally ordered. It follows that $\hat{A} \subseteq \hat{N_0} \subseteq \hat{A}$. Thus $f(\hat{A}) = f(\hat{N_0})$ is minimal in $\{f(\hat{N_0})\} = \hat{N_0} \cap N_1 = \hat{A} \cap N_1$. Consequently N_1 is special, in contradiction to the construction of N_0. This shows $\hat{N_0} = \varnothing$. By assumption, there exists an upper bound $m \in M$ of N_0. Here $m \in N_0$ holds and m is the only upper bound of N_0. Thus m is maximal in M. □

Remark II.1.7. One can show that Zorn's Lemma is equivalent to the axiom of choice. The same holds for the *well-ordering theorem*: every set can be well-ordered. Furthermore, Zorn's Lemma also holds in the dual version for lower bounds and minimal elements by replacing $\leq$ with $\geq$.

Example II.1.8. Let F be a (finite) set of women and M a set of men. For $f \in F$, let $M_f \subseteq M$ be the set of friends of f. In order for every woman f to find a partner in M_f, it must obviously hold that $|\bigcup_{e\in E} M_e| \geq |E|$ for all $E \subseteq F$ (assuming monogamy). The next theorem shows that this condition is even sufficient.

Theorem II.1.9 (HALLs Heiratssatz)**.** *Let $(M_i)_{i\in I}$ be a family of subsets of a set M with $|I| < \infty$ or $\forall i \in I : |M_i| < \infty$. Pairwise distinct $x_i \in M_i$ for $i \in I$ exist if and only if $|\bigcup_{i\in J} M_i| \geq |J|$ holds for every finite subset $J \subseteq I$.*

Proof. For $J \subseteq I$ we write $M_J := \bigcup_{i\in J} M_i$. Assume that pairwise distinct $x_i \in M_i$ exist (one calls $(x_i)_{i\in I}$ a *system of representatives*). Obviously, then $|M_J| \geq |\{x_i : i \in J\}| = |J|$ for every finite subset $J \subseteq I$. Conversely, let the condition

$$|M_J| \geq |J| \qquad (J \subseteq I,\ |J| < \infty) \tag{II.1.1}$$

be satisfied. We distinguish two cases:

Case 1: $|I| < \infty$.
Induction on $n := |I|$: The case $n \leq 1$ is obvious. So let $n > 1$ and wlog. $I = \{1, \ldots, n\}$. A subset $J \subseteq I$ is called *critical* , if $1 \leq |M_J| = |J| < n$ holds.

Assume first that no critical subsets exist. Because of $|M_1| = |M_{\{1\}}| \geq 1$ there exists an $x_1 \in M_1$. For $i \in J := \{2, \ldots, n\}$ let $N_i := M_i \backslash \{x_1\}$. For every subset $K \subseteq J$ it then holds that $|N_K| \geq |M_K| - 1 \geq |K|$, because K is not critical. Thus $(N_i)_{i\in J}$ satisfies condition (II.1.1) and by induction there exists a system of representatives $(x_i)_{i\in J}$ of $(N_i)_{i\in J}$. Then surely $(x_i)_{i\in I}$ is a system of representatives for $(M_i)_{i\in I}$.

Assume finally that a critical subset $J \subseteq I$ exists. Then $1 \leq m := |J| = |M_J| < n$ holds. By induction $(M_i)_{i\in J}$ possesses a system of representatives $(x_i)_{i\in J}$. For $i \in I \setminus J$ let $N_i := M_i \setminus M_J$. For every subset $K \subseteq I \setminus J$ it then holds that

$$|N_K| = |M_K \setminus M_J| = |M_{K\cup J}| - |M_J| \geq |K \cup J| - m = |K| + |J| - m = |K|,$$

i. e. $(N_i)_{i\in I\setminus J}$ satisfies (II.1.1). By induction there exists a system of representatives $(x_i)_{i\in I\setminus J}$. By construction $(x_i)_{i\in I}$ is then a system of representatives for $(M_i)_{i\in I}$.

Case 2: $\forall i \in I : |M_i| < \infty$.
Let $\mathcal{M}$ be the set of all families $(N_i)_{i\in I}$ with $N_i \subseteq M_i$ (for all $i \in I$), for which (II.1.1) holds. Because of $(M_i)_{i\in I} \in \mathcal{M}$, $\mathcal{M}$ is non-empty and ordered by

$$(N_i)_{i\in I} \leq (N'_i)_{i\in I} :\Longleftrightarrow \forall i \in I : N_i \subseteq N'_i.$$

Let $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ be a totally ordered subset and $K_j := \bigcap_{(N_i)_{i\in I}\in\mathcal{N}} N_j$ for $j \in I$. Then $(K_i)_{i\in I} \leq (N_i)_{i\in I}$ for all $(N_i)_{i\in I} \in \mathcal{N}$. Let $J \subseteq I$ be a finite subset and $j \in J$. Because of $|M_j| < \infty$ there exists a finite subset $\mathcal{N}_1 \subseteq \mathcal{N}$ with

$$K_j = \bigcap_{(N_i)_{i\in I}\in\mathcal{N}_1} N_j$$

for all $j \in J$. Since $\mathcal{N}$ is totally ordered, $\mathcal{N}_1$ possesses a smallest element $(N_i)_{i\in I}$. Obviously, then $(K_j)_{j\in J} = (N_j)_{j\in J}$. In particular, $|K_J| = |N_J| \geq |J|$. This shows that $(K_i)_{i\in I}$ satisfies condition (II.1.1) and thus is a lower bound of $\mathcal{N}$ in $\mathcal{M}$. By Zorn's Lemma there exists a minimal element $(N_i)_{i\in I} \in \mathcal{M}$. Since every system of representatives of $(N_i)_{i\in I}$ is also a system of representatives of $(M_i)_{i\in I}$, we can replace $(M_i)_{i\in I}$ by $(N_i)_{i\in I}$ and assume $\mathcal{M} = \{(M_i)_{i\in I}\}$.

Let $x \in M_I$ and $N_i := M_i \setminus \{x\}$ for $i \in I$. Because of $(N_i)_{i\in I} \notin \mathcal{M}$ there exists a finite subset $J \subseteq I$ with $|M_J| - 1 \leq |N_J| < |J| \leq |M_J|$. It follows that $|M_J| = |J|$ and $x \in M_J$. We now define

$$N_i := \begin{cases} M_i & \text{if } i \in J, \\ M_i \setminus M_J & \text{if } i \in I \setminus J. \end{cases}$$

Let $K \subseteq I$ be finite. Then

$$\begin{aligned} |N_K| &= |N_{K\cap J} \cup N_{K\setminus J}| = |M_{K\cap J}| + |M_{K\setminus J} \setminus M_J| \\ &= |M_{K\cap J}| + |M_{K\cup J}| - |M_J| \geq |K \cap J| + |K \cup J| - |J| = |K|. \end{aligned}$$

This shows $(N_i)_{i\in I} \in \mathcal{M} = \{(M_i)_{i\in I}\}$ and $M_i \cap M_J = \varnothing$ for $i \in I \setminus J$. It follows that $M_{I\setminus J} \cap M_J = \varnothing$. By Case 1 there exist pairwise distinct $x_i \in M_i$ for $i \in J$. If one now sets

$$N_i := \begin{cases} \{x_i\} & \text{if } i \in J, \\ M_i & \text{if } i \in I \setminus J, \end{cases}$$

then $(N_i)_{i\in I}$ again satisfies (II.1.1). Thus $M_i = \{x_i\}$ for $i \in J$. Since x was chosen arbitrarily, even $|M_i| = 1$ holds for all $i \in I$. Obviously, the M_i are also pairwise disjoint and the claim follows. □

Remark II.1.10. Theorem II.1.9 does not hold for $|I| = \infty$ if not all M_i are finite: Choose $I := \mathbb{N} =: M_1$ and $M_i := \{i - 1\}$ for $i \geq 2$.

II.2 Applications of Zorn's Lemma

Remark II.2.1. In the following, let V be a vector space over a field K. A subset $S \subseteq V$ is called *linearly dependent* if pairwise distinct $s_1, \ldots, s_n \in S$ ($n \in \mathbb{N}$) and $\lambda_1, \ldots, \lambda_n \in K^\times$ with $\sum_{i=1}^n \lambda_i s_i = 0$ exist. Otherwise, S is called *linearly independent*. A linearly independent subset $B \subseteq V$ is called a *basis* of V if

$$V = \sum_{b \in B} Kb =: \operatorname{Span}_K B =: \langle B \rangle.$$

The following theorem is proven in linear algebra only for finitely generated vector spaces.

Theorem II.2.2 (Basis Extension Theorem)**.** *Let V be a vector space with generating set $E \subseteq V$ and linearly independent subset $U \subseteq E$. Then there exists a basis B of V with $U \subseteq B \subseteq E$. In particular, every vector space has a basis.*[1]

Proof. The set $\mathcal{M}$ of all linearly independent subsets $M \subseteq V$ with $U \subseteq M \subseteq E$ is non-empty because of $U \in \mathcal{M}$ and ordered by $\subseteq$. Let $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ be a totally ordered subset. Then $U \subseteq W := \bigcup_{M \in \mathcal{N}} M \subseteq E$. Let $\sum_{i=1}^n \lambda_i w_i = 0$ with $\lambda_1, \ldots, \lambda_n \in K$ and $w_1, \ldots, w_n \in W$ pairwise distinct. Then there exist $M_1, \ldots, M_n \in \mathcal{N}$ with $w_i \in M_i$ for $i = 1, \ldots, n$. Since $\mathcal{N}$ is totally ordered, we can assume $M_1 \subseteq M_2 \subseteq \ldots \subseteq M_n$. In particular, $w_1, \ldots, w_n \in M_n$. Since M_n is linearly independent, it follows that $\lambda_1 = \ldots = \lambda_n = 0$. Therefore, $W \in \mathcal{M}$ is an upper bound of $\mathcal{N}$. By Zorn's Lemma, $\mathcal{M}$ has a maximal element B. By the definition of $\mathcal{M}$, B is linearly independent. For $e \in E \setminus B$, $B \cup \{e\}$ is linearly dependent, because $B \subsetneq B \cup \{e\} \subseteq E$. Thus $e \in \langle B \rangle$ and $V = \langle E \rangle \subseteq \langle B \rangle$. This shows that B is a basis of V. The second statement follows by choosing $U = \varnothing$ and $E = V$. □

Corollary II.2.3. *Every subspace U of a vector space V has a* complement $W \leq V$*, i. e. $V = U \oplus W$.*

Proof. According to Theorem II.2.2, a basis C of U can be extended to a basis B of V. The claim then follows with $W := \langle B \setminus C \rangle$. □

Theorem II.2.4. *Any two bases of a vector space have the same cardinality.*

Proof. Let B and C be bases of a vector space V. For each $b \in B$, there exists a finite subset $C_b \subseteq C$ with $b \in \langle C_b \rangle$. Thus $V = \langle B \rangle \subseteq \langle \bigcup_{b \in B} C_b \rangle$ and $\bigcup_{b \in B} C_b = C$, since C is a minimal generating set of V. Let $B_1 \subseteq B$ be a finite subset and $C_1 := \bigcup_{b \in B_1} C_b$. Then B_1 is a linearly independent subset in the vector space $U := \langle C_1 \rangle$ with $\dim U = |C_1| < \infty$. From linear algebra it follows that $|B_1| \leq |C_1|$. By the marriage theorem, there exist pairwise distinct $c_b \in C_b$ for $b \in B$. The map $B \to C$, $b \mapsto c_b$ is therefore injective. For reasons of symmetry, there must also be an injective map $C \to B$ and the claim follows by Cantor-Bernstein. □

[1] In functional analysis, one speaks of *Hamel bases*.

Remark II.2.5. The cardinality of a basis of a vector space V is called, as usual, the *dimension* of V. According to Theorem II.2.4, this does not depend on the choice of the basis. We will show later that the above theorems also hold for "vector spaces" over skew fields (Theorem II.9.11).

Example II.2.6. For every field K, the polynomial ring $K[X]$ as a K-vector space has the countable basis $1, X, X^2, \ldots$. Therefore $\dim K[X] = \aleph_0$. On the other hand, $\dim_{\mathbb{Q}} \mathbb{R} > \aleph_0$.

Theorem II.2.7 (Krull)**.** *Let R be a ring and $I \lhd R$ a proper ideal. Then there exists a maximal ideal M of R with $I \subseteq M$. In particular, every ring $R \neq \{0\}$ possesses a maximal ideal.*

Proof. The set $\mathcal{M}$ of all ideals $J \lhd R$ with $I \subseteq J$ is not empty because of $I \in \mathcal{M}$ and is ordered by $\subseteq$. Let $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ be totally ordered. Then $0 \in I \subseteq \cup_{N \in \mathcal{N}} N =: J$. For $x, y \in J$, there exist $X, Y \in \mathcal{N}$ with $x \in X$ and $y \in Y$. Since $\mathcal{N}$ is totally ordered, wlog. $X \subseteq Y$ holds. Certainly then $x - y, ax, xa \in Y \subseteq J$ for all $a \in R$. This shows $J \trianglelefteq R$. For all $N \in \mathcal{N}$, $1 \notin N$ holds, for otherwise $R = R1 \subseteq N$ would be true. Thus $1 \notin J$ and $J \in \mathcal{M}$ is an upper bound of $\mathcal{N}$. By Zorn, $\mathcal{M}$ has a maximal element M. Then $I \subseteq M \lhd R$ holds. If $M \subsetneq L \trianglelefteq R$, then $L \notin \mathcal{M}$ and one obtains $L = R$. Therefore M is a maximal ideal. The second statement follows by choosing $I = \{0\}$. □

Remark II.2.8. In Definition I.14.14 we defined the polynomial ring $K[X_1, \ldots, X_n]$ over a field K in finitely many unknowns $X_1, \ldots, X_n$. If I is an arbitrary index set, we define

$$K[X_i : i \in I] := \bigcup_{\substack{J \subseteq I \\ |J| < \infty}} K[X_j : j \in J].$$

Every element of $K[X_i : i \in I]$ is a polynomial in finitely many unknowns. Therefore, $K[X_i : i \in I]$ is (still) a ring. In the following, we prove the existence and uniqueness of the algebraic closure of an arbitrary field (cf. Theorem I.13.14).

Theorem II.2.9. *Every field K possesses an algebraic closure.*

Proof. Let $R := K[X_\alpha : \alpha \in K[X] \setminus K]$ and

$$I := (\alpha(X_\alpha) : \alpha \in K[X] \setminus K) \trianglelefteq R.$$

Assume $I = R$. Then there exist $\alpha_1, \ldots, \alpha_n \in K[X] \setminus K$ and $\beta_1, \ldots, \beta_n \in R$ with

$$1 = \beta_1 \alpha_1(X_{\alpha_1}) + \ldots + \beta_n \alpha_n(X_{\alpha_n}) \in I. \tag{II.2.1}$$

According to Kronecker, there exists a splitting field L of $\alpha_1 \ldots \alpha_n$. Let $x_1, \ldots, x_n \in L$ with $\alpha_i(x_i) = 0$ for $i = 1, \ldots, n$. Replacing each X_{α_i} in (II.2.1) by x_i, one obtains the contradiction $1 = 0$ in L. Therefore $I \neq R$. According to Krull, there exists a maximal ideal $M \lhd R$ with $I \subseteq M$. According to Theorem I.7.12, $K_1 := R/M$ is a field and the canonical map $\Gamma\colon K \to K_1$, $a \mapsto a + M$ is a field homomorphism. Since Γ is injective according to Lemma I.8.41, we can replace K by $\Gamma(K)$ and thus assume $K \subseteq K_1$. For $\alpha \in K[X] \setminus K$ let $x_\alpha := X_\alpha + M \in K_1$. Because of

$$\alpha(x_\alpha) = \alpha(X_\alpha + M) = \alpha(X_\alpha) + M \in (I + M)/M = 0$$

every α has a root in K_1. Furthermore, the x_α are algebraic over K. Since every element in K_1 has the form

$$\sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_{\alpha_1}^{i_1} \ldots X_{\alpha_n}^{i_n} + M = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} x_{\alpha_1}^{i_1} \ldots x_{\alpha_n}^{i_n} \qquad (\alpha_1, \ldots, \alpha_n \in K[X] \setminus K)$$

the extension $K \subseteq K_1$ is algebraic according to Theorem I.13.4. The same argument with K_1 instead of K yields an algebraic extension $K_1 \subseteq K_2$ such that every polynomial in $K_1[X] \setminus K_1$ has a root in K_2. In this way, one obtains fields $K \subseteq K_1 \subseteq K_2 \subseteq \ldots$ and defines

$$\overline{K} := \bigcup_{n=1}^{\infty} K_n$$

(cf. Theorem I.13.14). Obviously, $\overline{K}$ is a field and $K \subseteq \overline{K}$ is algebraic according to Lemma I.13.2. Every polynomial in $\overline{K}[X] \setminus \overline{K}$ has coefficients in some K_n and therefore has a root in $K_{n+1} \subseteq \overline{K}$. Thus $\overline{K}$ is algebraically closed.[2] □

Theorem II.2.10. *Let $K \subseteq L$ be an algebraic field extension and S an algebraically closed field. Then every homomorphism $K \to S$ can be extended to a homomorphism $L \to S$.*

Proof. Let $\sigma\colon K \to S$ be a homomorphism. Let $\mathcal{M}$ be the set of all pairs (M, τ), where M is a field with $K \subseteq M \subseteq L$ and $\tau\colon M \to S$ is a homomorphism with restriction $\tau_K = \sigma$. Because of $(K, \sigma) \in \mathcal{M}$, $\mathcal{M} \neq \varnothing$. By

$$(M, \tau) \leq (M', \tau') \ :\Longleftrightarrow\ M \subseteq M',\ \tau'_M = \tau$$

$\mathcal{M}$ is ordered. Let $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ be totally ordered. As usual, $N := \bigcup_{(M,\tau)\in\mathcal{N}} M$ is then a field with $K \subseteq N \subseteq L$. For each $x \in N$ there exists an $(M, \tau) \in \mathcal{N}$ with $x \in M$. We define $\gamma(x) := \tau(x)$. If also $(M', \tau') \in \mathcal{N}$ with $x \in M'$, then wlog. $(M, \tau) \leq (M', \tau')$ and $\tau'(x) = \tau'_M(x) = \tau(x)$ holds. Therefore $\gamma\colon N \to S$ does not depend on the choice of (M, τ). For $x, y \in N$ there analogously exists $(M, \tau) \in \mathcal{N}$ with $x, y \in M$. It then holds that

$$\gamma(x \mathbin{\dot{+}} y) = \tau(x \mathbin{\dot{+}} y) = \tau(x) \mathbin{\dot{+}} \tau(y) = \gamma(x) \mathbin{\dot{+}} \gamma(y).$$

Thus γ is a homomorphism with $\gamma_K = \sigma$. Consequently (N, τ) is an upper bound of $\mathcal{N}$. By Zorn there exists a maximal element $(K', \sigma') \in \mathcal{M}$.

Assumption: $K' \neq L$.
Let $x \in L \setminus K'$ with minimal polynomial $\mu \in K'[X]$ (note: $K \subseteq L$ is algebraic). Since S is algebraically closed, $\sigma'(\mu) \in S[X]$ has a root in S. According to the extension theorem, one can extend σ' to $\tau\colon K'(x) \to S$. But then $(K'(x), \tau) \in \mathcal{M}$ would be in contradiction to the choice of (K', σ'). Thus $K' = L$ and $\sigma'\colon L \to S$ is an extension of σ. □

Corollary II.2.11. *Any two algebraic closures of a field K are K-isomorphic.*

Proof. Let S_1, S_2 be algebraic closures of K. According to Theorem II.2.10, the inclusion map $K \hookrightarrow S_2$ can be extended to a monomorphism $\sigma\colon S_1 \to S_2$ (Lemma I.8.41). Every $x \in S_2$ is a root of its minimal polynomial $\mu \in K[X]$. Now μ splits in the algebraically closed field S_1 and σ maps these roots to the roots of $\sigma(\mu) = \mu$. Therefore $x \in \sigma(S_1)$ and σ is a K-isomorphism. □

[2] According to Theorem II.3.16, K_1 is already algebraically closed.

II.3 Separable Extensions

Remark II.3.1. We have seen in Theorems I.12.2 and I.12.3 that splitting fields in characteristic 0 are always Galois extensions and possess primitive elements. According to Artin, this is more generally true for perfect fields (cf. Exercise I.57). We show in this chapter that an arbitrary field extension $K \subseteq L$ always possesses an intermediate field that behaves like an extension over a perfect field.

Definition II.3.2. Let $K \subseteq L$ be a field extension.

- An irreducible polynomial $\alpha \in K[X]$ is called *separable*, if $\alpha' \neq 0$.
- An algebraic element $a \in L$ is called *separable* over K, if its minimal polynomial is separable. Otherwise a is called *inseparable* over K.
- The extension $K \subseteq L$ is called *separable*, if every $a \in L$ is separable over K. Otherwise $K \subseteq L$ is called *inseparable*. If all $a \in L \setminus K$ are inseparable over K, then the extension is called *purely inseparable*.

Example II.3.3.

(i) Every $a \in K$ is separable over K, because the minimal polynomial $X - a$ has derivative 1. Note: The trivial extension $K \subseteq K$ is both separable and purely inseparable.

(ii) Every separable (or purely inseparable) extension is algebraic. Therefore $\mathbb{Q} \subseteq \mathbb{C}$ is inseparable.

(iii) If $K \subseteq L$ is separable (or purely inseparable), then so is $K \subseteq M$ for all subfields $M \subseteq L$ containing K.

(iv) According to Theorem I.11.20, every algebraic extension of a perfect field is separable. As shown there, an irreducible $\alpha \in K[X]$ is in general separable if and only if α has no multiple roots in a splitting field. We use this in the following.

(v) According to Exercise I.63, $\alpha := Y^2 - X \in \mathbb{F}_2(X)[Y]$ is irreducible, but not separable, because $\alpha' = 2Y = 0$.

Theorem II.3.4. *Let $K \subseteq L$ be a finite, separable field extension. Then:*

(i) There exists a Galois extension $K \subseteq M$ with $L \subseteq M$.

(ii) There exists an $x \in L$ with $L = K(x)$ (Primitive Element Theorem).

Proof.

(i) Let $x_1, \ldots, x_n$ be a K-basis of L. Let $\mu_1, \ldots, \mu_n \in K[X]$ be the (separable) minimal polynomials of $x_1, \ldots, x_n$ over K. Wlog. let $\mu_1, \ldots, \mu_k$ be pairwise distinct and $\{\mu_1, \ldots, \mu_k\} = \{\mu_1, \ldots, \mu_n\}$. Because $\gcd(\mu_i, \mu_j) = 1$ for $1 \leq i < j \leq k$, $\alpha = \mu_1 \ldots \mu_k \in K[X]$ has pairwise distinct roots in a splitting field M. According to Artin, $K \subseteq M$ is a Galois extension with $L = K(x_1, \ldots, x_n) \subseteq M$.

(ii) Let M be as in (i). According to the Fundamental Theorem of Galois Theory, there exist only finitely many fields $L_1, \ldots, L_m$ with $K \subseteq L_i \subsetneq L$ for $i = 1, \ldots, m$. According to Lemma I.10.1, there exists an $x \in L \setminus \bigcup_{i=1}^{m} L_i$. Then certainly $K(x) = L$. □

Lemma II.3.5. *Let $K \subseteq L$ be a field extension with $p := \operatorname{char} K > 0$ and $a \in L$ algebraic over K. Then $a \in L$ is separable over K if and only if $K(a) = K(a^p)$ holds.*

Proof. In any case, $K(a^p) \subseteq K(a)$. Let a be separable with minimal polynomial $\mu \in K[X]$. The minimal polynomial $\nu \in K(a^p)[X]$ of a over $K(a^p)$ is a divisor of μ and therefore itself separable. On the other hand, ν also divides $(X-a)^p \overset{\text{I.11.10}}{=} X^p - a^p \in K(a^p)[X]$. This shows $\nu = X - a$ and $a \in K(a^p)$. Thus $K(a) = K(a^p)$.

Now let a be inseparable over K. Then $\mu' = 0$ and therefore

$$\mu = \sum_{k=0}^{n} a_k X^{pk} = \gamma(X^p) \qquad (a_i \in K)$$

for some $\gamma \in K[X]$. The minimal polynomial of a^p over K divides γ and it follows that

$$|K(a^p) : K| \leq \deg \gamma < \deg \mu = |K(a) : K|.$$

Thus $K(a^p) \neq K(a)$. □

Theorem II.3.6. *Galois extensions are separable.*

Proof. Let $K \subseteq L$ be a Galois extension and $a \in L$. Wlog. let $p := \operatorname{char} K > 0$. According to the Fundamental Theorem of Galois Theory, $K(a^p) \subseteq L$ is also a Galois extension. For $\sigma \in G := \operatorname{Gal}(L|K(a^p))$ we have

$$(\sigma(a) - a)^p \overset{\text{I.11.10}}{=} \sigma(a)^p - a^p = \sigma(a^p) - a^p = a^p - a^p = 0$$

and $\sigma(a) = a$. This shows $K(a) \subseteq L^G = K(a^p) \subseteq K(a)$ according to Artin. By Lemma II.3.5, a is separable over K. □

Lemma II.3.7. *If $K \subseteq L$ and $L \subseteq M$ are separable field extensions, then so is $K \subseteq M$.*

Proof. According to Lemma I.13.2, $K \subseteq M$ is algebraic. Let $x \in M$ and $\sum_{k=0}^{n} a_k X^k \in L[X]$ be the (separable) minimal polynomial of x over L. Then x is also separable over $K(a_0, \ldots, a_n) \subseteq L$. By the Primitive Element Theorem, there exists $c \in L$ with $K(a_0, \ldots, a_n) = K(c)$. By Lemma II.3.5 we have

$$K(c, x) = K(c)(x) = K(c^p)(x^p) = K(c^p, x^p).$$

Therefore, every element of $K(c, x)$ is a K-linear combination of p-th powers. As usual, $K(x)$ has a K-basis of the form $1, x, \ldots, x^k$. We extend this to a K-basis $x_1, \ldots, x_l$ of $K(c, x)$. For an arbitrary $b = \sum_{i=1}^{l} b_i x_i \in K(c, x)$ with $b_1, \ldots, b_l \in K$, it then holds that $b^p = \sum_{i=1}^{l} b_i^p x_i^p$. Since every element of $K(c, x)$ is a linear combination of p-th powers, $x_1^p, \ldots, x_l^p$ also form a K-basis of $K(c, x)$. In particular, $1, x^p, \ldots, x^{pk}$ are linearly independent over K. This shows

$$|K(x^p) : K| \geq k + 1 = |K(x) : K| \geq |K(x^p) : K|$$

and $K(x^p) = K(x)$. By Lemma II.3.5, x is separable over K. □

Theorem II.3.8. *The separable elements of an algebraic field extension $K \subseteq L$ form a subfield M of L with $K \subseteq M$. In this case, $M \subseteq L$ is purely inseparable.*

Proof. Certainly $K \subseteq M$. Let $a, b \in M$ with (separable) minimal polynomials $\mu_a, \mu_b \in K[X]$. Then

$$\mu := \frac{\mu_a \mu_b}{\gcd(\mu_a, \mu_b)} \in K[X]$$

has pairwise distinct roots in a splitting field Z. According to Artin, Z is a Galois extension with $K(a, b) \subseteq Z$. According to Theorem II.3.6, $K \subseteq Z$ is separable. Therefore, $a \dot{+} b$ and a/b (if $b \neq 0$) are also separable over K as elements of $K(a, b)$. This shows that M is a subfield of L.

Now assume that an $x \in L \setminus M$ is separable over M. As above, $M \subseteq M(x)$ is then separable and according to Lemma II.3.7, $K \subseteq M(x)$ is also separable. This yields the contradiction $x \in M$. Therefore, $M \subseteq L$ is purely inseparable. □

Definition II.3.9. In the situation of Theorem II.3.8, M is called the *separable closure* of K in L.[1] Furthermore, $|L : K|_s := |M : K|$ is called the *separability degree* of L over K.

Theorem II.3.10. *Let L be a field and G a finite subgroup of $\mathrm{Aut}(L)$. Then $L^G \subseteq L$ is a Galois extension with Galois group G.*

Proof. Let $K := L^G$ and $x \in L$. Let $\{x_1, \ldots, x_n\}$ be the orbit of x under G. Then x is a root of $\alpha := \prod_{i=1}^{n}(X - x_i) \in K[X]$. In particular, $|K(x) : K| \leq n \leq |G|$. The minimal polynomial of x, as a divisor of α, is separable over K. We choose x such that $|K(x) : K|$ is as large as possible. Suppose there exists $y \in L \setminus K(x)$. According to Theorem II.3.8, $K \subseteq K(x, y)$ is finite and separable. According to the primitive element theorem, there exists $z \in L$ with $K(x, y) = K(z)$ and $|K(z) : K| > |K(x) : K|$. This contradicts the choice of x. Thus $L = K(x)$ and $|L : K| \leq |G|$. According to Theorem I.10.6, conversely $|G| \leq |\mathrm{Aut}(L|K)| \leq |L : K|$. Thus $K \subseteq L$ is a Galois extension with $\mathrm{Gal}(L|K) = G$. □

Theorem II.3.11. *Let $p := \mathrm{char}\, K > 0$ and $\overline{K}$ be an algebraic closure of K. Then*

$$\overline{K}_p := \{x \in \overline{K} : \exists n \in \mathbb{N} : x^{p^n} \in K\}$$

is a perfect field and $\overline{K}_p \subseteq \overline{K}$ is separable. Furthermore, $K \subseteq \overline{K}_p$ is purely inseparable and every purely inseparable extension L of K is K-isomorphic to a subfield of $\overline{K}_p$.

Proof. Let $x, y \in \overline{K}_p$ with $x^{p^n}, y^{p^m} \in K$. Wlog. let $n \geq m$. Then $(x \dot{+} y)^{p^n} = x^{p^n} \dot{+} y^{p^n} \in K$ and likewise $(xy^{-1})^{p^n} \in K$ if $y \neq 0$. This shows that $\overline{K}_p$ is a subfield of $\overline{K}$, which obviously contains K. Since $\overline{K}$ is algebraically closed, $X^p - x$ has a root $z \in \overline{K}$. Because of $z^{p^{n+1}} = x^{p^n} \in K$, we have $z \in \overline{K}_p$. Thus z is a preimage of x under the Frobenius homomorphism. Consequently, $\overline{K}_p$ is perfect and $\overline{K}_p \subseteq \overline{K}$ is separable. Now let $x \notin K$. Then the minimal polynomial of x over K, as a divisor of $X^{p^n} - x^{p^n} = (X - x)^{p^n}$, has only one root up to multiplicity. Therefore x is inseparable over K. Overall, $K \subseteq \overline{K}_p$ is purely inseparable.

Finally, let $K \subseteq L$ also be purely inseparable (and thus algebraic). According to Theorem II.2.10, the inclusion map $K \hookrightarrow \overline{K}$ can be extended to a field homomorphism $\Gamma\colon L \to \overline{K}$. We can therefore replace L by $\Gamma(L)$. It then suffices to show $L \subseteq \overline{K}_p$. For $x \in L \setminus K$, we have $|K(x^p) : K| < |K(x) : K|$ according to Lemma II.3.5. By induction on $|K(x) : K|$, we can assume $x^p \in \overline{K}_p$. Then there exists an $n \in \mathbb{N}$ with $x^{p^{n+1}} = (x^p)^{p^n} \in K$, i. e. $x \in \overline{K}_p$. □

[1] If L is "the" algebraic closure of K, then M is called "the" separable closure of K.

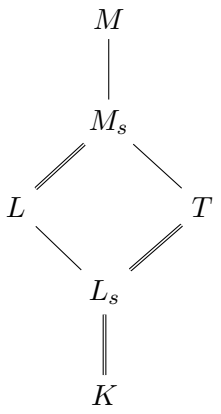
Corollary II.3.12. *The degree of a finite purely inseparable field extension $K \subsetneq L$ is a power of $p := \operatorname{char} K$.*

Proof. Obviously $p > 0$. According to Theorem II.3.11, we can assume $L \subseteq \overline{K}_p$. For every $a \in L$, there then exists an $n \in \mathbb{N}$ with $a^{p^n} \in K$. The minimal polynomial $\mu \in K[X]$ of a therefore divides $X^{p^n} - a^{p^n} = (X-a)^{p^n}$ and thus has only one root up to multiplicity. For every intermediate field $K \subseteq M \subseteq L$, the minimal polynomial of a over M is a divisor of μ and therefore also has only one root up to multiplicity. In particular, a is also inseparable over M if $a \notin M$. Therefore the extensions $K \subseteq M$ and $M \subseteq L$ are purely inseparable. By induction on $|L:K|$, we can assume using the degree theorem that no proper intermediate fields M exist. For $a \in L \setminus K$, we then have $L = K(a)$. According to Lemma II.3.5, $K(a^p) \subsetneq K(a)$, so $a^p \in K$. The minimal polynomial μ of a over K therefore divides $X^p - a^p$. On the other hand, because $\mu' = 0$, we have $\deg \mu \geq p$. This shows $|L:K| = |K(a):K| = \deg \mu = p$. □

Theorem II.3.13 (Degree theorem for $|L:K|_s$)**.** *Let $K \subseteq L \subseteq M$ be finite field extensions. Then*

$$\boxed{|M:K|_s = |M:L|_s |L:K|_s.}$$

Proof. We can assume $p := \operatorname{char} K > 0$, because otherwise the claim follows from the degree theorem. Let L_s and M_s be the separable closures of K in L and of L in M, respectively. Let T be the separable closure of L_s in M_s. According to Lemma II.3.7, $K \subseteq T$ is also separable.
Let $x \in M$ be separable over K. Then x is also separable over L and thus contained in M_s. Furthermore, x is also separable over L_s and therefore contained in T. This shows that T is the separable closure of K in M. It follows



$$|M:K|_s = |T:K| = |T:L_s||L_s:K| = |T:L_s||L:K|_s.$$

We must therefore show $|T:L_s| = |M:L|_s = |M_s:L|$. By the primitive element theorem, there exists an $x \in T$ with $T = L_s(x)$. The minimal polynomial $\mu \in L_s[X]$ is separable. Let $\nu \in L[X]$ be an irreducible divisor of μ. According to Vieta, the coefficients of ν can be expressed by the roots (in a splitting field). Since these roots are separable over L_s, the coefficients of ν are also separable over L_s. On the other hand, the coefficients of ν lie in L and $L_s \subseteq L$ is purely inseparable according to Theorem II.3.8. This shows $\nu \in L_s[X]$ and it follows $\nu = \mu$. Thus

$$|T:L_s| = |L_s(x):L_s| = \deg \mu = \deg \nu = |L(x):L| \leq |M_s:L|.$$

Now let x be a primitive element of the separable extension $L \subseteq M_s$, so $M_s = L(x)$. Since $T \subseteq M_s$ is purely inseparable, there exists by Theorem II.3.11 an $n \in \mathbb{N}$ with $y := x^{p^n} \in T$. According to Lemma II.3.5, $L(x) = L(x^p) = \ldots = L(y)$. By the same argument as above, the minimal polynomial of y over L_s is also irreducible in $L[X]$. This shows

$$|M_s:L| = |L(x):L| = |L(y):L| = |L_s(y):L_s| \leq |T:L_s|.$$ □

Remark II.3.14.

(i) Let I be an arbitrary index set. The field of fractions of $K[X_i : i \in I]$ is the field of rational functions $K(X_i : i \in I)$ consisting of the elements α/β with $\alpha, \beta \in K[X_i : i \in I]$ and $\beta \neq 0$ (Exercise I.40).

(ii) Let $K \subseteq L$ be a field extension and $S \subseteq L$ a subset. Then $K(S)$ contains the elements $\alpha(S)/\beta(S)$ with $\alpha, \beta \in K[X_s : s \in S]$ and $\beta(S) \neq 0$. On the other hand, these elements themselves form a subfield of L, which then must coincide with $K(S)$.

Example II.3.15. We consider the extension

$$K := \mathbb{F}_2(X^2, Y^2) \subseteq \mathbb{F}_2(X, Y) =: L.$$

Assume $X \in K$. Then there exist $\alpha, \beta \in \mathbb{F}_2[X, Y]$ with $X = \frac{\alpha(X^2,Y^2)}{\beta(X^2,Y^2)}$. It follows that $X\beta(X^2, Y^2) = \alpha(X^2, Y^2)$. On the left side, X occurs only with odd powers, but on the right side only with even powers. This contradiction shows $X \notin K$. Analogously, one shows $Y \notin K(X) = \mathbb{F}_2(X, Y^2)$. Therefore,

$$|L : K| = |L : K(X)||K(X) : K| = 4.$$

For every $\alpha = \sum_{i,j\geq 0} a_{ij}X^iY^j \in \mathbb{F}_2[X, Y]$, we have $\alpha^2 = \sum a_{ij}^2 X^{2i}Y^{2j} \in K$. Therefore, $a^2 \in K$ for all $a \in L$ as well. In the case $a \notin K$, $Z^2 - a^2 = (Z - a)^2 \in K[Z]$ is the minimal polynomial of a. Thus $K \subseteq L$ is purely inseparable. Furthermore, L possesses no primitive element. For $a \in K$, we consider the subfield $M_a := K(X + aY)$. Certainly $|M_a : K| \leq 2$. Let $b \in K$ with $M_a = M_b$. In the case $a \neq b$, we would have

$$Y = \frac{1}{a - b}\big(X + aY - X - bY\big) \in M_a$$

and $X = X + aY - aY \in M_a$. This yields the contradiction $M_a = L$. Thus $M_a \neq M_b$ for $a \neq b$. In particular, $K \subseteq L$ possesses infinitely many intermediate fields (cf. Exercise II.19).

Theorem II.3.16. *Let $K \subseteq L$ be an algebraic field extension such that every polynomial in $K[X]$ has a root in L. Then L is an algebraic closure of K.*

Proof. Every polynomial in $L[X]$ has a root x in a splitting field. Now x is algebraic over L and also over K. Thus x is a root of a polynomial in $K[X]$. It therefore suffices to show that every $\alpha \in K[X]$ splits into linear factors over L. Wlog. let α be irreducible.

First, let $K \subseteq L$ (and thus α) be separable. According to Artin, the splitting field M of α is a Galois extension and thus has the form $M = K(y)$ for some $y \in M$. The minimal polynomial $\beta \in K[X]$ of y has, by assumption, a root $z \in L$. Now one has a K-isomorphism

$$M = K(y) = K[X]/(\beta) \cong K(z).$$

Thus α also splits in $K(z) \subseteq L$ as desired.

Now let $K \subseteq L$ be inseparable and $p := \operatorname{char} K$. As in Theorem II.3.11, we construct the field

$$L_p := \{a \in L : \exists n \in \mathbb{N} : a^{p^n} \in K\}.$$

Let $a \in L_p$ with $a^{p^n} \in K$. By assumption, $X^{p^{n+1}} - a^{p^n} \in K[X]$ has a root $b \in L$. Because of $(b^p - a)^{p^n} = 0$, $b \in L_p$ is a preimage of a under the Frobenius homomorphism. Thus L_p is perfect and $L_p \subseteq L$ is separable. According to the first part of the proof, it suffices to show that every polynomial $\gamma = \sum_{k=0}^{n} c_k X^k \in L_p[X]$ has a root in L. There exists $m \in \mathbb{N}$ with

$$\gamma^m = \sum_{k=0}^{n} c_i^m X^{km} \in K[X].$$

By assumption, γ^m has a root in L, and thus so does γ. □

Definition II.3.17. Let $K \subseteq L$ be a finite field extension. For $x \in L$, $t_x \colon L \to L$, $a \mapsto xa$ is K-linear (Remark I.9.3). We call $S_K^L \colon L \to K$, $x \mapsto \operatorname{tr}(t_x)$ the *trace map* of L with respect to K. Obviously, S_K^L is a K-linear map.

Lemma II.3.18. *Let $K \subseteq L \subseteq M$ be finite field extensions and $x \in M$ with minimal polynomial $\mu = X^d + a_{d-1}X^{d-1} + \ldots + a_0 \in K[X]$. Then*

(i) $S_K^L \circ S_L^M = S_K^M$.

(ii) $S_K^M(x) = |M : K(x)| S_K^{K(x)}(x) = -|M : K(x)| a_{d-1}$.

Proof.

(i) Let $b_1, \ldots, b_n \in L$ be a K-basis of L and $c_1, \ldots, c_m \in M$ an L-basis of M. According to the proof of the degree theorem, $\{b_i c_j : i = 1, \ldots, n,\ j = 1, \ldots, m\}$ is a K-basis of M. Let $t_x(c_j) = \sum_{t=1}^m \gamma_{tj} c_t$ with $\gamma_{tj} \in L$ and $t_{\gamma_{tj}}(b_i) = \gamma_{tj} b_i = \sum_{s=1}^n \beta_{tjsi} b_s$ with $\beta_{tjsi} \in K$. Then

$$t_x(b_i c_j) = x b_i c_j = b_i t_x(c_j) = \sum_{t=1}^m \gamma_{tj} b_i c_t = \sum_{s=1}^n \sum_{t=1}^m \beta_{tjsi} b_s c_t$$

and it follows that

$$S_K^M(x) = \sum_{i=1}^n \sum_{j=1}^m \beta_{jjii} = \sum_{j=1}^m S_K^L(\gamma_{jj}) = S_K^L(S_L^M(x)).$$

(ii) Let $L := K(x)$. As an L-linear map, $t_x = x \operatorname{id}$ and $S_L^M(x) = |M : L| x$. Therefore, the first equation follows from (i). The matrix of t_x with respect to the K-basis $1, x, \ldots, x^{d-1}$ of L has the form

$$A := \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{d-2} \\ 0 & & 1 & -a_{d-1} \end{pmatrix}$$

(cf. Definition II.10.2). Thus $S_K^L(x) = \operatorname{tr}(A) = -a_{d-1}$. □

Lemma II.3.19. *Let $K \subseteq L$ be a finite separable field extension. Let $\sigma_1, \ldots, \sigma_n$ be all K-homomorphisms from L to $\overline{K}$. Then $S_K^L(x) = \sum_{i=1}^n \sigma_i(x)$ for $x \in L$.*

Proof. According to Exercise II.18, $n = |L : K|$. Let $d := |K(x) : K|$. Since $K \subseteq K(x)$ is also separable, there exist exactly d K-homomorphisms $\tau_1, \ldots, \tau_d \colon K(x) \to \overline{K}$. Furthermore, there exists a primitive element $y \in L$ with $L = K(y)$. Since the roots of the separable minimal polynomial of y over $K(x)$ are pairwise distinct, each τ_i has n/d extensions $\tau_{i,1}, \ldots, \tau_{i,n/d} \colon L \to \overline{K}$ according to the extension theorem. It holds that

$$\{\sigma_1, \ldots, \sigma_n\} = \{\tau_{i,j} : i = 1, \ldots, d,\ j = 1, \ldots, n/d\}$$

and

$$\sum_{i=1}^n \sigma_i(x) = \frac{n}{d} \sum_{i=1}^d \tau_i(x) = |L : K(x)| \sum_{i=1}^d \tau_i(x).$$

According to Lemma II.3.18, we can assume $L = K(x)$. Each σ_i is then uniquely determined by $\sigma_i(x)$. Let $\mu \in K[X]$ be the minimal polynomial of x. Because of $\sigma_i(\mu) = \mu$, $\sigma_i(x)$ must be a root of μ. From $\deg \mu = n$ it follows that $\mu = \prod_{i=1}^n (X - \sigma_i(x))$. The claim follows from Lemma II.3.18. □

Example II.3.20. For every Galois extension $K \subseteq L$, $S_K^L = \sum_{\sigma \in \mathrm{Gal}(L|K)} \sigma$ holds (cf. Remark I.10.13).

Theorem II.3.21. *A finite field extension $K \subseteq L$ is separable if and only if $S_K^L \neq 0$.*

Proof. Let $K \subseteq L$ be separable. According to Dedekind's Lemma I.14.1, the K-homomorphisms $\sigma_1, \ldots, \sigma_n \colon L \to \overline{K}$ are linearly independent. From Lemma II.3.19 it follows that $S_K^L = \sum_{i=1}^n \sigma_i \neq 0$. Now let $K \subseteq L$ be inseparable and $p := \mathrm{char}\, K > 0$. Let M be the separable closure of K in L. Because of $S_K^L = S_K^M \circ S_M^L$, we can assume $K = M$, i.e., $K \subseteq L$ is purely inseparable. For every $x \in L$, there exists by Theorem II.3.11 an $n \in \mathbb{N}$ with $x^{p^n} \in K$. Therefore, the minimal polynomial μ of x is a divisor of $(X-1)^{p^n}$. According to Corollary II.3.12, $\deg \mu$ is also a power of p. Thus $\mu = (X-1)^{p^k} = X^{p^k} - 1$ for some $k \leq n$. From Lemma II.3.18 it follows that $S_K^L(x) = 0$. □

II.4 Transcendental Extensions

Remark II.4.1. According to Theorem I.13.4, every field extension $K \subseteq L$ has an intermediate field $K \subseteq M \subseteq L$ such that $K \subseteq M$ is algebraic and every $x \in L \setminus M$ is transcendental over M. In this section, we use Zorn's Lemma to construct an intermediate field $K \subseteq M' \subseteq L$ with the opposite property: $M' \subseteq L$ is algebraic and every $x \in M' \setminus K$ is transcendental over K.

Definition II.4.2. Let $K \subseteq L$ be a field extension.

- A subset $S \subseteq L$ is called *algebraically independent* over K if every $s \in S$ is transcendental over $K(S \setminus \{s\})$. Otherwise, S is called *algebraically dependent* over K.
- If L contains an element that is transcendental over K, then the extension $K \subseteq L$ is called *transcendental*. If even every $x \in L \setminus K$ is transcendental over K, then $K \subseteq L$ is called *absolutely transcendental*. If there exists an algebraically independent subset $S \subseteq L$ with $L = K(S)$, then $K \subseteq L$ is called *purely transcendental*.
- An algebraically independent subset $S \subseteq L$ is called a *transcendence basis* of L over K if the extension $K(S) \subseteq L$ is algebraic.

Example II.4.3.

(i) $\{a\}$ is algebraically independent over K if and only if a is transcendental over K. According to Lindemann, $\{\pi\}$ is algebraically independent over $\mathbb{Q}$. On the other hand, it is open whether $\{\pi, e\}$ is algebraically independent over $\mathbb{Q}$.

(ii) If S is algebraically independent over K, then so is every subset of S.

(iii) The extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \pi)$ is transcendental, but not absolutely transcendental.

(iv) The field of rational functions $K(X)$ is purely transcendental over K with transcendence basis $\{X\}$ (cf. Remark I.9.3(iv)). However, $\{X^2\}$ is also a transcendence basis with $|K(X) : K(X^2)| = 2$.

(v) Every algebraic field extension has only the transcendence basis $\varnothing$. In particular, the trivial extension $K \subseteq K$ is purely transcendental.

Theorem II.4.4 (Lindemann-Weierstrass)**.** *$a_1, \ldots, a_n \in \overline{\mathbb{Q}}$ are linearly dependent over $\mathbb{Q}$ if and only if $e^{a_1}, \ldots, e^{a_n}$ are algebraically dependent over $\mathbb{Q}$.*

Proof. See Corollary A.10.7. □

Remark II.4.5. Theorem II.4.4 says (simplified) that the group homomorphism $\exp\colon (\mathbb{C}, +) \to \mathbb{C}^\times$ maps linearly dependent elements to algebraically dependent elements. From this, one obtains the transcendence of e (with $a_1 = 1$) and π (if π were algebraic, then so would be $\pi\mathrm{i}$ and $e^{\pi\mathrm{i}} = -1$ would be transcendental).

Lemma II.4.6. *Let $K \subseteq L$ be a field extension and $S \subseteq L$ a subset. S is algebraically independent over K if and only if the evaluation homomorphism*

$$\begin{aligned} K[X_s : s \in S] &\to K(S), \\ \alpha &\mapsto \alpha(S) \end{aligned}$$

is injective.

Proof. First, let S be algebraically independent and $\alpha \in K[X_s : s \in S]$ with $\alpha(S) = 0$. Then only finitely many $s_1, \ldots, s_n \in S$ occur in $\alpha(S)$. The equation $\alpha(S) = 0$ means that s_1 is algebraic over $K(s_2, \ldots, s_n) \subseteq K(S \setminus \{s_1\})$. Therefore, $\alpha = 0$ must hold and the evaluation homomorphism is injective.

Conversely, let S be algebraically dependent. Then some $s \in S$ is algebraic over $K(S \setminus \{s\})$. So let $\alpha \in K(S \setminus \{s\})[X] \setminus \{0\}$ with $\alpha(s) = 0$. By multiplying α by a common denominator of its coefficients, one can assume that these coefficients have the form $\alpha_i(s_1, \ldots, s_n)$ with $s_1, \ldots, s_n \in S \setminus \{s\}$ and $\alpha_i \in K[X_1, \ldots, X_n]$. Thus there exists a polynomial $\beta \in K[X_1, \ldots, X_{n+1}] \setminus \{0\}$ with $\beta(s_1, \ldots, s_n, s) = 0$, i. e. the evaluation homomorphism is not injective. □

Remark II.4.7. From Lemma II.4.6 it follows that $S \subseteq L$ is algebraically independent if and only if every *finite* subset of S is algebraically independent. If this is the case, then the evaluation homomorphism $K[X_s : s \in S] \to K(S)$ extends to an isomorphism $K(X_s : s \in S) \cong K(S)$ (universal property of the field of fractions, Exercise I.40). This corresponds to the statement that every n-dimensional vector space over K is isomorphic to K^n (linear algebra).

Example II.4.8. According to the fundamental theorem I.14.19 on symmetric polynomials and Lemma II.4.6, the elementary symmetric polynomials $\sigma_1, \ldots, \sigma_n$ as a subset of $K(X_1, \ldots, X_n)$ are algebraically independent over K. According to Vieta, each X_i is algebraic over $K(\sigma_1, \ldots, \sigma_n)$. Therefore, $\sigma_1, \ldots, \sigma_n$ is a transcendence basis of $K(X_1, \ldots, X_n)$. We give a new (non-constructive) proof in Theorem II.4.20. For arbitrary polynomials in $K(X_1, \ldots, X_n)$, one can check whether a transcendence basis is present using the Jacobian matrix of partial derivatives (see Theorem A.5.9).

Lemma II.4.9. *Every purely transcendental field extension is absolutely transcendental.*

Proof. Let $K \subseteq L$ be a purely transcendental field extension and $S \subseteq L$ algebraically independent with $L = K(S)$. For $a \in L \setminus K$ there exist $s_1, \ldots, s_n \in S$ with $a \in K(s_1, \ldots, s_n) = K(s_1, \ldots, s_{n-1})(s_n)$. Let n be chosen minimally. Then there exist coprime $\alpha, \beta \in K(s_1, \ldots, s_{n-1})[X]$ with $a = \alpha(s_n)/\beta(s_n)$. If a is algebraic over K, then there exist $\lambda_0, \ldots, \lambda_k \in K$ with $\lambda_k \neq 0$ and $\sum_{i=0}^{k} \lambda_i a^i = 0$, i. e.

$$\Big(\sum_{i=0}^{k} \lambda_i \alpha^i \beta^{k-i}\Big)(s_n) = \beta^k(s_n) \sum_{i=0}^{k} \lambda_i \Big(\frac{\alpha(s_n)}{\beta(s_n)}\Big)^i = 0.$$

Since s_n is transcendental over $K(s_1, \ldots, s_{n-1}) \subseteq K(S \setminus \{s_n\})$, it follows that $\sum \lambda_i \alpha^i \beta^{k-i} = 0$. It follows that

$$\beta \mid \lambda_{k-1} \alpha^{k-1} \beta + \ldots + \lambda_0 \beta^k = -\lambda_k \alpha^k.$$

Because of $\gcd(\alpha, \beta) = 1$ we obtain $\beta \in K(s_1, \ldots, s_{n-1})$. A comparison of degrees of $\sum \lambda_i \alpha^i \beta^{k-i} = 0$ also yields $\alpha \in K(s_1, \ldots, s_{n-1})$. This gives $a = \alpha(s_n)/\beta(s_n) = \alpha/\beta \in K(s_1, \ldots, s_{n-1})$ in contradiction to the choice of n. □

Remark II.4.10.

(i) We show in Example II.4.16 that the converse of Lemma II.4.9 is false.

(ii) The following theorems show that transcendence bases behave like bases of vector spaces.

Lemma II.4.11. *For a field extension $K \subseteq L$ and a subset $S \subseteq L$ the following are equivalent:*

(1) S is a transcendence basis of L over K.

(2) S is algebraically independent over K and for every $a \in L \setminus S$, $S \cup \{a\}$ is algebraically dependent over K.

(3) $K(S) \subseteq L$ is algebraic and for every $s \in S$, $K(S \setminus \{s\}) \subseteq L$ is transcendental.

Proof.

(1) $\Rightarrow$ (2): By definition, S is algebraically independent and $K(S) \subseteq L$ is algebraic. For $a \in L \setminus S$, a is algebraic over $K(S)$, i. e. $S \cup \{a\}$ is algebraically dependent.

(2) $\Rightarrow$ (3): Let $a \in L \setminus K(S) \subseteq L \setminus S$. Then $S \cup \{a\}$ is algebraically dependent. According to Lemma II.4.6, there exist $s_1, \ldots, s_n \in S \cup \{a\}$ and $\alpha \in K[X_1, \ldots, X_n] \setminus \{0\}$ with $\alpha(s_1, \ldots, s_n) = 0$. Since S is algebraically independent, a must appear in $\alpha(s_1, \ldots, s_n)$. Thus a is algebraic over $K(S)$ and $K(S) \subseteq L$ is algebraic. For $s \in S$, s is transcendental over $K(S \setminus \{s\})$, i. e. $K(S \setminus \{s\}) \subseteq L$ is transcendental.

(3) $\Rightarrow$ (1): We must show that S is algebraically independent. Suppose for this purpose that $s \in S$ is algebraic over $K(S \setminus \{s\})$. Then $K(S \setminus \{s\}) \subseteq K(S)$ is a finite field extension and thus algebraic. But then $K(S \setminus \{s\}) \subseteq L$ would also be algebraic according to Lemma I.13.2. □

Theorem II.4.12 (Basis Extension Theorem)**.** *Let $K \subseteq L$ be a field extension with an algebraically independent subset $U \subseteq L$ and $U \subseteq S \subseteq L$, such that $K(S) \subseteq L$ is algebraic. Then there exists a transcendence basis B of L over K with $U \subseteq B \subseteq S$. In particular, every field extension has a transcendence basis.*

Proof. The set

$$\mathcal{M} := \{U \subseteq M \subseteq S : M \text{ algebraically independent over } K\}$$

is non-empty and ordered by $\subseteq$. Let $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ be totally ordered and $N := \bigcup_{M \in \mathcal{N}} M \subseteq S$. Let $N_1 \subseteq N$ be a finite subset. Since $\mathcal{N}$ is totally ordered, there exists an $M \in \mathcal{N}$ with $N_1 \subseteq M$. Since M is algebraically independent over K, N_1 is as well. According to Remark II.4.7, N is also algebraically independent over K, i. e. $N \in \mathcal{M}$. Therefore N is an upper bound of $\mathcal{N}$. By Zorn's Lemma, there exists a maximal element $B \in \mathcal{M}$. For every $s \in S \setminus B$, $B \cup \{s\}$ is then algebraically dependent, i. e. s is algebraic over $K(B)$. If $x \in K(S)$ is arbitrary, then there exist $s_1, \ldots, s_n \in S$ with $x \in K(s_1, \ldots, s_n)$. Because $|K(B)(s_1, \ldots, s_n) : K(B)| < \infty$, x is also algebraic over $K(B)$. Thus $K(B) \subseteq K(S)$ is algebraic and therefore also $K(B) \subseteq L$. Thus B is a transcendence basis with the desired property. The second assertion follows by choosing $U = \varnothing$ and $S = L$. □

Theorem II.4.13 (Exchange Theorem)**.** *Let $K \subseteq L$ be a field extension and $U \subseteq L$ a finite algebraically independent subset. For every subset $S \subseteq L$ with $K(S) \subseteq L$ algebraic, it then holds that $|U| \leq |S|$.*

Proof. Let $U = \{u_1, \ldots, u_n\}$ and wlog. $S = \{s_1, \ldots, s_m\}$ (in the case $|S| = \infty$ we are finished). Then u_1 is algebraic over $K(S)$, i. e. there exists an $\alpha \in K(S)[X] \setminus \{0\}$ with root u_1. Multiplying α by a common denominator of its coefficients, one obtains $\beta \in K[X_1, \ldots, X_m, X]$ with $\beta(s_1, \ldots, s_m, u_1) = 0$. Since u_1 is transcendental over K, some s_i, say s_1, appears in $\beta(s_1, \ldots, s_m, u_1)$. In particular, s_1 is algebraic over $K(u_1, s_2, \ldots, s_m)$. Thus the extensions

$$K(u_1, s_2, \ldots, s_m) \subseteq K(\{u_1\} \cup S) \subseteq L$$

are algebraic and so is $K(u_1, s_2, \ldots, s_m) \subseteq L$. We can therefore replace S by $\{u_1, s_2, \ldots, s_m\}$ and repeat the argument with u_2. Since $\{u_1, u_2\}$ is algebraically independent, u_2 can also be exchanged for an s_i, say s_2. Iteration finally yields $S = \{u_1, \ldots, u_n, s_{n+1}, \ldots, s_m\}$ and $n \leq m$. □

Theorem II.4.14. *Any two transcendence bases of a field extension have the same cardinality.*

Proof. Let $K \subseteq L$ be a field extension with transcendence bases B and C. Each $b \in B$ is then algebraic over $K(C)$ and thus also over $K(C_b)$ for a finite subset $C_b \subseteq C$. Conversely, each $c \in C$ is algebraic over $K(B)$ and thus also over $K(\bigcup_{b\in B} C_b)$. Thus $K(\bigcup_{b\in B} C_b) \subseteq K(C) \subseteq L$ are algebraic field extensions and Lemma II.4.11 shows $C = \bigcup_{b\in B} C_b$.

Now let $B_1 \subseteq B$ be a finite subset. Then $L_1 := K(B_1 \cup \bigcup_{b\in B_1} C_b)$ is algebraic (even finite) over $K(\bigcup_{b\in B_1} C_b)$. Theorem II.4.13 with L_1 instead of L shows $|B_1| \leq \left|\bigcup_{b\in B_1} C_b\right|$. Hall's Marriage Theorem now provides pairwise distinct $c_b \in C_b$ for all $b \in B$. Thus the map $B \to C$, $b \mapsto c_b$ is injective. For reasons of symmetry, there is also an injective map $C \to B$. By Cantor-Bernstein, B and C have the same cardinality. □

Definition II.4.15. The cardinality of a transcendence basis of a field extension $K \subseteq L$ is called the *transcendence degree* of L over K and is written as $\operatorname{trg}(L|K)$ (by Theorem II.4.14 this is well-defined).

Example II.4.16.

(i) $K \subseteq L$ is algebraic if and only if $\operatorname{trg}(L|K) = 0$.

(ii) $\operatorname{trg}(K(X)|K) = \operatorname{trg}(\mathbb{Q}(\pi)|\mathbb{Q}) = 1$.

(iii) If L and M are purely transcendental extensions of K with the same transcendence degree, then

$$L = K(B) \overset{\text{II.4.7}}{\cong} K(X_b : b \in B) \cong M,$$

where B is a transcendence basis of L.

(iv) Let $K := \mathbb{Q}(X)$ and L be a splitting field of $\alpha := Y^2 + X^2 + 1 \in K[Y]$. We show that $\mathbb{Q} \subseteq L$ is absolutely transcendental, but not purely transcendental. Suppose α has a root $y \in K$. Then there exist $\beta, \gamma \in \mathbb{Q}[X] \setminus \{0\}$ with $y = \beta/\gamma$ and $(\beta/\gamma)^2 = -X^2 - 1$. One obtains the contradiction $\beta^2 = -(X^2+1)\gamma^2$ (compare signs of the leading coefficients). Thus α is irreducible and $|L : K| = 2$. Now let ω be a root of α in L.

Let $x \in L$ be algebraic over $\mathbb{Q}$. Then there exist $a, b \in K$ with $x = a + b\omega$. As a Galois extension of degree 2 (Exercise I.57), L has an automorphism $\sigma \in \operatorname{Gal}(L|K)$ with $\sigma(\omega) = -\omega$. Along with x, $\sigma(x)$ is also algebraic over $\mathbb{Q}$. According to Theorem I.13.4,

$$\frac{1}{4}(x - \sigma(x))^2 = b^2\omega^2 = -b^2(X^2 + 1) \in K$$

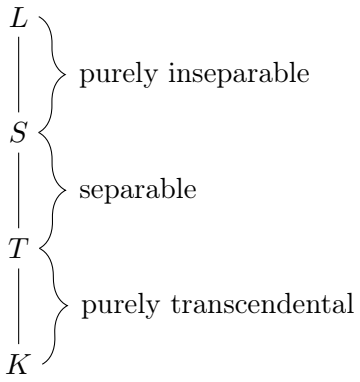
is also algebraic over $\mathbb{Q}$. Since $\mathbb{Q} \subseteq K$ is absolutely transcendental according to Lemma II.4.9, it follows that $q := b^2(X^2+1) \in \mathbb{Q}$. Writing $b = \beta/\gamma$ with $\beta, \gamma \in \mathbb{Q}[X]$, one obtains $\beta^2(X^2+1) = q\gamma^2$. In the case $b \neq 0$, the multiplicity of the irreducible polynomial X^2+1 is odd on the left side and even on the right. The unique factorization (Theorem I.8.24) therefore implies $b = 0$ and $x = a \in K$. Since $\mathbb{Q} \subseteq K$ is absolutely transcendental, it follows that $x \in \mathbb{Q}$. Thus $\mathbb{Q} \subseteq L$ is absolutely transcendental.

Since $\{X\}$ is a transcendence basis of L over $\mathbb{Q}$, we have $\operatorname{trg}(L|\mathbb{Q}) = 1$. Suppose there exists a transcendence basis $\{z\}$ with $L = \mathbb{Q}(z)$. Then there exist $\beta, \gamma, \delta, \rho \in \mathbb{Q}[X]\backslash\{0\}$ with $X = \beta(z)/\gamma(z)$ and $\omega = \delta(z)/\rho(z)$. From $\omega^2 + X^2 + 1 = 0$ it follows that

$$\delta(z)^2\gamma(z)^2 + \beta(z)^2\rho(z)^2 + \gamma(z)^2\rho(z)^2 = 0.$$

Since z is transcendental over $\mathbb{Q}$, we have $(\delta\gamma)^2 + (\beta^2+\gamma^2)\rho^2 = 0$. This is impossible, because the leading coefficient of this polynomial is positive. Therefore $\mathbb{Q} \subseteq L$ is not purely transcendental. One can show that every subfield of $\mathbb{Q}(X)$ is purely transcendental (Theorem A.5.3).

Remark II.4.17. According to Theorem II.3.8 and the results above, every field extension $K \subseteq L$ can be split into $K \subseteq T \subseteq S \subseteq L$, where $K \subseteq T$ is purely transcendental, $T \subseteq S$ is separable, and $S \subseteq L$ is purely inseparable.



Theorem II.4.18 (Degree Theorem for $\operatorname{trg}(L|K)$)**.** *For field extensions $K \subseteq L \subseteq M$, it holds that*

$$\boxed{\operatorname{trg}(M|K) = \operatorname{trg}(M|L) + \operatorname{trg}(L|K).}$$

Proof. Let B and C be transcendence bases of L over K and M over L, respectively. It suffices to show that $B \cup C$ is a transcendence basis of M over K with $B \cap C = \varnothing$. Every $c \in C$ is transcendental over L and therefore not contained in $B \subseteq L$. This shows $B \cap C = \varnothing$. By assumption, $K(B) \subseteq L$ and $L(C) \subseteq M$ are algebraic. Thus, $K(B \cup C) \subseteq L(C)$ and $K(B \cup C) \subseteq M$ are also algebraic. According to Theorem II.4.12, there exists a transcendence basis S of M over K with $B \subseteq S \subseteq B \cup C$. With $K(S) \subseteq L$, $L(S \cap C) \subseteq M$ is also algebraic, because $K(S) = K(B)(S \cap C) \subseteq L(S \cap C)$. Lemma II.4.11 shows $S = B \cap C$. □

Example II.4.19. Let B be a transcendence basis of $\mathbb{C}$ over $\mathbb{Q}$. Suppose that B is at most countable. As a countable union of countable sets,

$$\mathbb{Q}(B) \cong \mathbb{Q}(X_1, \ldots) = \bigcup_{n=1}^{\infty} \mathbb{Q}(X_1, \ldots, X_n)$$

is then also countable. Since $\mathbb{Q}(B) \subseteq \mathbb{C}$ is algebraic, every complex number is a root of a polynomial in $\mathbb{Q}(B)[X]$. Thus, $\mathbb{C}$ would also be countable. This contradiction shows that B is uncountable. More precisely, $\operatorname{trg}(\mathbb{C}|\mathbb{Q}) = |\mathbb{R}|$ holds. Because of $\operatorname{trg}(\mathbb{C}|\mathbb{R}) = 0$, it follows that $\operatorname{trg}(\mathbb{R}|\mathbb{Q}) = |\mathbb{R}|$ according to Theorem II.4.18.

Theorem II.4.20 (Fundamental Theorem on Symmetric Rational Functions)**.** *Let $\alpha \in K(X_1, \ldots, X_n)$ be invariant under all permutations of the X_i. Then there exists exactly one $\gamma \in K(X_1, \ldots, X_n)$ with $\alpha = \gamma(\sigma_1, \ldots, \sigma_n)$, where $\sigma_1, \ldots, \sigma_n$ are the elementary symmetric polynomials.*

Proof. Let $M := K(X_1, \ldots, X_n)$, $L := K(\sigma_1, \ldots, \sigma_n) \subseteq M$ and $G := \mathrm{Gal}(M|L)$. According to Vieta, M is a splitting field of $(Y - X_1) \ldots (Y - X_n) \in L[Y]$. According to Artin and Kronecker, $L \subseteq M$ is a Galois extension with $|G| = |M : L| \leq n!$. On the other hand, every permutation $\sigma \in S_n$ induces an automorphism $f_\sigma \in G$ with $f_\sigma(X_i) = X_{\sigma(i)}$ for $i = 1, \ldots, n$. This shows $G \cong S_n$ and $\alpha \in M^G = L$. Therefore, there exists a $\gamma = \frac{\gamma_1}{\gamma_2} \in L$ with $\alpha = \gamma(\sigma_1, \ldots, \sigma_n)$.

Let also $\delta = \frac{\delta_1}{\delta_2}$ with $\alpha = \delta(\sigma_1, \ldots, \sigma_n)$. Then $(\gamma_1\delta_2)(\sigma_1, \ldots, \sigma_n) = (\delta_1\gamma_2)(\sigma_1, \ldots, \sigma_n)$ holds. Because of $\mathrm{trg}(L|K) = \mathrm{trg}(L|K) + \mathrm{trg}(M|L) = \mathrm{trg}(M|K) = n$, $\sigma_1, \ldots, \sigma_n$ are algebraically independent over K. From Lemma II.4.6 it follows that $\gamma_1\delta_2 = \delta_1\gamma_2$ and $\delta = \gamma$. □

Remark II.4.21. According to Exercise I.53, $\mathrm{Aut}(\mathbb{Q}) = 1 = \mathrm{Aut}(\mathbb{R})$. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ with $\sigma(\mathbb{R}) = \mathbb{R}$. Then $\sigma_\mathbb{R} \in \mathrm{Aut}(\mathbb{R})$ and $\sigma_\mathbb{R} = \mathrm{id}_\mathbb{R}$. As a Galois automorphism of $\mathbb{C}$ over $\mathbb{R}$, σ is either trivial or the complex conjugation. We show that $\mathbb{C}$ possesses many more automorphisms (which then cannot leave $\mathbb{R}$ fixed).

Theorem II.4.22. *The field $\mathbb{C}$ possesses uncountably many automorphisms.*

Proof. Let B be a transcendence basis of $\mathbb{C}$ over $\mathbb{Q}$. Every permutation $\sigma \in \mathrm{Sym}(B)$ induces an automorphism $\hat{\sigma}$ on $\mathbb{Q}[X_b : b \in B]$ with $\hat{\sigma}(X_b) = X_{\sigma(b)}$. According to the universal property of the field of fractions (Exercise I.40), we can extend $\hat{\sigma}$ to an automorphism on $\mathbb{Q}(X_b : b \in B)$. Because of $\mathbb{Q}(B) \cong \mathbb{Q}(X_b : b \in B)$, one obtains from this an automorphism $\Gamma_\sigma \in \mathrm{Aut}(\mathbb{Q}(B))$ with $\Gamma_\sigma(b) = \sigma(b)$. Since $\mathbb{Q}(B) \subseteq \mathbb{C}$ is algebraic and $\mathbb{C}$ is algebraically closed, Γ_σ can be extended to a homomorphism $\hat{\Gamma}_\sigma \colon \mathbb{C} \to \mathbb{C}$ according to Theorem II.2.10. Every $x \in \mathbb{C}$ is a root of its minimal polynomial $\mu \in \mathbb{Q}(B)[X]$. Since $\Gamma_{\sigma^{-1}}(\mu) \in \mathbb{Q}(B)[X]$ splits into linear factors over $\mathbb{C}$, there exists a $y \in \mathbb{C}$ with $\hat{\Gamma}_\sigma(y) = x$. Therefore, $\hat{\Gamma}_\sigma$ is surjective and, as usual, also injective (Lemma I.8.41). Since B is uncountable, $\mathrm{Sym}(B)$ and $\mathrm{Aut}(\mathbb{C})$ are also uncountable. □

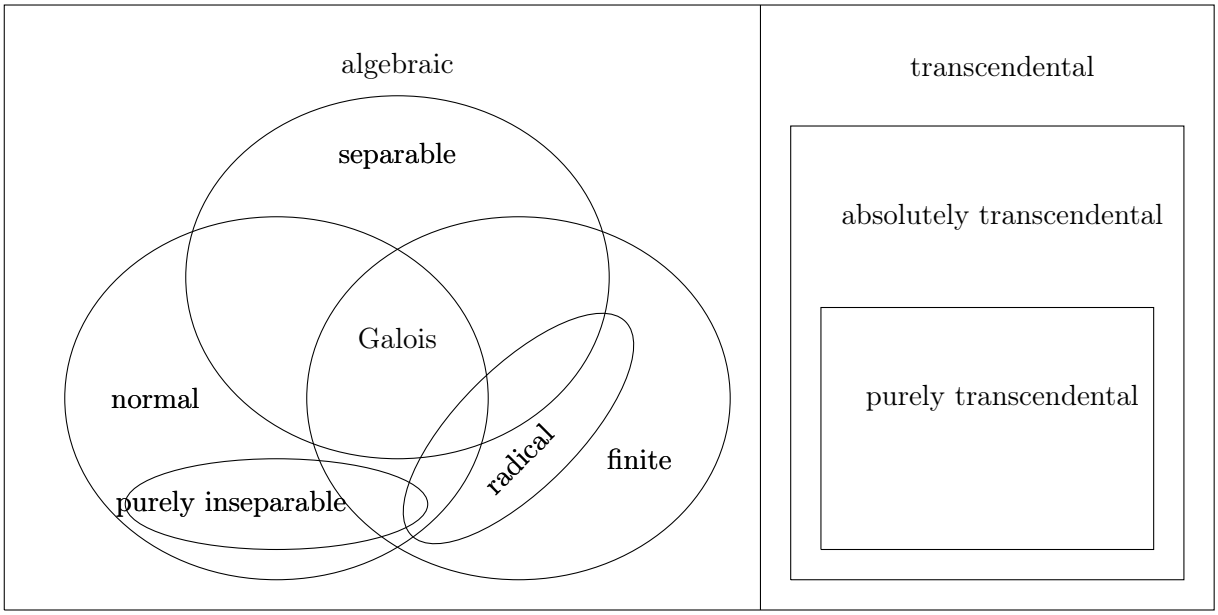
Remark II.4.23.

(i) With a bit more set theory[1] one can show $|\mathrm{Aut}(\mathbb{C})| \geq |\mathrm{Sym}(B)| = |\mathrm{Sym}(\mathbb{R})| > |\mathbb{R}|$. See also Corollary A.7.12.

(ii) With the *normal* field extensions defined in Exercise II.23, the following overview results, in which

[1] See notes on logic and set theory

the trivial extension $K \subseteq K$ has been neglected:



II.5 Divisibility in Integral Domains

Remark II.5.1. In this chapter we investigate when a ring possesses a unique prime factorization just as in $\mathbb{Z}$ or $K[X]$. For this purpose, let R always be an integral domain (commutative ring without zero divisors).

Definition II.5.2. For $a, b \in R$ we write (as usual) $a \mid b$ if there exists a $c \in R$ with $ac = b$. One then says: *a divides b*, *a is a divisor of b* or *b is divisible by a*.

Remark II.5.3. For $a, b, c, d, e \in R$ the usual calculation rules hold:

- $\pm 1 \mid a \mid 0$,
- $0 \mid a \iff a = 0$,
- $a \mid b \mid c \implies a \mid c$,
- $a \mid b, c \implies a \mid (bd + ce)$.

Lemma II.5.4. *For $a, b \in R$ the following statements are equivalent:*

(1) $a \mid b \mid a$,

(2) $\exists e \in R^\times : a = be$,

(3) $(a) = (b)$.

In this case, a and b are called associated.

Proof.

(1) $\Rightarrow$ (2): There exist $d, e \in R$ with $ad = b$ and $be = a$. Therefore $a(de - 1) = be - a = 0$. In the case $a = 0$, then also $b = 0d = 0$ and the claim holds with $e = 1$. Otherwise $de = 1 = ed$ holds, since R is an integral domain and commutative. It follows that $e \in R^\times$ with $a = be$.

(2) $\Rightarrow$ (3): By assumption, it holds that

$$(a) = aR = beR \subseteq bR = (b) = ae^{-1}R \subseteq aR = (a).$$

(3) $\Rightarrow$ (1): Because $a \in (a) = (b) = bR$, there exists a $c \in R$ with $a = bc$. Thus $b \mid a$ and for reasons of symmetry, $a \mid b$ also holds. □

Remark II.5.5. The unit group $R^\times$ acts on R by ${}^e a := ea$. Two elements $a, b \in R$ are associated if and only if they lie in the same orbit of this action. Therefore, being associated is an equivalence relation on R.

Example II.5.6.

(i) The elements in R associated to 1 are exactly the units $R^\times$. In a field, all non-zero elements are therefore associated.

(ii) In $R = \mathbb{Z}$, a and b are associated if and only if $b = \pm a$ holds (Example I.7.5).

Definition II.5.7. One calls $p \in R \setminus (R^\times \cup \{0\})$

- *irreducible*, if for all $a, b \in R$ it holds: $p = ab \Rightarrow a \in R^\times \vee b \in R^\times$ (cf. prime number).
- *prime element*, if for all $a, b \in R$ it holds: $p \mid ab \Rightarrow p \mid a \vee p \mid b$ (cf. Lemma I.2.16).

Lemma II.5.8. *Prime elements are irreducible.*

Proof. Let $p \in R$ be a prime element and $p = ab$ with $a, b \in R$. Then p is a divisor of a or b, say $p \mid a$. Because $a \mid p$, a and p are associated. Let $e \in R^\times$ with $p = ae$. Then it follows that $a(b - e) = 0$. Because $p \neq 0 \neq a$, it holds that $b = e \in R^\times$. Thus p is irreducible. □

Example II.5.9.

(i) If R is a field, then there exist neither irreducible elements nor prime elements, because $R = R^\times \cup \{0\}$.

(ii) In $\mathbb{Z}$ the following holds: p irreducible $\iff$ p prime element $\iff$ $|p|$ prime number. In $K[X]$ for a field K, the irreducible elements likewise coincide with the prime elements (Theorem I.8.24) and each such element is associated to exactly one irreducible polynomial (note: irreducible polynomials are monic).

(iii) If $p \in R$ is irreducible (or a prime element), then so is every element associated to p.

(iv) In general, not every irreducible element is a prime element (see also Exercise II.24): We consider

$$R := \mathbb{Z}[\sqrt{-5}] := \mathbb{Z} + \mathbb{Z}\sqrt{-5} = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\}.$$

Because of $(a+b\sqrt{-5})(c+d\sqrt{-5}) = ac-5bd+(bc+ad)\sqrt{-5}$, R is a subring of $\mathbb{C}$ and therefore an integral domain. For all $x = a+b\sqrt{-5} \in R$, it holds that $|x|^2 = a^2+5b^2 \in \mathbb{Z}$. Let $x := 1+\sqrt{-5} \in R$. In the case $x \in R^\times$, it would follow that $1 = |x|^2|x^{-1}|^2 = 6|x^{-1}|^2 \in 6\mathbb{Z}$. Thus $x \notin R^\times$. For $y, z \in R$ with $x = yz$, it holds that $|y|^2|z|^2 = |x|^2 = 6$. Since the equation $a^2 + 5b^2 = 2$ has no integer solution, wlog. $|y|^2 = 1$. This shows $y = \pm 1 \in R^\times$. Thus x is irreducible. On the other hand, $x \mid x\bar{x} = 6 = 2 \cdot 3$. If x were a prime element, there would exist $y \in R$ with $xy = 2$ or $xy = 3$. This is excluded because $|xy|^2 = 6|y|^2 \notin \{4, 9\}$. Thus x is not a prime element.

Lemma II.5.10. *Let $p_1, \ldots, p_s, q_1, \ldots, q_t \in R$ be prime elements with $p_1 \ldots p_s = q_1 \ldots q_t$. Then $s = t$ and, with suitable numbering, p_i is associated to q_i for $i = 1, \ldots, s$.*

Proof. Induction on s: In the case $s = 0$, we have $q_1 \ldots q_t = 1$ and $q_1 \in R^\times$. Since prime elements are not units, $t = 0$ holds. Now let $s \geq 1$ and the assertion be already proven for $s - 1$. From $p_s \mid p_1 \ldots p_s = q_1 \ldots q_t$ it follows that $p_s \mid q_i$ for some $i \in \{1, \ldots, t\}$, say $i = t$. So let $e \in R$ with $p_s e = q_t$. Since q_t is irreducible by Lemma II.5.8, $e \in R^\times$ holds. In particular, p_s and q_t are associated. It follows that

$$(p_1 \ldots p_{s-1} - q_1 \ldots q_{t-1}e)p_s = p_1 \ldots p_s - q_1 \ldots q_t = 0.$$

Because $p_s \neq 0$, we have $p_1 \dots p_{s-1} = q_1 \dots (q_{t-1}e)$. By induction, $s = t$ and, with suitable numbering, p_i is associated to q_i or to $q_{t-1}e$ for $i = 1, \dots, s-1$. This shows the assertion. □

Definition II.5.11. An integral domain R is called *factorial*[1], if every element in $R \setminus (R^\times \cup \{0\})$ is a product of prime elements.

Theorem II.5.12. *The following statements are equivalent:*

(1) R is factorial.

(2) Every $a \in R \setminus (R^\times \cup \{0\})$ can be written as a product of irreducible elements and every irreducible element is a prime element.

(3) Every $a \in R \setminus (R^\times \cup \{0\})$ can be written uniquely as a product of irreducible elements up to order and associates.

Proof.

(1) ⇒ (2): Since every prime element is irreducible, we only need to show the second part. Every irreducible element $p \in R$ can be written as a product of prime elements. Since prime elements are not units, p itself is a prime element.

(2) ⇒ (3): Follows from Lemma II.5.10.

(3) ⇒ (1): It suffices to show that every irreducible element $p \in R$ is a prime element. Let $p \mid ab$ for $a, b \in R$. Let $c \in R$ with $pc = ab$. We decompose $a = a_1 \dots a_r$, $b = b_1 \dots b_s$ and $c = c_1 \dots c_t$ into irreducible elements. From the uniqueness of the decomposition

$$pc_1 \dots c_t = a_1 \dots a_r b_1 \dots b_s$$

it follows that p is associated to an a_i or to a b_i. Therefore $p \mid a$ or $p \mid b$ holds. Thus p is a prime element. □

Example II.5.13.

(i) Every field is factorial.

(ii) Certainly $\mathbb{Z}$ and $K[X]$ for a field K are factorial.

(iii) According to Example II.5.9, $\mathbb{Z}[\sqrt{-5}]$ is not factorial, because $1 + \sqrt{-5}$ is irreducible but not a prime element. This phenomenon ruined Cauchy's and Lamé's attempts at a proof for Fermat's Last Theorem.

(iv) Most integral domains are already factorial if every irreducible element is a prime element (Exercise II.31).[2]

[1] or *UFD* (unique factorization domain)

[2] A counterexample is constructed in `http://ramanujan.math.trinity.edu/rdaileda/teach/m4363s07/non_ufd.pdf`.

Remark II.5.14.

(i) Let R be a factorial ring and $P \subseteq R$ a system of representatives for the classes of associated prime elements (for example the prime numbers in $R = \mathbb{Z}$ or the irreducible polynomials in $R = K[X]$). Then every $x \in R \setminus \{0\}$ has a unique *prime factorization*

$$x = e \prod_{p \in P} p^{\nu_p(x)}$$

with $e \in R^\times$ and $\nu_p(x) \in \mathbb{N}_0$ for $p \in P$. For $x, y \in R \setminus \{0\}$, $x \mid y$ holds if and only if $\nu_p(x) \leq \nu_p(y)$ for all $p \in P$. For $x_1, \ldots, x_n \in R \setminus \{0\}$ one sets

$$\gcd(x_1, \ldots, x_n) := \prod_{p \in P} p^{\min\{\nu_p(x_1), \ldots, \nu_p(x_n)\}},$$
$$\operatorname{lcm}(x_1, \ldots, x_n) := \prod_{p \in P} p^{\max\{\nu_p(x_1), \ldots, \nu_p(x_n)\}}.$$

Up to associativity, gcd and lcm do not depend on P. In the case $\gcd(x_1, \ldots, x_n) \in R^\times$, one calls $x_1, \ldots, x_n$ *coprime*.

(ii) In the field of fractions $Q(R)$, every $x \in Q(R) \setminus \{0\}$ has a unique decomposition of the form

$$x = e \prod_{p \in P} p^{\nu_p(x)}$$

with $e \in R^\times$ and $\nu_p(x) \in \mathbb{Z}$ for $p \in P$.

Definition II.5.15. An integral domain R is called a *principal ideal domain*, if every ideal in R is a principal ideal.

Example II.5.16. According to Example I.7.9(vii) and Lemma I.8.37, $\mathbb{Z}$ and $K[X]$ are principal ideal domains. According to Exercise I.48, $\mathbb{Z}[X]$ is not a principal ideal domain.

Remark II.5.17. According to Exercise II.4, $P \lhd R$ is a *prime ideal*, if $ab \in P \Rightarrow a \in P \vee b \in P$ holds for all $a, b \in R$. If $p \in R$ is a prime element, then (p) is a prime ideal.

Lemma II.5.18. *For every element $p \neq 0$ of a principal ideal domain R, the following statements are equivalent:*

(1) (p) is a maximal ideal,

(2) (p) is a prime ideal,

(3) p is a prime element,

(4) p is irreducible.

Proof. According to Exercise II.4, (1)⇒(2) holds. If (p) is a prime ideal and $p \mid ab$, then $ab \in (p)$, so $a \in (p)$ or $b \in (p)$. This shows $p \mid a$ or $p \mid b$. Therefore p is a prime element. According to Lemma II.5.8, (3)⇒(4) holds. Finally, let p be irreducible. Because of $p \notin R^\times$, $(p) \neq R$. Let $(p) \subseteq I \lhd R$. Since R is a principal ideal domain, there exists an $a \in R$ with $I = (a)$. Because of $p \in I$, there exists a $b \in R$ with $p = ab$. Because of $I \neq R$, $a \notin R^\times$. Since p is irreducible, it follows that $b \in R^\times$. This shows $I = (p)$ according to Lemma II.5.4. Therefore (p) is a maximal ideal. □

Theorem II.5.19. *Principal ideal domains are factorial.*

Proof. Let R be a principal ideal domain. According to Lemma II.5.18, every irreducible element is a prime element. According to Theorem II.5.12, it suffices to show that every $x_1 \in R \setminus (R^\times \cup \{0\})$ is a product of irreducible elements. Suppose the contrary. Then there exist $x_2, y \in R \setminus R^\times$ with $x_1 = x_2 y$, where x_2 is not irreducible. Because $y \notin R^\times$, we have $(x_1) \subsetneq (x_2)$. We can now repeat the argument with x_2 and obtain $x_3 \in R \setminus R^\times$ with $(x_2) \subsetneq (x_3)$ and so on. Obviously, $I := \bigcup_{i=1}^{\infty}(x_i)$ is then an ideal. Since R is a principal ideal domain, there exists an $x \in R$ with $I = (x)$. Then there exists an $i \in \mathbb{N}$ with $x \in (x_i)$. This yields the contradiction $(x_{i+1}) \subseteq I = (x) \subseteq (x_i)$. □

Lemma II.5.20 (Bézout)**.** *Let R be a principal ideal domain and $a_1, \ldots, a_n \in R \setminus \{0\}$. Then there exist $x_1, \ldots, x_n \in R$ with $\gcd(a_1, \ldots, a_n) = x_1 a_1 + \ldots + x_n a_n$.*

Proof. Let $g := \gcd(a_1, \ldots, a_n)$. Since R is a principal ideal domain, there exists an $a \in R$ with $(a) = (a_1, \ldots, a_n) \subseteq (g)$. Let P be a system of representatives for the classes of associated prime elements. Because $(a_i) \subseteq (a) \subseteq (g)$, it holds that $\nu_p(g) \leq \nu_p(a) \leq \nu_p(a_i)$ for $i = 1, \ldots, n$ and $p \in P$. Therefore

$$\nu_p(g) \overset{\text{II.5.14}}{=} \min_{1 \leq i \leq n} \nu_p(a_i) = \nu_p(a)$$

for all $p \in P$, i. e. a and g are associated. It follows that $(g) = (a) = (a_1, \ldots, a_n) = Ra_1 + \ldots + Ra_n$. Therefore there exist $x_1, \ldots, x_n$ with $x_1 a_1 + \ldots + x_n a_n = g$. □

Remark II.5.21. As a subring of $Q(R)[X]$, the polynomial ring $R[X]$ over R is an integral domain. Because $\deg(\alpha\beta) = \deg(\alpha) + \deg(\beta)$, we have $R[X]^\times = R^\times$. Irreducible elements in R are also irreducible in $R[X]$. In particular, irreducible elements in $R[X]$ can also be constant (e. g. 2 in $\mathbb{Z}[X]$). In the following, we generalize our earlier results about $\mathbb{Z}[X]$ (Lemma I.8.48).

Definition II.5.22. A polynomial $\alpha \in R[X]$ over a factorial ring R is called *primitive*, if the gcd of its coefficients is a unit.

Example II.5.23. A primitive polynomial has no divisors in $R \setminus R^\times$. In particular, every irreducible element $\alpha \in R[X] \setminus R$ is primitive.

Lemma II.5.24. *Let R be a factorial ring with quotient field $K = Q(R)$ and $\alpha, \beta \in R[X]$.*

(i) $\alpha\beta$ is primitive if and only if α and β are primitive.

(ii) For $\alpha \in K[X] \setminus \{0\}$ there exist $b \in K$ and $\tilde{\alpha} \in R[X]$ primitive with $\alpha = b\tilde{\alpha}$.

(iii) If $\alpha, \beta \in R[X]$ are primitive and $\alpha \mid \beta$ in $K[X]$, then $\alpha \mid \beta$ also holds in $R[X]$.

(iv) If $\alpha \in R[X] \setminus R$ is irreducible in $R[X]$, then α is also irreducible in $K[X]$ (up to normalization).

Proof.

(i) Obviously, $\alpha\beta$ can only be primitive if α and β are primitive. Conversely, assume that $\alpha\beta$ is not primitive. Since R is factorial, $\alpha\beta$ is divisible by a prime element $p \in R$. By replacing the coefficients with their residue classes in $\overline{R} := R/(p)$, we obtain $\overline{\alpha\beta} = 0$ in $\overline{R}[X]$ (reduction modulo p). Since (p) is a prime ideal, $\overline{R}$ is an integral domain according to Exercise II.4. Therefore, $\overline{R}[X]$ is also an integral domain and it follows that $\overline{\alpha} = 0$ or $\overline{\beta} = 0$ (as usual, the reduction modulo p is a ring homomorphism). Therefore, the coefficients of α or β are divisible by p.

(ii) Let $r \neq 0$ be a common denominator of the coefficients of α. Then $r\alpha \in R[X]$. Let s be a ggT of the coefficients of $r\alpha$. Then $b := \frac{s}{r} \in K$ and $\tilde{\alpha} := b^{-1}\alpha \in R[X]$ is primitive.

(iii) By assumption, there exists a $\gamma \in K[X]$ with $\alpha\gamma = \beta$. According to (ii), there exists a $b \in K$ such that $b\gamma \in R[X]$ is primitive. According to (i), $b\alpha\gamma = b\beta$ is also primitive. Since β is primitive, it follows that $b \in R^\times$ and $\gamma \in R[X]$. Therefore, $\alpha \mid \beta$ holds in $R[X]$.

(iv) According to Example II.5.23, α is primitive. Assume indirectly $\alpha = \beta\gamma$ with $\beta, \gamma \in K[X] \setminus K$. According to (ii), there exist primitive $\tilde{\beta}, \tilde{\gamma} \in R[X]$ as well as $b, c \in K$ with $\beta = b\tilde{\beta}$ and $\gamma = c\tilde{\gamma}$. According to (i), $\tilde{\beta}\tilde{\gamma}$ is primitive and $\alpha = bc\tilde{\beta}\tilde{\gamma} \in R[X]$. Since α is primitive, it follows that $bc \in R^\times$. Since α is irreducible, then $\tilde{\beta}$ or $\tilde{\gamma}$ would be in $R[X]^\times = R^\times \subseteq K$. □

Theorem II.5.25 (Gauss)**.** *If R is factorial, then so is $R[X]$.*

Proof. Let $K = Q(R)$. We first show that every $\alpha \in R[X] \setminus (R^\times \cup \{0\})$ is a product of irreducible elements. Let $\alpha = a\tilde{\alpha}$ with $a \in R$ and $\tilde{\alpha} \in R[X]$ primitive. Since R is factorial, a is a product of irreducible elements of R, which are also irreducible in $R[X]$. We can therefore assume $\alpha = \tilde{\alpha}$. If α is reducible in $R[X]$, then there exist $\beta, \gamma \in R[X] \setminus R$ with $\alpha = \beta\gamma$. One can now replace α by β or γ. Because $\deg\beta, \deg\gamma < \deg\alpha$, one eventually obtains a decomposition into irreducible elements.

Now we show that every irreducible element $\alpha \in R[X]$ is a prime element. Let $\alpha \mid \beta\gamma$ for $\beta, \gamma \in R[X]$. We write $\beta = b\tilde{\beta}$ and $\gamma = c\tilde{\gamma}$ with $b, c \in R$ and $\tilde{\beta}, \tilde{\gamma} \in R[X]$ primitive. In the case $\alpha \in R$, α is also irreducible in R and thus a prime element of R, since R is factorial. Since $\tilde{\beta}\tilde{\gamma}$ is primitive (Lemma II.5.24), it then follows that $\alpha \mid bc$ and wlog. $\alpha \mid b$. This shows $\alpha \mid b\tilde{\beta} = \beta$. Now let $\alpha \notin R$. According to Lemma II.5.24, α is then irreducible in $K[X]$. Since $K[X]$ is factorial as a principal ideal ring, α is a prime element in $K[X]$. According to Lemma II.5.24, α is then also a prime element in $R[X]$. According to Theorem II.5.12, $R[X]$ is factorial. □

Example II.5.26. According to Theorem II.5.25, $\mathbb{Z}[X]$ is factorial, but not a principal ideal ring (Exercise I.48). Inductively, one obtains that $K[X_1, \ldots, X_n]$ is also factorial for every field K.

Remark II.5.27. In a similar way, the Eisenstein criterion and the reduction criterion (Lemma I.8.56) can be generalized to factorial rings (Exercise II.27).

Example II.5.28. The polynomial $X^2 + Y^3(Y-2)X + Y - 2$ is irreducible in $\mathbb{Z}[X,Y] = \mathbb{Z}[Y][X]$ according to Eisenstein, because $Y - 2$ is irreducible (and thus a prime element) in $\mathbb{Z}[Y]$.

Definition II.5.29. An integral domain R is called *Euclidean*, if a map $H\colon R \to \mathbb{N}_0$ with the following property exists: For all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ with $a = qb + r$ and $H(r) < H(b)$ (Euclidean division).[3]

Theorem II.5.30. *Euclidean rings are principal ideal rings and thus factorial.*

Proof. Let $I \trianglelefteq R$ and wlog. $I \neq \{0\}$. Then $M := \{H(a) : 0 \neq a \in I\}$, as a non-empty subset of $\mathbb{N}_0$, has a smallest element $H(b)$ for some $b \in I \setminus \{0\}$. Certainly $(b) \subseteq I$. For $a \in I$ there exist $q, r \in R$ with $a = qb + r$ and $H(r) < H(b)$. Because of $r = a - qb \in I$, it follows that $r = 0$ from the choice of b. This shows $a = qb \in (b)$ and $I = (b)$. □

[3] To simplify calculations, one often additionally requires $H(0) = 0$ and $H(a) \leq H(ab)$ for all $a, b \in R \setminus \{0\}$, see [P. Samuel, *About Euclidean rings*, J. Algebra 19 (1971), 282–301]

Example II.5.31.

(i) Every field K is Euclidean with $H(0) := 0$ and $H(a) := 1$ if $a \neq 0$.

(ii) Obviously $\mathbb{Z}$ with $H(a) := |a|$ is Euclidean. Analogously $K[X]$ with $H(0) := 0$ and $H(\alpha) := 1 + \deg \alpha$ for $\alpha \neq 0$ is Euclidean according to Theorem I.8.15.

(iii) We show that the ring of *Gaussian integers*

$$\mathbb{Z}[\mathrm{i}] := \mathbb{Z} + \mathbb{Z}\mathrm{i} \subseteq \mathbb{C}$$

is Euclidean with $H(x) := |x|^2 = a^2 + b^2$ for $x = a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$. Because of $(a + b\mathrm{i})(c + d\mathrm{i}) = ac - bd + (ad + bc)\mathrm{i}$ for $a, b, c, d \in \mathbb{Z}$, $\mathbb{Z}[\mathrm{i}]$ is a subring of $\mathbb{C}$ and therefore an integral domain. For $x, y \in \mathbb{Z}[\mathrm{i}]$ with $y \neq 0$ we have $\frac{x}{y} = \alpha + \beta\mathrm{i}$ with $\alpha, \beta \in \mathbb{R}$. Choose $s, t \in \mathbb{Z}$ with $|\alpha - s|, |\beta - t| \leq \frac{1}{2}$ and set $q := s + t\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ as well as $r := x - qy$. Then

$$H(r) = |x - qy|^2 = |y|^2 \Big|\frac{x}{y} - q\Big|^2 = |y|^2\big(|\alpha - s|^2 + |\beta - t|^2\big) \leq \frac{1}{2}|y|^2 < |y|^2 = H(y).$$

Analogously one shows that $\mathbb{Z}[\sqrt{d}]$ for $d \in \{-2, 2, 3\}$ is Euclidean (Exercise II.29). On the other hand, $\mathbb{Z}[\sqrt{-5}]$ is not Euclidean, as it is not a factorial ring.

(iv) One can show that $\mathbb{Z}\Big[\frac{1+\sqrt{-19}}{2}\Big]$ is a non-Euclidean principal ideal domain.[4] Note:

$$\begin{aligned} \text{Field} &\implies \text{Euclidean} \implies \text{Principal ideal domain} \implies \text{Factorial ring} \\ &\implies \text{Integral domain} \implies \text{Commutative} \end{aligned}$$

Remark II.5.32. In every Euclidean ring R, a $\gcd(a, b)$ for $a, b \in R \setminus \{0\}$ can be determined using the extended Euclidean algorithm:

- Set $(x_0, y_0, z_0) := (1, 0, a)$, $(x_1, y_1, z_1) := (0, 1, b)$ and $k := 0$.
- As long as $z_{k+1} \neq 0$ repeat:

  $$(x_{k+2}, y_{k+2}, z_{k+2}) := (x_k - x_{k+1}q_{k+1}, y_k - y_{k+1}q_{k+1}, r_{k+1}),$$

  where $z_k = q_{k+1}z_{k+1} + r_{k+1}$ with $H(r_{k+1}) < H(z_{k+1})$.
- For $z_{k+1} = 0$ we have $\gcd(a, b) = z_k = x_k a + y_k b$.

Example II.5.33. We determine the units and prime elements of $R = \mathbb{Z}[\mathrm{i}]$. For $e = a + b\mathrm{i} \in R^\times$, it holds that $1 = |ee^{-1}|^2 = H(e)H(e^{-1})$. This shows $a^2 + b^2 = H(e) = 1$ and $R^\times = \{\pm 1, \pm\mathrm{i}\}$. Now let $\pi \in R$ be a prime element. Because $\pi \notin R^\times$, $\pi \mid \pi\overline{\pi} = |\pi|^2 \geq 2$. Therefore, π divides a prime factor p of $H(\pi)$. If π also divides $q \in \mathbb{P} \setminus \{p\}$, then π also divides $\gcd(p, q) = 1$ and one obtains the contradiction $\pi \in R^\times$. Thus, p is the only prime number divisible by π. One can therefore determine the prime elements in R by decomposing the prime numbers into prime elements. Every $\pi \in R$ with $H(\pi) \in \mathbb{P}$ is obviously irreducible and therefore a prime element in R. In particular, $1 + \mathrm{i} \in R$ is a prime element and $2 = -\mathrm{i}(1 + \mathrm{i})^2$ is the prime factorization of 2 (one says: 2 is *ramified*).

Now let $p \equiv 3 \pmod 4$ and $\sigma, \tau \in R$ with $p = \sigma\tau$. Then

$$H(\sigma)H(\tau) = H(p) = p^2. \tag{II.5.1}$$

[4] See [R.A. Wilson, *An elementary proof that not all principal ideal domains are Euclidean domains*, Math. Gaz. 101 (2017), 289–293, `https://www.jstor.org/stable/pdf/44821320.pdf`]

Because $a^2+b^2 \not\equiv 3 \pmod 4$ for all $a, b \in \mathbb{Z}$, the equation $a^2+b^2 = p$ has no integer solutions. Therefore, p is a prime element in R (one says: p is *inert*).

Finally, let $p \equiv 1 \pmod 4$ and $q := (p-1)/2 \in 2\mathbb{Z}$. According to Wilson (Exercise I.9)

$$-1 \equiv (p-1)! \equiv \prod_{k=1}^{q} k(p-k) \equiv (-1)^q (q!)^2 \equiv (q!)^2 \pmod p.$$

This shows $p \mid (q!)^2 + 1 = (q! - \mathrm{i})(q! + \mathrm{i})$. If p were a prime element in R, then $p = \bar{p} \mid q! \pm \mathrm{i}$ and

$$0 \not\equiv 2q! = (q! + \mathrm{i}) + (q! - \mathrm{i}) \equiv 0 \pmod p.$$

Thus p is not a prime element and according to (II.5.1) there exists a prime factor $\pi \mid p$ with $\pi\overline{\pi} = H(\pi) = p$. Wlog. let $\pi \mid q! + \mathrm{i}$. Suppose π and $\overline{\pi}$ are associated. Then π and $\overline{\pi}$ would be divisors of $q! \pm \mathrm{i}$ and therefore also divisors of $2 = \mathrm{i}((q! - \mathrm{i}) - (q! + \mathrm{i}))$. However, we already know that every prime element divides only one prime number. Therefore, π and $\overline{\pi}$ are not associated (one says: p is *split*). For example, $5 = (2+\mathrm{i})(2-\mathrm{i})$.

Theorem II.5.34. *$n \in \mathbb{N}$ can be written as a sum of two integer squares if and only if the multiplicity of every prime number $p \equiv 3 \pmod 4$ in the prime factorization of n is even. In particular, every prime number $p \equiv 1 \pmod 4$ is a sum of two squares.*

Proof.

$\Rightarrow$: Let $n = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i})$ with $a, b \in \mathbb{Z}$. According to Example II.5.33, one obtains the prime factorization of $a + b\mathrm{i}$ as follows

$$a + b\mathrm{i} = e(1+\mathrm{i})^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} \pi_p^{\delta_p} \overline{\pi_p}^{\delta'_p}$$

with $e \in \{\pm 1, \pm \mathrm{i}\}$ and $\delta_2, \delta_p, \delta'_p \in \mathbb{N}_0$. Therefore

$$n = |a + b\mathrm{i}|^2 = 2^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{2\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} p^{\delta_p + \delta'_p}$$

is the prime factorization of n.

$\Leftarrow$: By assumption

$$n = 2^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{2\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} p^{\delta_p} = |\alpha|^2 = H(\alpha)$$

with

$$\alpha = (1+\mathrm{i})^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} \pi_p^{\delta_p} \in \mathbb{Z}[i].$$

Therefore there exist $a, b \in \mathbb{Z}$ with $\alpha = a + b\mathrm{i}$ and $a^2 + b^2 = H(\alpha) = n$. □

II.6 Modules

Remark II.6.1. In this chapter, we investigate vector spaces over rings instead of fields. Unlike in linear algebra, bases do not exist in general in this situation. Even if bases exist, they do not have to be of the same size. The theory thereby becomes more complicated, but also richer.

Definition II.6.2. Let R be a ring (not necessarily commutative). An abelian group $(M, +)$ is called an (R-)*left module*, if a scalar multiplication $R \times M \to M$, $(r, m) \mapsto rm$ exists with the following properties:

- $r(m + n) = rm + rn$,
- $(r + s)m = rm + sm$,
- $(rs)m = r(sm)$,
- $1_R m = m$

for all $r, s \in R$ and $m, n \in M$. Right modules are defined analogously.

Remark II.6.3. In the following, we always mean left modules by *modules*. In some books and computer algebra systems, right modules are often preferred.

Example II.6.4.

(i) The *trivial* module $0 := \{0\}$.

(ii) If R is a field, then the modules are precisely the vector spaces.

(iii) Every abelian group A is a $\mathbb{Z}$-module if one defines (as in Remark I.3.2)

$$za := \begin{cases} a + \ldots + a \ (z \text{ summands}) & \text{if } z \geq 0, \\ -|z|a & \text{if } z < 0 \end{cases}$$

for $z \in \mathbb{Z}$ and $a \in A$. Conversely, every ($\mathbb{Z}$-)module is of course an abelian group.

(iv) With the ring addition and ring multiplication, R becomes an R-module, which is called the *regular* R-module.

(v) If one replaces the multiplication in R by

$$a * b := ba \qquad (a, b \in R) \qquad (a, b \in R),$$

one obtains the *opposite* ring R^o with $1_{R^0} = 1_R$. Every R-left module M becomes an R^o-right module via $mr := rm$ ($r \in R$, $m \in M$), because for $r, s \in R$ we have

$$m(r * s) = m(sr) = (sr)m = s(rm) = (rm)s = (mr)s.$$

(vi) Let K be a field and $R := K^{n\times n}$ for $n \in \mathbb{N}$. For $m \in \mathbb{N}$, $K^{n\times m}$ is then an R-module with matrix multiplication.

(vii) If M is an R-module and $f\colon S \to R$ is a ring homomorphism, then M becomes an S-module via $sm := f(s)m$ ($s \in S$, $m \in M$). If S is a subring of R and f is the inclusion map, one obtains in this way the *restriction* of M to S. In the case $R = S/I$ for an $I \trianglelefteq S$, one can choose the canonical epimorphism $f\colon S \to S/I$. Every S/I-module is therefore also an S-module.

(viii) If $(M_i)_{i\in I}$ is a family of R-modules, then the *direct product* $\bigtimes_{i\in I} M_i$ becomes an R-module with component-wise operations. In the case $I = \{1, \ldots, n\}$, one writes as usual $M_1 \times \ldots \times M_n$ and M_1^n if $M_1 = \ldots = M_n$.

Remark II.6.5. Let M be an R-module, $r \in R$ and $m \in M$. Then

$$r0_M = r(0_M + 0_M) = r0_M + r0_M = 0_M,$$
$$0_R m = (0_R + 0_R)m = 0_R m + 0_R m = 0_M.$$

Definition II.6.6. A subset N of an R-module M is called a *submodule* of M if N itself is an R-module with the restricted operations. As with groups, we then write $N \leq M$ or $N < M$ if $N \neq M$.

Remark II.6.7. A subset N of an R-module M is a submodule if and only if $(N, +) \leq (M, +)$ and $rN \subseteq N$ for all $r \in R$. Equivalent is also: $N \neq \varnothing$ and $rx + sy \in N$ for all $x, y \in N$ and $r, s \in R$.

Example II.6.8.

(i) For modules over fields, the submodules are of course the subspaces.

(ii) The submodules of a $\mathbb{Z}$-module are exactly the subgroups.

(iii) 0 and M are always submodules of M.

(iv) The intersection of any number of submodules is a submodule.

(v) For an R-module M and $S \subseteq M$,

$$RS := \langle S\rangle := \bigcap_{\substack{N\leq M\\ S\subseteq N}} N \leq M$$

is the submodule *generated* by S. Obviously, RS consists of the elements of the form $r_1s_1+\ldots+r_ns_n$ with $r_1, \ldots, r_n \in R$ and $s_1, \ldots, s_n \in S$. In the case $RS = M$, S is a *generating set* of M. If additionally $|S| < \infty$, then M is called *finitely generated*.

(vi) For every family of submodules $(N_i)_{i\in I}$ of M, the *sum*

$$\sum_{i\in I} N_i := \Big\langle \bigcup_{i\in I} N_i \Big\rangle = \Big\{ x_1 + \ldots + x_n : n \in \mathbb{N},\ x_1, \ldots, x_n \in \bigcup N_i \Big\}$$

is also a submodule of M. In the case $N_i \cap \sum_{j\neq i} N_j = 0$ for all $i \in I$, we call the sum *direct* and write, as with groups, $\bigoplus_{i\in I} N_i$. This means that the representation of an element $x = x_1+\ldots+x_n$ with $x_j \in N_{i_j}$ ($j = 1, \ldots, n$) is unique up to the order of the summands.

(vii) The submodules of the regular module are called *left ideals* of R. Certainly every ideal is a left ideal. If R is commutative, the converse also holds. In the future, we will denote the zero ideal by 0 instead of $\{0\}$.

(viii) If M is an R-module and $I \trianglelefteq R$, then

$$IM := \left\{ \sum_{i=1}^{n} x_i m_i : n \in \mathbb{N}, x_1, \ldots, x_n \in I, m_1, \ldots, m_n \in M \right\} \leq M.$$

Theorem II.6.9. *If $N \leq M$ are R-modules, then the factor group M/N becomes an R-module via*

$$r(x + N) := rx + N \qquad (r \in R, x \in M),$$

which is called the factor module.

Proof. Since M is an abelian group, every subgroup is normal and M/N is a group. For $x, y \in M$ with $x + N = y + N$, it holds that $x - y \in N \Longrightarrow rx - ry = r(x - y) \in N \Longrightarrow rx + N = ry + N$. Therefore, the scalar multiplication is well-defined. The calculation rules transfer easily from M to M/N. □

Definition II.6.10. A map $f\colon M \to N$ for R-modules M, N is called a *homomorphism* (or *R-linear*) if $f(rx + y) = rf(x) + f(y)$ holds for $r \in R$ and $x, y \in M$. The set of all homomorphisms is denoted by $\mathrm{Hom}_R(M, N)$. As usual, one defines mono-, epi-, endo-, iso- and automorphisms. Differing from groups and rings, we write $M \simeq N$ or more precisely $M \simeq_R N$ for the isomorphism of modules.

Remark II.6.11.

(i) Every homomorphism $f\colon M \to N$ of R-modules is also a group homomorphism. As usual, it therefore holds that $\mathrm{Ker}(f) \leq M$ and $f(M) \leq N$.

(ii) For modules $N \leq M$, the *canonical* group epimorphism $M \to M/N$ is also R-linear.

(iii) If $f\colon M \to N$ is a bijective homomorphism, then $f^{-1}\colon N \to M$ is also a homomorphism, because

$$f^{-1}(rm) = f^{-1}\big(rf(f^{-1}(m))\big) = f^{-1}\big(f(rf^{-1}(m))\big) = rf^{-1}(m)$$

for $m \in M$ and $r \in R$.

(iv) If $f, g\colon M \to N$ are R-linear, then so is $f + g\colon M \to N$, $m \mapsto f(m) + g(m)$. This makes $\mathrm{Hom}_R(M, N)$ into an abelian group. In the case $M = N$, $f \circ g \in \mathrm{Hom}_R(M, M) =: \mathrm{End}_R(M)$ also holds. As usual, $f \circ (g + h) = f \circ g + f \circ h$ and $(f + g) \circ h = f \circ h + g \circ h$ then hold for $f, g, h \in \mathrm{End}_R(M)$. In this way, $\mathrm{End}_R(M)$ becomes a ring with identity element id_M (in the case of finite-dimensional vector spaces, $\mathrm{End}_R(M)$ is nothing more than a matrix ring). $\mathrm{End}_R(M)$ is called the *endomorphism ring* of M.

(v) Every R-module M becomes an $\mathrm{End}_R(M)$-module via $\varphi \cdot m := \varphi(m)$ for $\varphi \in \mathrm{End}_R(M)$ and $m \in M$.

Theorem II.6.12.

(i) (Homomorphism theorem) For every homomorphism of modules $f\colon M \to N$, it holds that

$$\boxed{M/\mathrm{Ker}(f) \simeq f(M).}$$

(ii) (Correspondence theorem) For modules $N \leq M$, the canonical epimorphism $M \to M/N$ induces a bijection between the set of submodules $L \leq M$ with $N \leq L$ and the set of submodules of M/N.

(iii) (*1st Isomorphism theorem*) *For $U, V \leq M$, it holds that $V \leq U + V \leq M$, $U \cap V \leq U$ and*

$$\boxed{(U+V)/V \simeq U/U \cap V.}$$

(iv) (*2nd Isomorphism theorem*) *For modules $U \leq V \leq M$,*

$$\boxed{M/V \simeq (M/U)/(V/U).}$$

Proof. We already know from Theorem I.3.29 that the map $F\colon M/\mathrm{Ker}(f) \to f(M)$, $m+\mathrm{Ker}(f) \mapsto f(m)$ is a well-defined group isomorphism. Because of

$$F\big(r(m+\mathrm{Ker}(f))\big) = F(rm+\mathrm{Ker}(f)) = f(rm) = rf(m) = rF(m+\mathrm{Ker}(f))$$

for $r \in R$ and $m \in M$, F is also an isomorphism of modules. The other statements are consequences of the homomorphism theorem and therefore also hold for modules. □

Definition II.6.13. An R-module $M \neq 0$ is called *simple* if 0 and M are the only submodules of M.

Lemma II.6.14 (Schur's Lemma)**.** *Let M and N be non-isomorphic simple R-modules. Then* $\mathrm{End}_R(M)$ *is a division ring and* $\mathrm{Hom}_R(M,N) = 0$.

Proof. Let $f \in \mathrm{Hom}_R(M,N)$. From the simplicity of M and N it follows that $\mathrm{Ker}(f) \in \{0, M\}$ and $f(M) \in \{0, N\}$. In the case $\mathrm{Ker}(f) = 0$ one obtains the contradiction $M \simeq M/\mathrm{Ker}(f) \simeq f(M) = N$. Thus $\mathrm{Ker}(f) = M$, i. e. $f = 0$. In the case $M = N$ one obtains

$$f \neq 0 \iff \mathrm{Ker}(f) = 0 \wedge f(M) = N \iff f \text{ bijective.}$$

With f, then also $f^{-1} \in \mathrm{End}_R(M)$. Thus $\mathrm{End}_R(M)^\times = \mathrm{End}_R(M) \setminus \{0\}$. □

Example II.6.15.

(i) A vector space V over a field K is simple if and only if $\dim V = 1$. In this case, $\mathrm{End}_K(V) \cong K$.

(ii) An abelian group A is a simple $\mathbb{Z}$-module if and only if A is simple as a group. If applicable, $A \cong C_p$ and $\mathrm{End}_{\mathbb{Z}}(A) \cong \mathbb{F}_p$ for some $p \in \mathbb{P}$ (Example I.6.3).

(iii) Let I be a proper left ideal of a ring R. As in Krull's Theorem, one proves using Zorn's Lemma the existence of a maximal left ideal M of R with $I \subseteq M$. According to the correspondence theorem (applied to the regular module), R/M is then a simple R-module. In particular, every ring $R \neq \{0\}$ possesses a simple module (choose $I = 0$).

(iv) Conversely, let M be a simple R-module and $0 \neq m \in M$. Then the map $f\colon R \to M$, $r \mapsto rm$ is an epimorphism and the isomorphism theorem shows $M \simeq R/\mathrm{Ker}(f)$.

Remark II.6.16. As with groups, one defines composition series for modules and proves the Jordan-Hölder Theorem (the proof is even simpler, since one no longer has to worry about the normal subgroup property). However, not every module possesses a composition series (for example, the regular $\mathbb{Z}$-module).

II.7 Finiteness conditions

Remark II.7.1. In linear algebra, one proves theorems for finite-dimensional vector spaces. Since finitely generated modules generally behave less decently, we introduce a series of stronger finiteness conditions.

Theorem II.7.2. *For an R-module M, the following statements are equivalent:*

(1) Every submodule of M is finitely generated.

(2) Every ascending chain of submodules $N_1 \subseteq N_2 \subseteq \ldots$ of M becomes stationary*, i. e. there exists a $k \in \mathbb{N}$ with $N_k = N_{k+1} = \ldots$.*

(3) Every non-empty set of submodules of M possesses a maximal element (w.r.t. $\subseteq$).

If applicable, M is called noetherian.

Proof.

(1) $\Rightarrow$ (2): Let $N_1 \subseteq N_2 \subseteq \ldots$ be a sequence of submodules of M. According to (1), $\sum_{i=1}^{\infty} N_i = Rm_1 + \ldots + Rm_n$ holds for certain $m_1, \ldots, m_n \in M$. Let $k \in \mathbb{N}$ with $m_1, \ldots, m_n \in N_k$. For $l \geq k$ it then follows that

$$N_l \subseteq \sum_{i=1}^{\infty} N_i = Rm_1 + \ldots + Rm_n \leq N_k \leq N_l.$$

(2) $\Rightarrow$ (3): Let $\mathcal{N}$ be a non-empty set of submodules of M and $N_1 \in \mathcal{N}$. If N_1 is maximal, then we are finished. Otherwise there exists $N_2 \in \mathcal{N}$ with $N_1 \subsetneq N_2$. If N_2 is also not maximal, then there exists $N_3 \in \mathcal{N}$ with $N_1 \subsetneq N_2 \subsetneq N_3$ and so on. According to (2), one finds a maximal element in this way after finitely many steps.

(3) $\Rightarrow$ (1): Let $N \leq M$. If N is not finitely generated, then there exist $x_1, x_2, \ldots \in N$ with

$$Rx_1 \subsetneq Rx_1 + Rx_2 \subsetneq \ldots.$$

Then the set of submodules $Rx_1 + \ldots + Rx_n$ ($n \in \mathbb{N}$) possesses no maximal element, in contradiction to (3). □

Theorem II.7.3. *For an R-module M, the following statements are equivalent:*

(1) Every descending sequence of submodules $N_1 \supseteq N_2 \supseteq \ldots$ of M becomes stationary.

(2) Every non-empty set of submodules of M possesses a minimal element (with respect to $\subseteq$).

If applicable, M is called Artinian.

Proof.

(1) ⇒ (2): Let $\mathcal{N}$ be a non-empty set of submodules of M and $N_1 \in \mathcal{N}$. If N_1 is minimal, then we are finished. Otherwise there exists $N_2 \in \mathcal{N}$ with $N_1 \supsetneq N_2$ and so on. After finitely many steps, one finds a minimal element.

(2) ⇒ (1): Let $N_1 \supseteq N_2 \supseteq \ldots$ be a sequence of submodules of M. Then the set $\{N_i : i \in \mathbb{N}\}$ possesses a minimal element N_k. For $l \geq k$, it then holds that $N_l \subseteq N_k \subseteq N_l$. □

Theorem II.7.4. *For an R-module M, the following statements are equivalent:*

(1) M is a sum of simple submodules.

(2) M is a direct sum of simple submodules.

(3) For every submodule $U \leq M$, there exists a $V \leq M$ with $M = U \oplus V$.

If applicable, M is called semisimple.

Proof.

(1) ⇒ (2): Let $M = \sum_{i \in I} S_i$ with simple submodules $S_i \leq M$ $(i \in I)$. Then

$$\mathcal{I} := \Big\{ J \subseteq I : \sum_{j \in J} S_j = \bigoplus_{j \in J} S_j \Big\}$$

is non-empty because of $\varnothing \in \mathcal{I}$ and ordered by $\subseteq$. For a totally ordered subset $\varnothing \neq \mathcal{K} \subseteq \mathcal{I}$, let $T := \bigcup_{K \in \mathcal{K}} K \subseteq I$ and $N := \sum_{t \in T} S_t$. Suppose $0 \neq x \in S_t \cap \sum_{i \in T \setminus \{t\}} S_i$ for some $t \in T$. Then there exist $t_1, \ldots, t_n \in T \setminus \{t\}$ and $x_i \in S_{t_i}$ with $x = x_1 + \ldots + x_n$. Since $\mathcal{K}$ is totally ordered, there exists $K \in \mathcal{K}$ with $t, t_1, \ldots, t_n \in K$. But then $\sum_{k \in K} S_k \neq \bigoplus_{k \in K} S_k$. Thus $N = \bigoplus_{t \in T} S_t$ and $T \in \mathcal{I}$ is an upper bound of $\mathcal{K}$. By Zorn's Lemma, $\mathcal{I}$ has a maximal element J. In the case $\bigoplus_{j \in J} S_j \neq M$, there exists an $i \in I$ with $S_i \nsubseteq \bigoplus_{j \in J} S_j$. Since $S_i \cap \bigoplus_{j \in J} S_j$ is a proper submodule of the simple module S_i, it follows that $S_i \cap \bigoplus_{j \in J} S_j = 0$. Thus

$$S_i + \bigoplus_{j \in J} S_j = \bigoplus_{j \in J \cup \{i\}} S_j$$

in contradiction to the maximality of J. This shows $M = \bigoplus_{j \in J} S_j$.

(2) ⇒ (3): Let $M = \bigoplus_{i \in I} S_i$ with simple submodules $S_i \leq M$ $(i \in I)$. For $U \leq M$,

$$\mathcal{I} := \Big\{ J \subseteq I : U \cap \sum_{j \in J} S_j = 0 \Big\}$$

has a maximal element J as above. In the case $M \neq U + \sum_{j \in J} S_j$, there exists an $i \in I$ with $S_i \nsubseteq U + \sum_{j \in J} S_j$. As above, $S_i \cap \big(U + \sum_{j \in J} S_j\big) = 0$. But then also $U \cap \sum_{j \in J \cup \{i\}} S_j = 0$ in contradiction to the maximality of J. This shows $M = U \oplus \sum_{j \in J} S_j$ and we can set $V := \sum_{j \in J} S_j$.

(3) ⇒ (1): Let U be the sum of all simple submodules of M. Then there exists $V \leq M$ with $M = U \oplus V$. Suppose $V \neq 0$ and choose $0 \neq x \in V$. The map $\alpha \colon R \to V$, $r \mapsto rx$ is then a homomorphism from the regular R-module to V. Because $1 \notin \operatorname{Ker}(\alpha)$, there exists a maximal left ideal I of R with $\operatorname{Ker}(\alpha) \subseteq I$ (Example II.6.15). By the Correspondence Theorem, R/I is a simple R-module. By assumption, there exists $N \leq M$ with $\alpha(I) \oplus N = M$. The Dedekind identity shows

$$\alpha(R) = M \cap \alpha(R) = (\alpha(I) + N) \cap \alpha(R) = \alpha(I) + (N \cap \alpha(R)) = \alpha(I) \oplus (N \cap \alpha(R)).$$

Therefore $N \cap \alpha(R) \simeq \alpha(R)/\alpha(I) \simeq R/I$ is simple and we obtain the contradiction $N \cap \alpha(R) \subseteq U \cap V = 0$. Thus $M = U$ is a sum of simple submodules. $\square$

Example II.7.5.

(i) Every simple module is semisimple.

(ii) According to Corollary II.2.3, every vector space V is semisimple. In contrast,

$$V \text{ noetherian} \iff \dim V < \infty \iff V \text{ artinian.}$$

(iii) Every finite abelian group is noetherian and artinian as a $\mathbb{Z}$-module, because it possesses only finitely many submodules. On the other hand, $V_4 \cong C_2 \times C_2$ is semisimple, but C_4 is not. Furthermore, $\mathbb{Z}$ is noetherian (since every subgroup is cyclic, thus finitely generated), but not artinian because of $\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq \ldots$.

(iv) We consider the *Prüfer group*

$$A_p := \left\{ \frac{a}{p^n} + \mathbb{Z} : a \in \mathbb{Z},\ n \in \mathbb{N} \right\} \leq \mathbb{Q}/\mathbb{Z}$$

for the prime number p. Let $B < A_p$ and $\frac{1}{p^n} + \mathbb{Z} \in B$ with $n \in \mathbb{N}_0$ chosen maximal. For $\frac{a}{p^m} + \mathbb{Z} \in B$ with $p \nmid a$ there exist $k, l \in \mathbb{Z}$ with $ak + p^m l = \gcd(a, p^m) = 1$. Then

$$\frac{1}{p^m} + \mathbb{Z} = k\frac{a}{p^m} + l + \mathbb{Z} = k\frac{a}{p^m} + \mathbb{Z} \in B$$

and the maximality of n shows $m \leq n$. Thus

$$B = \left\{ \frac{a}{p^n} + \mathbb{Z} : a = 0, \ldots, p^n - 1 \right\} = \left\langle \frac{1}{p^n} + \mathbb{Z} \right\rangle \cong C_{p^n}.$$

In particular, every proper subgroup of A_p is finite. Therefore A_p is an artinian $\mathbb{Z}$-module, but because of

$$\left\langle \frac{1}{p} + \mathbb{Z} \right\rangle \subsetneq \left\langle \frac{1}{p^2} + \mathbb{Z} \right\rangle \subsetneq \ldots$$

not noetherian. There are thus no implications whatsoever between the three finiteness conditions noetherian, artinian and semisimple.

(v) Let $M = \bigoplus_{i \in I} S_i$ be semisimple with simple submodules $S_i \leq M$. If M is additionally noetherian (or artinian), then $|I| < \infty$, because otherwise there would be a chain $S_{i_1} < S_{i_1} \oplus S_{i_2} < \ldots$ (resp. $M > \bigoplus_{i \in I \setminus \{i_1\}} S_i > \ldots$). In this case M is also artinian (resp. noetherian).

Lemma II.7.6. *Let $N \leq M$ be modules. M is noetherian (resp. artinian) if and only if N and M/N are noetherian (resp. artinian).*

Proof. Let M be noetherian. Every sequence of submodules $N_1 \subseteq N_2 \subseteq \ldots$ of N is then also a sequence of submodules of M and therefore becomes stationary. Analogously, if $M_1/N \subseteq M_2/N \subseteq \ldots$ is a sequence of submodules of M/N, then $M_1 \subseteq M_2 \subseteq \ldots$ also becomes stationary (Correspondence Theorem). Therefore N and M/N are noetherian.

Now let N and M/N be noetherian. Let $M_1 \subseteq M_2 \subseteq \ldots$ be a sequence of submodules of M. Then $M_1 \cap N \subseteq M_2 \cap N \subseteq \ldots$ are submodules of N and there exists a $k \in \mathbb{N}$ with $M_k \cap N = M_{k+1} \cap N = \ldots$.

Analogously $(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq \ldots$ are submodules of M/N and there exists an $l \in \mathbb{N}$ with $M_l + N = M_{l+1} + N = \ldots$. For $n \geq \max\{k, l\}$, the Dedekind identity implies:

$$M_n = M_n + (N \cap M_n) = M_n + (N \cap M_{n+1}) = (M_n + N) \cap M_{n+1} = (M_{n+1} + N) \cap M_{n+1} = M_{n+1}.$$

The statement for artinian instead of noetherian is shown analogously. □

Remark II.7.7. If M and N are noetherian (resp. artinian) R-modules, then so is $M \times N$, because $(M \times N)/(M \times 0) \simeq N$.

Theorem II.7.8. *An R-module M possesses a composition series if and only if M is noetherian and artinian.*

Proof. Let $0 = M_0 \leq \ldots \leq M_l = M$ be a composition series. For $l = 0$, $M = 0$ is certainly noetherian and artinian. Now let $l > 0$. Then $0 = M_0 \leq \ldots \leq M_{l-1}$ is a composition series of M_{l-1}. By induction on l, we can assume that M_{l-1} is noetherian and artinian. The simple module M/M_{l-1} is also noetherian and artinian. According to Lemma II.7.6, M is noetherian and artinian.

Conversely, let M be noetherian and artinian. Let $\mathcal{M}$ be the set of all submodules of M that possess a composition series. Since $0 \in \mathcal{M}$, $\mathcal{M} \neq \varnothing$. Since M is noetherian, $\mathcal{M}$ possesses a maximal element $N \leq M$. Assume $N < M$. Since M is artinian, M/N is also artinian (Lemma II.7.6). Therefore, the set of all non-trivial submodules of M/N possesses a minimal element L/N. Obviously, L/N is then simple. But then L also possesses a composition series, contradicting the choice of N. Thus $M = N$ possesses a composition series. □

Remark II.7.9. Assume that the regular R-module possesses a composition series. Let M be a simple R-module. According to Example II.6.15, there exists a left ideal I of R with $M \simeq R/I$. According to Theorem II.7.8 and Lemma II.7.6, I also possesses a composition series, which can be extended to a composition series of R. In particular, M is isomorphic to a composition factor of R. According to Jordan-Hölder, there are therefore only finitely many simple R-modules up to isomorphism.

Lemma II.7.10. *If M is a semisimple R-module and $N \leq M$, then N and M/N are also semisimple.*

Proof. For $U \leq N$ there exists a $V \leq M$ with $M = U \oplus V$. According to the Dedekind identity,

$$N = M \cap N = (U \oplus V) \cap N = U \oplus (V \cap N)$$

with $V \cap N \leq N$. Therefore N is semisimple. Furthermore, there exists an $N' \leq M$ with $M = N \oplus N'$. Then $N' \simeq M/N$ is also semisimple. □

Example II.7.11. The converse of Lemma II.7.10 is false: C_4 is not semisimple as a $\mathbb{Z}$-module, but $C_2 \leq C_4$ and $C_4/C_2 \cong C_2$.

Theorem II.7.12. *For an R-module $M \neq 0$, the following statements are equivalent:*

(1) There are no proper submodules $M_1, M_2 < M$ with $M = M_1 \oplus M_2$.

(2) 0 and id_M are the only idempotents in $\mathrm{End}_R(M)$.

If applicable, M is called indecomposable.

Proof.

(1) ⇒ (2): Let $f \in \mathrm{End}_R(M)$ be an idempotent. Let $M_1 := \mathrm{Ker}(f)$ and $M_2 := f(M)$. For $x \in M$ it holds that $f(x) = f(f(x))$ and $x - f(x) \in M_1$. This shows $x = (x - f(x)) + f(x) \in M_1 + M_2$. For $x \in M_1 \cap M_2$ there exists a $y \in M$ with $x = f(y)$. It follows that $x = f(f(y)) = f(x) = 0$. Thus $M_1 \cap M_2 = 0$ and $M = M_1 \oplus M_2$ holds. From the assumption it follows that $M_1 = 0$, $M_2 = M$ or $M_1 = M$, $M_2 = 0$. In the first case f is bijective and $f = f^2 f^{-1} = f f^{-1} = \mathrm{id}_M$. In the second case $f = 0$.

(2) ⇒ (1): Let $M_1, M_2 \leq M$ with $M = M_1 \oplus M_2$. Let $\pi_i \colon M \to M_i$ be the i-th projection for $i = 1, 2$. From $\pi_i^2 = \pi_i$ it follows that $\pi_i = \mathrm{id}_M$ or $\pi_i = 0$ by assumption. In the first case $M_1 = M$ and in the second case $M_2 = M$. □

Example II.7.13.

(i) Every simple module is indecomposable. Conversely, every indecomposable, semisimple module is simple.

(ii) The $\mathbb{Z}$-module C_4 is indecomposable, but not (semi)simple.

Lemma II.7.14 (Fitting)**.** *Let M be a Noetherian and Artinian R-module. For $f \in \mathrm{End}_R(M)$ there exists a $k \in \mathbb{N}$ with $M = \mathrm{Ker}(f^k) \oplus f^k(M)$.*

Proof. Since M is Noetherian and Artinian, the sequences $\mathrm{Ker}(f) \subseteq \mathrm{Ker}(f^2) \subseteq \ldots$ and $f(M) \supseteq f^2(M) \supseteq \ldots$ become stationary. Let $k \in \mathbb{N}$ with $\mathrm{Ker}(f^k) = \mathrm{Ker}(f^{k+1}) = \ldots$ and $f^k(M) = f^{k+1}(M) = \ldots$. For $x \in \mathrm{Ker}(f^k) \cap f^k(M)$ there exists $y \in M$ with $f^k(y) = x$. From $f^{2k}(y) = f^k(x) = 0$ it follows that $y \in \mathrm{Ker}(f^{2k}) = \mathrm{Ker}(f^k)$ and $x = f^k(y) = 0$. Thus $\mathrm{Ker}(f^k) \cap f^k(M) = 0$ holds. For an arbitrary $x \in M$ there exists $y \in M$ with $f^k(x) = f^{2k}(y)$. It follows that $x - f^k(y) \in \mathrm{Ker}(f^k)$ and

$$x = (x - f^k(y)) + f^k(y) \in \mathrm{Ker}(f^k) + f^k(M). \qquad \square$$

Lemma II.7.15. *Let M be a Noetherian, Artinian, indecomposable R-module and $f, g \in \mathrm{End}_R(M)$. If $f + g$ is bijective, then f or g is bijective.*

Proof. For $\tilde{f} := (f + g)^{-1} \circ f$ and $\tilde{g} := (f + g)^{-1} \circ g$, it holds that $\tilde{f} + \tilde{g} = \mathrm{id}_M$. Wlog. let f be not bijective. Then $\tilde{f}$ is also not bijective. According to Fitting, there exists $k \in \mathbb{N}$ with $\tilde{f}^k = 0$, since M is indecomposable. Because of

$$(\mathrm{id}_M - \tilde{f})(\mathrm{id}_M + \tilde{f} + \ldots + \tilde{f}^{k-1}) = \mathrm{id}_M$$

$\tilde{g} = \mathrm{id}_M - \tilde{f}$ is bijective. Thus $g = (f + g) \circ \tilde{g}$ is also bijective. □

Theorem II.7.16 (Krull-Schmidt)**.** *Every Noetherian, Artinian R-module M possesses a decomposition into indecomposable modules $M = M_1 \oplus \ldots \oplus M_k$, which are uniquely determined up to order and isomorphism.*

Proof.
Existence: If M is indecomposable, then the claim holds with $M_1 = M$. So let $M = M_1 \oplus M_2$ with $M_1, M_2 < M$. If M_1 and M_2 are indecomposable, then we are finished. So let wlog. $M_1 = M_3 \oplus M_4$ with $M_3, M_4 < M_1$. Iteration yields a sequence $M > M_1 > M_3 > \ldots$. Since M is Artinian, the process must terminate. One has then found a desired decomposition.

Uniqueness: Let $M = M_1 \oplus \ldots \oplus M_k = N_1 \oplus \ldots \oplus N_l$ be decompositions into indecomposable modules. Induction on k: For $k = 1$, M is indecomposable and $l = 1$. So let $k \geq 2$. Let $\pi_i \colon M \to M_i$ be the i-th projection of the first decomposition and $\rho \colon M \to N_1$ the first projection of the second decomposition. Then

$$\mathrm{id}_{N_1} = \rho_{|N_1} = \rho \circ (\pi_1 + \ldots + \pi_k)_{|N_1} = (\rho \circ \pi_1)_{|N_1} + \ldots + (\rho \circ \pi_k)_{|N_1}.$$

According to Lemma II.7.15, $(\rho \circ \pi_i)_{|N_1}$ is bijective for some i; wlog. $i = 1$. In particular, $(\pi_1)_{|N_1}$ is injective and $\rho_{|M_1}$ is surjective. For $\sigma := \pi_1 \circ (\rho \circ \pi_1)^{-1}_{|N_1} \circ \rho_{|M_1} \in \mathrm{End}_R(M_1)$, it clearly holds that

$$\sigma^2 = \pi_1 \circ (\rho \circ \pi_1)^{-1}_{|N_1} \circ \rho \circ \pi_1 \circ (\rho \circ \pi_1)^{-1}_{|N_1} \circ \rho_{|M_1} = \sigma \neq 0.$$

From Theorem II.7.12 it follows that $\sigma = \mathrm{id}_{M_1}$. Therefore $(\pi_1)_{|N_1}$ is also surjective. This shows $N_1 \simeq M_1$. For $x \in M_1$ there exists $y \in N_1$ with $\pi_1(x) = x = \pi_1(y)$ and $x - y \in \mathrm{Ker}(\pi_1) = M_2 + \ldots + M_k$. It follows that $M = N_1 + M_2 + \ldots + M_k$. For $x \in N_1 \cap (M_2 + \ldots + M_k)$, $\pi_1(x) = 0$ and $x = 0$, since $(\pi_1)_{|N_1}$ is injective. Thus

$$M = N_1 \oplus M_2 \oplus \ldots \oplus M_k$$

is shown. Because of $M_2 \oplus \ldots \oplus M_k \simeq M/N_1 \simeq N_2 \oplus \ldots \oplus N_l$, the claim now follows by induction. □

Definition II.7.17. For an R-module M,

$$\mathrm{Ann}_R(M) := \{r \in R : rM = 0\} \subseteq R$$

is called the *annihilator* of M.

Example II.7.18.

(i) For the regular R-module, $\mathrm{Ann}_R(R) = 0$ holds.

(ii) Let $A \cong C_{n_1} \times \ldots \times C_{n_k}$ be an abelian group. Then

$$m \in \mathrm{Ann}_{\mathbb{Z}}(A) \iff \forall a \in A : ma = 0 \iff \forall a \in A : |\langle a \rangle| \,\big|\, m \iff n_1, \ldots, n_k \mid m.$$

Thus $\mathrm{Ann}_{\mathbb{Z}}(A) = \mathbb{Z}\,\mathrm{lcm}(n_1, \ldots, n_k)$.

Lemma II.7.19.

(i) Annihilators are ideals.

(ii) Isomorphic modules have the same annihilators.

Proof.

(i) Let M be an R-module. Because of $0 \in \mathrm{Ann}_R(M)$, $\mathrm{Ann}_R(M)$ is non-empty. For $x, y \in \mathrm{Ann}_R(M)$ and $r \in R$, it holds that $(x - y)M \subseteq xM - yM = 0$, $rxM = r0 = 0$ and $xrM \subseteq xM = 0$.

(ii) Let $f \colon M \to N$ be an isomorphism of R-modules. Then

$$r \in \mathrm{Ann}_R(M) \iff rM = 0 \iff rN = rf(M) = f(rM) = 0 \iff r \in \mathrm{Ann}_R(N). \qquad \square$$

Lemma II.7.20. *For R-modules M, M', N, N', the following hold:*

(i) *For every idempotent $e \in R$, $\mathrm{End}_R(Re) \cong (eRe)^o$. In particular,* $\boxed{\mathrm{End}_R(R) \cong R^o.}$

(ii) $\boxed{\mathrm{End}_R(M^n) \cong \mathrm{End}_R(M)^{n\times n}}$ *for $n \in \mathbb{N}$.*

(iii) $\mathrm{Hom}_R(M,N) = 0 = \mathrm{Hom}_R(N,M) \implies \mathrm{End}_R(M \times N) \cong \mathrm{End}_R(M) \times \mathrm{End}_R(N)$.

(iv) $\mathrm{Hom}_R(M, N \times N') \simeq_{\mathbb{Z}} \mathrm{Hom}_R(M,N) \times \mathrm{Hom}_R(M,N')$.

(v) $\mathrm{Hom}_R(M \times M', N) \simeq_{\mathbb{Z}} \mathrm{Hom}_R(M,N) \times \mathrm{Hom}_R(M',N)$.

Proof.

(i) According to Exercise II.7, eRe is a ring with identity element e. Obviously, Re is a left ideal of R. We consider the map

$$\begin{aligned}\Phi\colon \mathrm{End}_R(Re) &\to (eRe)^o,\\ f &\mapsto f(e) = f(e^2) = ef(e).\end{aligned}$$

Because of $\mathrm{id}(e) = e$, $(f+g)(e) = f(e) + g(e)$ and

$$(f \circ g)(e) = f(g(e)) = f(g(e)e) = g(e)f(e) = f(e) * g(e)$$

Φ is a ring homomorphism. From $f(e) = 0$ it follows that $f(re) = rf(e) = 0$ for all $r \in R$. Therefore, Φ is injective. For a given $x \in eRe$, the map $f_x\colon Re \to Re$, $s \mapsto sx$ is R-linear. Because of $\Phi(f_x) = f_x(e) = ex = x$, Φ is also surjective. The last assertion follows with $e = 1$.

(ii) For $i = 1, \ldots, n$, the maps

$$\begin{aligned}\pi_i\colon M^n &\to M,\ (m_1, \ldots, m_n) \mapsto m_i,\\ \rho_i\colon M &\to M^n,\ m \mapsto (0, \ldots, 0, m, 0, \ldots, 0)\end{aligned}$$

are R-linear. It holds that

$$\pi_i\rho_j = \begin{cases}\mathrm{id}_M & \text{if } i = j,\\ 0 & \text{if } i \neq j,\end{cases} \qquad \mathrm{id}_{M^n} = \sum_{i=1}^n \rho_i\pi_i.$$

We define $\Phi\colon \mathrm{End}_R(M^n) \to \mathrm{End}_R(M)^{n\times n}$, $f \mapsto (\pi_i f \rho_j)_{i,j=1}^n$. Then $\Phi(\mathrm{id}) = (\pi_i\rho_j)_{i,j} = 1_n$ and $\Phi(f+g) = \Phi(f) + \Phi(g)$ for $f, g \in \mathrm{End}_R(M^n)$. Furthermore,

$$\Phi(fg) = (\pi_i f\,\mathrm{id}\, g\rho_j)_{i,j} = \Big(\pi_i f \sum_{k=1}^n \rho_k\pi_k g\rho_j\Big)_{i,j} = (\pi_i f\rho_j)_{i,j}(\pi_i g\rho_j)_{i,j} = \Phi(f)\Phi(g).$$

Therefore, Φ is a ring homomorphism. For $\Phi(f) = 0$, we also have

$$f = \Big(\sum_{i=1}^n \rho_i\pi_i\Big) f \Big(\sum_{j=1}^n \rho_j\pi_j\Big) = \sum_{i,j=1}^n \rho_i(\pi_i f\rho_j)\pi_j = 0$$

and Φ is injective. Finally, let $(f_{ij})_{i,j} \in \mathrm{End}_R(M)^{n\times n}$ be given. Then $f := \sum_{i,j=1}^n \rho_i f_{ij}\pi_j \in \mathrm{End}_R(M^n)$ with

$$\Phi(f) = \Big(\pi_i \sum_{k,l=1}^n \rho_k f_{kl}\pi_l\rho_j\Big)_{i,j} = (\mathrm{id}\, f_{ij}\, \mathrm{id})_{i,j} = (f_{ij})_{i,j}.$$

Thus Φ is surjective.

(iii) With the notation from (ii), let $\Phi\colon \mathrm{End}_R(M \times N) \to \mathrm{End}_R(M) \times \mathrm{End}_R(N)$, $f \mapsto (\pi_1 f \rho_1, \pi_2 f \rho_2)$. It is easily shown that Φ is a ring homomorphism. Let $\Phi(f) = 0$. Because of

$$\pi_1 f \rho_2 \in \mathrm{Hom}_R(N, M) = 0 \qquad\qquad \pi_2 f \rho_1 \in \mathrm{Hom}_R(M, N) = 0$$

we also have

$$f = (\rho_1\pi_1 + \rho_2\pi_2) f (\rho_1\pi_1 + \rho_2\pi_2) = 0$$

and Φ is injective. For $(f_1, f_2) \in \mathrm{End}_R(M) \times \mathrm{End}_R(N)$, let $f\colon = \rho_1 f_1 \pi_1 + \rho_2 f_2 \pi_2 \in \mathrm{End}_R(M \times N)$. Then

$$\Phi(f) = \big(\pi_1(\rho_1 f_1 \pi_1 + \rho_2 f_2 \pi_2)\rho_1, \pi_2(\rho_1 f_1 \pi_1 + \rho_2 f_2 \pi_2)\rho_2\big) = (f_1, f_2).$$

Therefore, Φ is also surjective.

(iv) It is easily shown that the maps

$$\begin{aligned} \mathrm{Hom}_R(M, N \times N') &\to \mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(M, N'), & f &\mapsto (\pi_1 f, \pi_2 f), \\ \mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(M, N') &\to \mathrm{Hom}_R(M, N \times N'), & (g_1, g_2) &\mapsto \rho_1 g_1 + \rho_2 g_2 \end{aligned}$$

are mutually inverse isomorphisms of $\mathbb{Z}$-modules.

(v) Analogous. □

II.8 Semisimple and Artinian Rings

Remark II.8.1. We transfer the finiteness conditions for modules to rings and will find that (in contrast to modules) there are indeed dependencies between the concepts.

Definition II.8.2. A ring R is called (*left*) *Noetherian* (resp. (*left*) *Artinian*, (*left*) *semisimple*), if the regular R-left module is Noetherian (resp. Artinian, semisimple).[1]

Example II.8.3.

(i) Every field K is Noetherian, Artinian and semisimple, because here 0 and K are the only left ideals.

(ii) Every principal ideal domain is Noetherian, because here every submodule is a principal ideal and therefore generated by only one element. On the other hand, the principal ideal domains $\mathbb{Z}$ and $K[X]$ are not Artinian (see Example II.7.5).

(iii) The (finite) ring $\mathbb{Z}/4\mathbb{Z}$ is Artinian, but not semisimple.

(iv) Let K be a field, $n \in \mathbb{N}$ and $R := K^{n\times n}$. Every left ideal $M \leq R$ is then a K-vector space because of $\lambda m = (\underbrace{\lambda 1_n}_{\in R})m \in M$ for all $m \in M$ and $\lambda \in K$. For dimension reasons, R is both Noetherian and Artinian.

(v) Now let Q be a division ring, $n \in \mathbb{N}$ and $R := Q^{n\times n}$. The set of column vectors $Q^{n\times 1}$ is obviously an R-module with respect to matrix multiplication. Let $0 \neq a = (a_1, \ldots, a_n)^{\mathrm{t}} \in Q^{n\times 1}$ and $b \in Q^{n\times 1}$ be arbitrary. Let $a_i \neq 0$ and $x := ba_i^{-1}e_i \in R$, where $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)$. Then $xa = b$ holds. This shows that $Q^{n\times 1}$ is simple. Obviously then

$$R = Q^{n\times 1}e_1 \oplus \ldots \oplus Q^{n\times 1}e_n \simeq (Q^{n\times 1})^n$$

is semisimple. According to Remark II.7.9, every simple R-module is furthermore isomorphic to $Q^{n\times 1}$.

Lemma II.8.4.

(i) If R is Noetherian (resp. Artinian), then every finitely generated R-module is Noetherian (resp. Artinian).

(ii) If R is semisimple, then every R-module is semisimple.

[1] Attention: In most books Noetherian = left Noetherian + right Noetherian (cf. Exercise II.39). The same applies to Artinian and semisimple.

Proof.

(i) Let $M = Rm_1 + \ldots + Rm_k$. Then the map $f\colon R^k \to M$, $(r_1, \ldots, r_k) \mapsto r_1m_1 + \ldots + r_km_k$ is an epimorphism. According to Remark II.7.7 and Lemma II.7.6, R^k and $M \simeq R^k/\mathrm{Ker}(f)$ are Noetherian (resp. Artinian).

(ii) Because of $R = \sum_{m\in M} Rm$, it suffices to show that Rm is semisimple. This follows from Lemma II.7.10, because for $f\colon R \to Rm$, $r \mapsto rm$, we have $Rm \simeq R/\mathrm{Ker}(f)$. □

Theorem II.8.5 (Artin-Wedderburn)**.** *For every ring R, the following statements are equivalent:*

(1) R is semisimple.

(2) There exist $n_1, \ldots, n_k \in \mathbb{N}$ and division rings $Q_1, \ldots, Q_k$ with

$$R \cong Q_1^{n_1\times n_1} \times \ldots \times Q_k^{n_k\times n_k}.$$

In this case, k is the number of isomorphism classes of simple R-modules and the pairs (n_i, Q_i) are uniquely determined up to the order (and isomorphism).

Proof.

(1) ⇒ (2): Let R be semisimple and $R = \bigoplus_{i\in I} M_i$ with simple submodules $M_i \leq R$ for $i \in I$. Then $1 = x_1 + \ldots + x_n$ with wlog. $x_i \in M_i \setminus \{0\}$ for $i = 1, \ldots, n$. From the simplicity of the M_i it follows that $M_i = Rx_i$ for $i = 1, \ldots, n$. Therefore

$$R = R1 \subseteq Rx_1 + \ldots + Rx_n = M_1 \oplus \ldots \oplus M_n \subseteq R.$$

After renumbering, it holds that $R \simeq M_1^{n_1} \oplus \ldots \oplus M_k^{n_k}$ with $M_i \not\simeq M_j$ for $i \neq j$. By Schur's Lemma, $\mathrm{Hom}_R(M_i, M_j) = 0$ for $i \neq j$ and $\mathrm{End}_R(M_i)$ is a division ring. Thus $Q_i := \mathrm{End}_R(M_i)^o$ is also a division ring for $i = 1, \ldots, k$. From Lemma II.7.20 it follows that

$$\begin{aligned} R &\cong \mathrm{End}_R(R)^o \cong \mathrm{End}_R(M_1^{n_1} \times \ldots \times M_k^{n_k})^o \cong (\mathrm{End}_R(M_1^{n_1}) \times \ldots \times \mathrm{End}_R(M_k^{n_k}))^o \\ &\cong (\mathrm{End}_R(M_1)^{n_1\times n_1} \times \ldots \times \mathrm{End}_R(M_k)^{n_k\times n_k})^o \\ &\cong (\mathrm{End}_R(M_1)^{n_1\times n_1})^o \times \ldots \times (\mathrm{End}_R(M_k)^{n_k\times n_k})^o. \end{aligned}$$

Finally, the transposition map $(\mathrm{End}_R(M_i)^{n_i\times n_i})^o \to (\mathrm{End}_R(M_i)^o)^{n_i\times n_i} = Q_i^{n_i\times n_i}$, $A \mapsto A^{\mathrm{t}}$ is a ring isomorphism, because

$$(BA)^{\mathrm{t}} = \Big(\sum_{k=1}^{n} b_{jk}a_{ki}\Big)_{i,j} = \Big(\sum_{k=1}^{n} a_{ki} * b_{jk}\Big)_{i,j} = A^{\mathrm{t}} * A^{\mathrm{t}}.$$

Thus R has the specified structure.

(2) ⇒ (1): According to Example II.8.3, the rings $R_i := Q_i^{n_i\times n_i}$ are semisimple and $R_i = M_{i1} \oplus \ldots \oplus M_{in_i}$ holds with simple R_i-modules $M_{i1} \simeq \ldots \simeq M_{in_i}$. Obviously, then

$$\widetilde{M}_{ij} := 0 \times \ldots \times 0 \times M_{ij} \times 0 \times \ldots \times 0 \qquad (1 \leq i \leq k,\ 1 \leq j \leq n_i)$$

are simple R-modules with

$$R = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{n_i} \widetilde{M}_{ij}.$$

Thus R is also semisimple. Obviously, $\widetilde{M}_{i1}, \ldots, \widetilde{M}_{in_i}$ are also isomorphic as R-modules. On the other hand, $(1_{n_1}, \ldots, 1_{n_{i-1}}, 0, 1_{n_{i+1}}, \ldots, 1_{n_k})$ lies in the annihilator of $\widetilde{M}_{i1}$, but not in the annihilator of $\widetilde{M}_{j1}$ if $i \neq j$. By Lemma II.7.19, the R-modules $\widetilde{M}_{i1}$ and $\widetilde{M}_{j1}$ are not isomorphic (even if $R_i = R_j$). According to Remark II.7.9, every simple R-module occurs as a composition factor of R. Therefore k is the number of isomorphism classes of simple R-modules. Furthermore, n_i is uniquely determined by R as the multiplicity of the composition factor $\widetilde{M}_{i1}$. For

$$e_i := (0, \ldots, 0, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, 0, \ldots, 0) \in R$$

it holds that $e_i^2 = e_i$ and $Re_i = \widetilde{M}_{i1}$. By Lemma II.7.20,

$$\mathrm{End}_R(\widetilde{M}_{i1}) = \mathrm{End}_R(Re_i) \cong (e_i R e_i)^o = (0, \ldots, 0, \begin{pmatrix} Q_i & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, 0, \ldots, 0)^o \cong Q_i^o.$$

In this way, the isomorphism type of Q_i is also determined by R. □

Corollary II.8.6. *Every semisimple ring is Artinian.*

Proof. As in the proof of Theorem II.8.5, $R = M_1 \oplus \ldots \oplus M_n$ with simple modules $M_1, \ldots, M_n$. Obviously, $0 \leq M_1 \leq M_1 + M_2 \leq \ldots \leq R$ is then a composition series of the regular R-module. According to Theorem II.7.8, R is Artinian. □

Theorem II.8.7 (Wedderburn)**.** *Finite division rings are fields.*

Proof (Witt). Let R be a finite division ring. Then the center $Z := \mathrm{Z}(R)$ is a commutative subring of R. Because of $xr = rx \Leftrightarrow rx^{-1} = x^{-1}r$, Z is even a field. Let $q := |Z|$. Obviously, R is a Z-vector space and therefore $|R| = q^n$ for some $n \in \mathbb{N}$. We assume indirectly $n > 1$. For $x \in R$, the centralizer $\mathrm{C}_R(x) = \{r \in R : rx = xr\}$ is also a Z-vector space (verify) and it follows $|\mathrm{C}_R(x)| = q^{a_x}$ for some $a_x \leq n$. Let S be a set of representatives for the conjugacy classes of the unit group $G := R^\times = R \setminus \{0\}$. The class equation shows

$$\begin{aligned} q^n - 1 = |G| &= \sum_{x \in S} |G : \mathrm{C}_G(x)| = |\mathrm{Z}(G)| + \sum_{x \in S \setminus Z} |G : \mathrm{C}_G(x)| \\ &= |Z^\times| + \sum_{x \in S \setminus Z} \frac{|R \setminus \{0\}|}{|\mathrm{C}_R(x) \setminus \{0\}|} = q - 1 + \sum_{x \in S \setminus Z} \frac{q^n - 1}{q^{a_x} - 1}. \end{aligned} \tag{II.8.1}$$

According to Lagrange, $q^{a_x} - 1 = |\mathrm{C}_G(x)|$ is a divisor of $|G| = q^n - 1$. According to the Euclidean algorithm, there exist $s, t \in \mathbb{Z}$ with

$$q^{\gcd(a_x, n)} = q^{sa_x + tn} = (q^{a_x})^s (q^n)^t \equiv 1 \pmod{q^{a_x} - 1}.$$

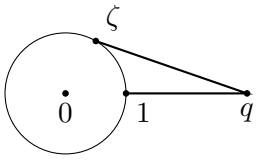
From $\gcd(a_x, n) \leq a_x$ it follows $a_x \mid n$ for all $x \in R$.

For all $x \in R \setminus Z$, $a_x < n$ holds. With the cyclotomic polynomials, it follows that

$$\Phi_n(q) \mid \prod_{\substack{d \mid n \\ d \nmid a_x}} \Phi_d(q) \overset{\text{I.12.9}}{=} \frac{q^n - 1}{q^{a_x} - 1} \mid q^n - 1.$$

From (II.8.1) it now follows $\Phi_n(q) \mid q - 1$. In particular, $|\Phi_n(q)| \leq q - 1$. For every primitive n-th root of unity $\zeta := \alpha + \beta\mathrm{i}$ with $\alpha, \beta \in \mathbb{R}$, $\alpha < 1$ because of $n > 1$. It follows

$$\begin{aligned} |q - \zeta|^2 &= (q - \alpha)^2 + \beta^2 = q^2 - 2\alpha q + \alpha^2 + \beta^2 \\ &> q^2 - 2q + |\zeta|^2 = q^2 - 2q + 1 = (q - 1)^2 \end{aligned}$$



and $|q - \zeta| > |q - 1| \geq 1$. Thus one obtains the contradiction

$$|\Phi_n(q)| = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n) = 1}} |q - \zeta^k| > |q - 1|. \qquad \square$$

Definition II.8.8. For an R-module M, let $\mathrm{J}(M)$ be the intersection of all maximal submodules of M. If M possesses no maximal submodules, one sets $\mathrm{J}(M) = M$. One calls $\mathrm{J}(M)$ the (*Jacobson*) *radical* of M. Furthermore, let $\mathrm{J}(R)$ be the radical of the regular R-module.

Example II.8.9.

(i) Let M be a semisimple R-module and $M = \bigoplus_{i \in I} S_i$ with simple submodules $S_i \leq M$ $(i \in I)$. For $i \in I$, $M_i := \bigoplus_{j \in I \setminus \{i\}} S_j$ is then a maximal submodule of M, because $M/M_i \simeq S_i$ is simple. This shows

$$\mathrm{J}(M) \subseteq \bigcap_{i \in I} M_i = 0.$$

(ii) Let M be an Artinian R-module with $\mathrm{J}(M) = 0$. Then there already exist finitely many maximal submodules $M_1, \ldots, M_k \leq M$ with $M_1 \cap \ldots \cap M_k = 0$ (otherwise one could construct a descending chain). Since the canonical homomorphism

$$\begin{aligned} M &\to M/M_1 \times \ldots \times M/M_k, \\ m &\mapsto (m + M_1, \ldots, m + M_k) \end{aligned}$$

is injective, M is isomorphic to a submodule of the semisimple module $M/M_1 \times \ldots \times M/M_k$. According to Lemma II.7.10, M itself is semisimple. In general, $\mathrm{J}(M)$ is thus the "smallest" submodule of M such that $M/\mathrm{J}(M)$ is semisimple.

(iii) For every field K and $n \in \mathbb{N}$, $\mathrm{J}(K^{n \times n}) = 0$ according to (i) (cf. Exercise II.3).

(iv) The maximal submodules of $\mathbb{Z}$ have the form $\mathbb{Z}p$ for $p \in \mathbb{P}$. This shows $\mathrm{J}(\mathbb{Z}) = 0$. The only maximal submodule of the $\mathbb{Z}$-module C_4 is C_2, thus $\mathrm{J}(C_4) = C_2$.

Lemma II.8.10 (Nakayama)**.** *Let M be a finitely generated R-module and $N \leq M$ with $M = N + \mathrm{J}(M)$. Then $M = N$. In particular, $\mathrm{J}(M) < M$ if $M \neq 0$.*

Proof. Let $M = Rm_1 + \ldots + Rm_k$. Suppose $N \neq M$. Then $\mathcal{M} := \{L < M : N \leq L\} \neq \varnothing$. Let $\varnothing \neq \mathcal{W} \subseteq \mathcal{M}$ be totally ordered. As usual, $L := \bigcup_{W \in \mathcal{W}} W \leq M$. In the case $L = M$, there exists a $W \in \mathcal{W}$ with $m_1, \ldots, m_k \in W$. Then one obtains the contradiction $M = Rm_1 + \ldots + Rm_k \subseteq W < M$. Thus $L \in \mathcal{M}$ is an upper bound for $\mathcal{W}$. By Zorn, there exists therefore a maximal submodule $S \leq M$ containing N. One obtains the contradiction $M = N + \mathrm{J}(M) \subseteq S < M$. □

Lemma II.8.11. *Let $R \neq \{0\}$ be a ring and let $\mathcal{M}$ be a system of representatives for the isomorphism classes of simple R-modules. Then*

$$\mathrm{J}(R) = \bigcap_{M \in \mathcal{M}} \mathrm{Ann}_R(M).$$

In particular, $\mathrm{J}(R)$ is a proper ideal of R.

Proof. According to Example II.6.15, $\mathcal{M} \neq \varnothing$. For $0 \neq m \in M \in \mathcal{M}$, the map $f\colon R \to M$, $r \to rm$ is an epimorphism. According to the homomorphism theorem, $R/\mathrm{Ker}(f) \simeq M$ is simple and $\mathrm{Ker}(f)$ is a maximal left ideal. Therefore $\mathrm{J}(R) \subseteq \mathrm{Ker}(f)$ and $\mathrm{J}(R)m = 0$. This shows $\mathrm{J}(R) \subseteq \mathrm{Ann}_R(M)$ and

$$\mathrm{J}(R) \subseteq \bigcap_{M \in \mathcal{M}} \mathrm{Ann}_R(M) =: A$$

Conversely, let $N \leq R$ be a maximal left ideal. Then there exists an $M \in \mathcal{M}$ with $R/N \simeq M$. According to Lemma II.7.19, $A \subseteq \mathrm{Ann}_R(M) = \mathrm{Ann}_R(R/N)$. Therefore

$$(A + N)/N \subseteq (AR + N)/N = A(R/N) = 0$$

and $A \subseteq N$. This shows $A \subseteq \mathrm{J}(R)$. As an intersection of ideals, $\mathrm{J}(R) = A \trianglelefteq R$ (Lemma II.7.19). Because of $\mathcal{M} \neq \varnothing$, $\mathrm{J}(R) \neq R$. □

Remark II.8.12. For every semisimple R-module M, $\mathrm{J}(R)M = 0$ according to Lemma II.8.11. For $r + \mathrm{J}(R) = s + \mathrm{J}(R)$ and $m \in M$, it therefore holds that $rm = (r - s + s)m = (r - s)m + sm = sm$. By

$$(r + \mathrm{J}(R))m := rm \qquad (r \in R,\ m \in M)$$

M thus becomes an $R/\mathrm{J}(R)$-module (well-defined). The simple R-modules correspond in this way to the simple $R/\mathrm{J}(R)$-modules. Thus M is also semisimple as an $R/\mathrm{J}(R)$-module. Conversely, every semisimple $R/\mathrm{J}(R)$-module is also semisimple as an R-module.

Lemma II.8.13. *Let R be Artinian and M a finitely generated R-module. Then $R/\mathrm{J}(R)$ is a semisimple ring and $\mathrm{J}(M) = \mathrm{J}(R)M$.*

Proof. Since R is Artinian, the R-module $R/\mathrm{J}(R)$ is also Artinian. According to the correspondence theorem, $\mathrm{J}(R/\mathrm{J}(R)) = 0$. Thus $R/\mathrm{J}(R)$ is a semisimple R-module according to Example II.8.9. According to Remark II.8.12, the regular $R/\mathrm{J}(R)$-module is also semisimple.

According to Lemma II.8.4, M is Artinian with $\mathrm{J}(M/\mathrm{J}(M)) = 0$. According to Example II.8.9, $M/\mathrm{J}(M)$ is semisimple and $\mathrm{J}(R)(M/\mathrm{J}(M)) = 0$. This shows $\mathrm{J}(R)M \subseteq \mathrm{J}(M)$. On the other hand, $M/\mathrm{J}(R)M$ is an $R/\mathrm{J}(R)$-module. Since $R/\mathrm{J}(R)$ is semisimple, $M/\mathrm{J}(R)M$ is also semisimple (Lemma II.8.4). It follows that $\mathrm{J}(M/\mathrm{J}(R)M) = 0$ and $\mathrm{J}(M) \subseteq \mathrm{J}(R)M$. □

Remark II.8.14.

(i) A ring $R \neq \{0\}$ is called *simple*, if 0 and R are the only ideals of R. From Lemma II.8.11 it then follows that $\mathrm{J}(R) = 0$. Unfortunately, not all simple rings are semisimple (Exercise II.48). However, if R is additionally artinian, then R is semisimple according to Lemma II.8.13. By Artin-Wedderburn, R is then isomorphic to a matrix ring over a division ring. Conversely, such matrix rings are always simple (cf. Exercise II.3).

(ii) For $I, J \trianglelefteq R$, according to Exercise I.37,

$$IJ = \Big\{ \sum_{i=1}^{n} x_i y_j : x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J \Big\}$$

is also an ideal of R with $IJ \subseteq I \cap J$. We define $I^0 := R$ and inductively $I^{n+1} := II^n$ for $n \in \mathbb{N}$. Then $R \supseteq I \supseteq I^2 \supseteq \ldots$ holds. If there exists an $n \in \mathbb{N}$ with $I^n = 0$, then I is called *nilpotent*.

Lemma II.8.15. *If R is artinian, then $\mathrm{J}(R)$ is nilpotent and every nilpotent ideal of R lies in $\mathrm{J}(R)$.*

Proof. Since the regular R-module is artinian, the sequence $J := J(R) \supseteq J(R)^2 \supseteq \ldots$ becomes stationary. Let $k \in \mathbb{N}$ such that $J^k = J^{k+1} = \ldots$. Suppose $J^k \neq 0$. Then the set $\mathcal{M}$ of all left ideals $I \leq R$ with $J^k I \neq 0$ is non-empty and thus possesses a minimal element $I \in \mathcal{M}$. In particular, there exists an $x \in I$ with $J^k x \neq 0$. Like J^k, $J^k x$ is also a left ideal and it holds that

$$J^k(J^k x) = J^{2k} x = J^k x \neq 0,$$

i. e. $J^k x \in \mathcal{M}$. Because of $J^k x \subseteq Rx \subseteq I$, it follows that $I = J^k x$ from the minimality of I. Therefore $x = yx$ for some $y \in J^k \subseteq J$. According to Exercise II.46, $1 - y \in R^\times$ and the contradiction $x \in Rx = R(1-y)x = R(x - yx) = 0$ follows. Thus $\mathrm{J}(R)$ is nilpotent.

Conversely, let $I \trianglelefteq R$ be nilpotent. Then $\overline{I} := (I + \mathrm{J}(R))/\mathrm{J}(R)$ is a nilpotent ideal of the semisimple ring $\overline{R} := R/\mathrm{J}(R)$. Let $\overline{R} = Q_1^{n_1 \times n_1} \times \ldots \times Q_k^{n_k \times n_k}$ be the Artin-Wedderburn decomposition. Then the projection of $\overline{I}$ onto $Q_i^{n_i \times n_i}$ is also a nilpotent ideal $\overline{I}_i$. According to Remark II.8.14, $Q_i^{n_i \times n_i}$ is simple and it follows that $\overline{I}_i = 0$ for $i = 1, \ldots, k$. This shows $\overline{I} = 0$ and $I \subseteq \mathrm{J}(R)$. □

Theorem II.8.16 (Hopkins-Levitzki)**.** *Every artinian ring is noetherian.*

Proof. Let R be artinian. By Lemma II.8.15 there exists a $k \in \mathbb{N}$ with $\mathrm{J}(R)^k = 0$. By Lemma II.7.6 the R-modules $J_i := \mathrm{J}(R)^{i-1}/\mathrm{J}(R)^i$ for $i = 1, \ldots, k$ are artinian. It holds that

$$\mathrm{J}(J_i) \overset{\text{II.8.13}}{=} \mathrm{J}(R)\mathrm{J}(R)^{i-1}/\mathrm{J}(R)^i = 0.$$

Now J_i is semisimple by Example II.8.9. From Example II.7.5 it follows that J_i is noetherian. By Lemma II.7.6, since $J_k, J_{k-1}, \ldots, J_1$ are noetherian, so are $\mathrm{J}(R)^{k-1} \simeq J_k$, $\mathrm{J}(R)^{k-2}, \ldots, \mathrm{J}(R)^0 = R$. Thus R is noetherian as a ring. □

Remark II.8.17.

(i) For rings we have shown: semisimple $\Longrightarrow$ artinian $\Longrightarrow$ noetherian. The converses are each false (Example II.8.3).

(ii) In contrast to Lemma II.7.10, a subring of a semisimple ring does not have to be semisimple itself. For example, the ring of upper 2×2 matrices in $K^{2\times 2}$ is not semisimple (Exercise II.37).

(iii) In the following we study the structure of artinian rings R. By Lemma II.8.4, Theorem II.7.8 and Krull-Schmidt, every finitely generated R-module possesses a composition series and a "unique" decomposition into indecomposable modules. By Lemma II.8.13 and Artin-Wedderburn, R is semisimple if and only if $\mathrm{J}(R) = 0$.

Definition II.8.18. Idempotents e, f of a ring R are called *orthogonal*, if $ef = fe = 0$. If $e \neq 0$ possesses no decomposition $e = e_1 + e_2$ with orthogonal idempotents $e_1, e_2 \in R \setminus \{0\}$, then e is called *primitive*. One calls e *centrally primitive*, if $e \in \mathrm{Z}(R)$ and e is primitive in $\mathrm{Z}(R)$.

Example II.8.19.

(i) If $e \in R$ is an idempotent, then so is $1-e$ and e is orthogonal to $1-e$, because $e(1-e) = e-e^2 = e-e = 0 = (1-e)e$.

(ii) If $e, f \in R$ are orthogonal idempotents, then $e+f$ is also an idempotent, because $(e+f)^2 = e^2 + ef + fe + f^2 = e + f$.

(iii) If $e \in R$ is a (primitive) idempotent and $x \in R^\times$, then xex^{-1} is also a (primitive) idempotent.

(iv) Let Q be a division ring and $R := Q^{n\times n}$. The matrices $E_{kk} := (\delta_{ik}\delta_{jk})_{i,j} \in A$ (δ_{is} is the Kronecker delta) with a one at position (k,k) and zeros elsewhere are obviously pairwise orthogonal idempotents with

$$1_n = E_{11} + \ldots + E_{nn}.$$

Lemma II.8.21 will show that 1_n is centrally primitive and E_{kk} is primitive, because R is a simple ring (Remark II.8.14) and $AE_{kk} = Q^{n\times 1}$ is a simple R-module (Example II.8.3).

(v) Let K be a field and $e \in K^{n\times n}$ an idempotent. Then the minimal polynomial of e is a divisor of $X^2 - X$. In particular, e is diagonalizable with eigenvalues $0, 1$ (for example by the Weierstrass normal form, Remark II.10.7). Therefore there exists $x \in \mathrm{GL}(n, K)$ with $xex^{-1} = E_{11} + \ldots + E_{kk}$ for some $0 \leq k \leq n$.

Remark II.8.20. In the following, we call an ideal I of a ring R *indecomposable* if there are no ideals $I_1, I_2 \neq 0$ of R with $I = I_1 \oplus I_2$.

Lemma II.8.21. *For every idempotent e of a ring R, the following holds:*

(i) e is primitive if and only if the R-module Re is indecomposable.

(ii) e is centrally primitive if and only if $e \in \mathrm{Z}(R)$ and the ideal $Re \trianglelefteq R$ is indecomposable.

Proof. Let $e = e_1 + e_2$ with orthogonal idempotents $e_1, e_2 \in R \setminus \{0\}$. Then $Re \subseteq Re_1 + Re_2$ and $Re_i = Re_i^2 = Re_ie \subseteq Re$ for $i = 1, 2$. Because of $e_i = e_i^2 \in Re_i$, we have $Re_i \neq 0$. For $x \in Re_1 \cap Re_2$, it holds that $x = xe_1 = xe_1e_2 = 0$. This shows $R = Re_1 \oplus Re_2$. If additionally $e, e_1, e_2 \in \mathrm{Z}(R)$, then $Re = ReR$ and $Re_i = Re_iR$ are ideals.

Conversely, let $Re = R_1 \oplus R_2$ with non-trivial left ideals I_1, I_2. Then there exist $e_i \in I_i$ with $e = e_1 + e_2$. In the case $e_1 = 0$, we would have $Re = Re_2 \subseteq I_2$. Thus $e_1 \neq 0 \neq e_2$. From $e_1 \in Re$ it follows that $e_1 = e_1e = e_1^2 + e_1e_2$. The unique representation in the direct sum shows $e_1^2 = e_1$ and $e_1e_2 = 0$. Analogously, $e_2^2 = e_2$ and $e_2e_1 = 0$. Thus e_1 and e_2 are orthogonal idempotents and e is not primitive. If $I_1, I_2 \trianglelefteq R$ and $e \in \mathrm{Z}(R)$, then $ae_1 + ae_2 = ae = ea = e_1a + e_2a$ and it follows that $ae_i = e_ia$ for all $a \in R$. This shows $e_1, e_2 \in \mathrm{Z}(R)$ and e is not centrally primitive. □

Theorem II.8.22. *Let R be an Artinian ring. Then there exist pairwise orthogonal primitive idempotents $e_1, \ldots, e_n \in R$ with $1 = e_1 + \ldots + e_n$. If $1 = f_1 + \ldots + f_m$ is also such a decomposition, then $n = m$ and there exists $x \in R^\times$ with $e_i = x f_i x^{-1}$ for $i = 1, \ldots, n$ given a suitable ordering. Furthermore,*

$$R = Re_1 \oplus \ldots \oplus Re_n$$

is a decomposition into indecomposable modules.

Proof. According to Krull-Schmidt, the regular R-module has a decomposition into indecomposable left ideals $R = R_1 \oplus \ldots \oplus R_n$. Let $e_i \in R_i$ with $1 = e_1 + \ldots + e_n$. As in the proof of Lemma II.8.21, one shows that $e_1, \ldots, e_n$ are pairwise orthogonal primitive idempotents. Let $1 = f_1 + \ldots + f_m$ also be such a decomposition. According to Lemma II.8.21, $R = Rf_1 \oplus \ldots \oplus Rf_m$ is a decomposition into indecomposable R-modules. According to Krull-Schmidt, $n = m$ and, given a suitable ordering, there exist isomorphisms $\gamma_i \colon R_i \to Rf_i$. Obviously,

$$\begin{aligned} \gamma &\colon R \to R, \\ a_1 + \ldots + a_n &\mapsto \gamma_1(a_1) + \ldots + \gamma_n(a_n) \qquad (a_i \in R_i) \end{aligned}$$

defines an automorphism of the regular R-module. Let $x := \gamma(1)$ and $y := \gamma^{-1}(1)$. From $xy = \gamma^{-1}(x1) = \gamma^{-1}(\gamma(1)) = 1 = yx$ it follows that $x = y^{-1} \in R^\times$. Because of

$$\begin{aligned} e_1 + \ldots + e_n = 1 = \gamma^{-1}(x) &= \gamma^{-1}(xf_1 1 + \ldots + xf_n 1) \\ &= \underbrace{xf_1\gamma^{-1}(1)}_{\in R_1} + \ldots + \underbrace{xf_n\gamma^{-1}(1)}_{\in R_n} = xf_1x^{-1} + \ldots + xf_nx^{-1} \end{aligned}$$

we have $e_i = x f_i x^{-1}$ for $i = 1, \ldots, n$. □

Remark II.8.23. If $1 = e_1 + \ldots + e_n$ is a decomposition into pairwise orthogonal primitive idempotents, then according to Theorem II.8.22, every primitive idempotent is conjugate to some e_i. However, the e_i can also be conjugate to each other. In $K^{n\times n}$, for example, every primitive idempotent is conjugate to E_{11} (one conjugates with suitable permutation matrices).

Theorem II.8.24 (Peirce)**.** *Let R be Artinian. Then there exist only finitely many central-primitive idempotents $z_1, \ldots, z_k \in \mathrm{Z}(R)$. It holds that $1 = z_1 + \ldots + z_k$ and*

$$R = Rz_1 \oplus \ldots \oplus Rz_k,$$

where $Rz_1, \ldots, Rz_k$ are the indecomposable ideals of R. Furthermore, $Rz_i = z_i R z_i$ is a ring with identity element z_i for $i = 1, \ldots, k$.

Proof. An application of Theorem II.8.22 to $\mathrm{Z}(R)$ yields $1 = z_1 + \ldots + z_k$ with pairwise orthogonal central-primitive idempotents $z_1, \ldots, z_k \in \mathrm{Z}(R)$. Conversely, let $w \in \mathrm{Z}(R)$ be a central-primitive idempotent. Then one can refine $R = Rw \oplus R(1-w)$ to a decomposition into indecomposable modules. According to Lemma II.8.21, one obtains a corresponding decomposition into pairwise orthogonal central-primitive idempotents $1 = w_1 + \ldots + w_k$ with $w = w_1$. According to Theorem II.8.22, there exists $x \in \mathrm{Z}(R)^\times$ with $w = xz_ix^{-1} = z_i$ for some $1 \le i \le k$ (note: $\mathrm{Z}(R)$ is commutative). Thus $z_1, \ldots, z_k$ are the only central-primitive idempotents. According to Lemma II.8.21, $R = Rz_1 \oplus \ldots \oplus Rz_k$ is the only decomposition into indecomposable ideals. The last assertion follows from Exercise II.7. □

Remark II.8.25.

(i) In the situation of Theorem II.8.24, $Rz_1, \ldots, Rz_k$ are called the *blocks* of R. Furthermore, z_i is called the *block idempotent* of Rz_i. If R possesses only one block, then R is called a *block algebra*. The next result reduces the determination of the simple modules of R to block algebras.

(ii) If $R = Q_1^{n_1 \times n_1} \oplus \ldots \oplus Q_k^{n_k \times n_k}$ is semisimple with skew fields $Q_1, \ldots, Q_k$, then $Q_i^{n_i \times n_i}$ are indecomposable (even minimal) ideals of R. The Peirce decomposition thus coincides with the Artin-Wedderburn decomposition.

(iii) The decomposition $1 = z_1 + \ldots + z_k$ into central-primitive idempotents can be refined to a decomposition into pairwise orthogonal primitive idempotents by applying Krull-Schmidt to each block.

Theorem II.8.26. *Let R be Artinian and M an indecomposable R-module. Then there exists exactly one block B of R with $BM \neq 0$. In this case, M is a B-module. Conversely, every B-module is also an R-module. Here, the following hold:*

(i) A B-module M is simple (resp. indecomposable) if and only if M is simple (resp. indecomposable) as an R-module.

(ii) Two B-modules are isomorphic if and only if they are isomorphic as R-modules.

Proof. Let $B_1, \ldots, B_k$ be the blocks of R and $e_1, \ldots, e_k$ the corresponding block idempotents. Then $M = RM = B_1M + \ldots + B_kM$ holds, where $B_1M, \ldots, B_kM$ are submodules of M according to Example II.6.8. Let $b_i \in B_i$ and $m_1, \ldots, m_k \in M$ with $b_1m_1 + \ldots + b_km_k = 0$. Then

$$b_im_i = e_i(b_1m_1 + \ldots + b_km_k) = 0$$

holds for $i = 1, \ldots, k$. Thus $M = B_1M \oplus \ldots \oplus B_kM$. Since M is indecomposable, it follows that $B_iM \neq 0$ and $B_jM = 0$ for one i and all $j \neq i$. For every submodule $N \leq M$, $N = RN = B_iN$ holds. In particular, M is simple (resp. indecomposable) as a B-module if M is simple (resp. indecomposable) as an R-module. Finally, let $f\colon M \to N$ be an isomorphism of R-modules. Then

$$B_iN = B_if(M) = f(B_iM) = f(M) = N$$

holds. Thus M and N are also isomorphic as B-modules.

Conversely, let M be a B_i-module. It is easy to check that M becomes an R-module via $r \cdot m := re_im$ for $r \in R$ and $m \in M$. Of course, the B-submodules of M can also be understood as R-modules. From this, (i) follows. Let $f\colon M \to N$ be an isomorphism of B-modules. For $r \in R$ and $m \in M$, $f(rm) = f(re_im) = re_if(m) = rf(m)$ holds. Therefore, M and N are also isomorphic as R-modules. □

Remark II.8.27. The following results hold for arbitrary rings R. We use the fact that every R-module M is also an $\mathrm{End}_R(M)$-module via $\varphi \cdot m := \varphi(m)$ for $\varphi \in \mathrm{End}_R(M)$ and $m \in M$ (Remark II.6.11).

Lemma II.8.28. *Let S be a simple R-module and $D := \mathrm{End}_R(S)$. Let $T \subseteq S$ be a finite subset and $L := \{r \in R : rT = 0\}$. For $s \in S$ with $Ls = 0$, then $s \in DT$ holds.*

Proof. Induction on $|T|$. In the case $T = \varnothing$, $L = R$ and $s = 0 \in DT$. So let $t \in T$ and assume the statement is already shown for $T' := T \setminus \{t\}$. Let

$$L' := \{r \in R : rT' = 0\}.$$

In the case $L't = 0$, then $L' = L$ and $s \in DT' \subseteq DT$ by induction. So let $L't \neq 0$. Obviously $L't$ is an R-submodule of S and the simplicity of S yields $L't = S$. We consider $f\colon S \to S$, $xt \mapsto xs$ with $x \in L'$. If $x, y \in L'$ with $xt = yt$, then $(x - y)t = 0$, so $x - y \in L$ and it follows that $xs = ys$. Therefore f is well-defined and obviously also R-linear, i. e. $f \in D$. For $x \in L'$ it follows that

$$x(s - f(t)) = xs - xf(t) = xs - f(xt) = 0.$$

Thus $L'(s - f(t)) = 0$ and $s - f(t) \in DT'$ by induction. This shows $s \in DT$. □

Theorem II.8.29 (Jacobson's Density Theorem)**.** *Let S be a simple R-module and $Q := \mathrm{End}_R(S)$. Let $T \subseteq S$ be a finite subset and $f \in \mathrm{End}_Q(S)$. Then there exists an $x \in R$ with $f(t) = xt$ for all $t \in T$.*

Proof. Induction on $|T|$: Wlog. let $T \neq \varnothing$, $s \in T$ and $T' := T \setminus \{s\}$. By induction there exists $x' \in R$ with $f(t) = x't$ for all $t \in T'$. First assume $s = \sum_{t \in T'} \lambda_t t$ with $\lambda_t \in Q$. Then

$$f(s) = \sum_{t \in T'} \lambda_t f(t) = \sum_{t \in T'} \lambda_t x't = \sum_{t \in T'} \lambda_t (x't) = x' \sum_{t \in T'} \lambda_t t = x's.$$

Now let $s \notin DT$ and $L := \{r \in R : rT' = 0\}$. By Lemma II.8.28 we then have $Ls \neq 0$. As usual $Ls = S$ and there exists $r \in L$ with $rs = f(s) - x's$. For $x := x' + r \in R$ and $t \in T$ we now have

$$f(t) = \begin{cases} x't = xt & \text{if } t \neq s, \\ xt & \text{if } t = s. \end{cases}$$

□

Remark II.8.30.

(i) If S in the situation of Theorem II.8.29 is finitely generated as a Q-module, then one can choose a generating system for T. One then obtains $R/\mathrm{Ann}_R(S) \cong \mathrm{End}_Q(S)$. We show in Corollary II.9.13 that $\mathrm{End}_Q(S)$ is a matrix ring over the division ring Q^o. This is a further generalization of Artin-Wedderburn.

(ii) In chapter III.1 we deal with commutative Noetherian rings.

II.9 Modules over Principal Ideal Rings

Definition II.9.1.

(i) A subset S of an R-module M is called (as in Remark II.2.1) *linearly dependent*, if there exist pairwise distinct $s_1, \ldots, s_n \in S$ ($n \in \mathbb{N}$) and $r_1, \ldots, r_n \in R \setminus \{0\}$ with $\sum_{i=1}^{n} r_i s_i = 0$. Otherwise S is called *linearly independent*. One calls M *free*, if M possesses a linearly independent generating system E. If applicable, one calls E a *basis* of M. A free $\mathbb{Z}$-module is called a *free abelian group*.

(ii) For every family of R-modules $(M_i)_{i \in I}$, the *coproduct*

$$\coprod_{i \in I} M_i := \Big\{ (m_i) \in \bigtimes M_i : \big|\{i \in I : m_i \neq 0\}\big| < \infty \Big\}$$

is a submodule of $\bigtimes_{i \in I} M_i$.

Remark II.9.2. If M is a free R-module with basis B, then $M = \bigoplus_{b \in B} Rb$. The map

$$\begin{aligned} \coprod_{b \in B} R &\to M, \\ (r_b)_{b \in B} &\mapsto \sum_{b \in B} r_b b \end{aligned}$$

is then an isomorphism. Therefore every free module is isomorphic to $\coprod_{b \in B} R$ for some set B.

Example II.9.3.

(i) According to Theorem II.2.2, every vector space is a free module.

(ii) The trivial module 0 is free with basis $\varnothing$.

(iii) The regular R-module is free with basis $\{1\}$. More generally, $R^n = \coprod_{i=1}^{n} R$ is also a free R-module with the standard basis $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$.

(iv) A finite abelian group A is free only if $A = 0$, because the free modules $\coprod \mathbb{Z}$ are infinite or trivial.

Theorem II.9.4. *Every R-module is isomorphic to a factor module of a free R-module.*

Proof. Let M be an R-module. Then the map $\coprod_{m \in M} R \to M$, $(r_m)_{m \in M} \mapsto \sum_{m \in M} r_m m$ is an epimorphism. The claim follows from the homomorphism theorem. □

Lemma II.9.5. *Every finitely generated free R-module possesses a finite basis.*

Proof. Let $M = Rm_1 + \ldots + Rm_k$ be a finitely generated free R-module with basis B. Then each m_i can be written as a linear combination of only finitely many $b \in B$. Therefore, there exists a finite subset $C \subseteq B$ with

$$M = Rm_1 + \ldots + Rm_k \subseteq \bigoplus_{c \in C} Rc \subseteq M.$$

Thus C is a finite basis of M. □

Example II.9.6.

(i) The above proof shows that two bases B and C of a free module are either both finite or both infinite. In contrast to vector spaces, however, $|B| \neq |C|$ can hold: Let $S \neq 0$ be an arbitrary ring, $M := \bigtimes_{i \in \mathbb{N}} S$ and $R := \mathrm{End}_S(M)$. Obviously $M \times M \to M$, $((a_i)_i, (b_i)_i) \mapsto (a_1, b_1, a_2, b_2, \ldots)$ is an isomorphism of S-modules. According to Lemma II.7.20, there exists a $\mathbb{Z}$-isomorphism

$$F \colon R \times R \to \mathrm{Hom}_S(M \times M, M) \simeq R, \qquad (\varphi, \psi) \mapsto \varphi\pi_1 + \psi\pi_2,$$

where $\pi_i \colon M \times M \to M$ is the i-th projection. Obviously F is also R-linear. For the regular R-module, it thus holds that $R \simeq R \times R \simeq R^3 \simeq \ldots$, i. e. R possesses bases of every finite cardinality. We show in the following that the situation for skew fields and principal ideal rings is significantly better.

(ii) With a bit more set theory, one can show that any two infinite bases of a free module have the same cardinality.

Theorem II.9.7. *If R is commutative, then any two bases of a free R-module have the same cardinality.*

Proof. Let M be a free R-module with basis B. According to Krull, there exists a maximal ideal $I \trianglelefteq R$. Then $IM \leq M$ and $K := R/I$ is a field according to Theorem I.7.12. By

$$(r + I)(m + IM) := rm + IM$$

the R-module M/IM becomes a K-vector space with generating set $\{b + IM : b \in B\}$. Because of $M = \bigoplus_{b \in B} Rb$, it holds that

$$IM \subseteq \bigoplus_{b \in B} IRb \subseteq \bigoplus_{b \in B} Ib \subseteq IM.$$

For

$$\sum_{b \in B} r_b b + IM = \sum_{b \in B} (r_b + I)(b + IM) = 0 \in M/IM$$

with $r_b \in R$, it follows that $r_b \in I$ for all $b \in B$. Therefore, $\{b + IM : b \in B\}$ is also a K-basis of M/IM. According to Theorem II.2.4, the cardinality of B is uniquely determined. □

Definition II.9.8. Let M be a free module over a commutative ring. The cardinality of a basis of M is then called the *rank* of M and is written as $\mathrm{rk}\, M$ (well-defined according to Theorem II.9.7).

Remark II.9.9. Let R be commutative and M a free R-module with rank $n < \infty$. Then every generating set of M with n elements is already a basis (Theorem II.11.5). On the other hand, not every linearly independent subset of M with n elements is a generating set. For example, $2 \in \mathbb{Z}$ is linearly independent in the regular $\mathbb{Z}$-module.

Theorem II.9.10. *A ring $R \neq \{0\}$ is a skew field if and only if every R-module is free.*

Proof. Let R be a skew field. According to Artin-Wedderburn, R is semisimple. According to Lemma II.8.4, every R-module M is also semisimple. Thus, let $M = \bigoplus_{i \in I} M_i$ with simple R-modules $M_i \leq M$ $(i \in I)$. For $0 \neq m_i \in M_i$, it then holds that $M_i = Rm_i$. Let $r_1, \ldots, r_n \in R$ with

$$\sum_{i=1}^{n} r_i m_i = 0.$$

Then $r_1 m_1 = \ldots = r_n m_n = 0$. In the case $r_i \in R \setminus \{0\} = R^\times$, it would follow that $m_i = r_i^{-1} r_i m_i = 0$. Thus $r_1 = \ldots = r_n = 0$ and $\{m_i : i \in I\}$ is a basis of M.

Conversely, let every R-module be free. According to Example II.6.15, there exists a simple R-module M. Since M is free, $M \simeq \coprod_{b \in B} R$ for a basis B of M. The simplicity of M shows $|B| = 1$ and $M \simeq R$. In particular, the regular R-module is simple. For every $x \in R \setminus \{0\}$, it therefore holds that $Rx = R$, i.e., every non-zero element is left-invertible. Thus $R \setminus \{0\}$ is a group and it follows that $R \setminus \{0\} = R^\times$. Consequently, R is a skew field. □

Theorem II.9.11. *Let R be a skew field and M an R-module. Then the following hold:*

(i) (*Basis Extension Theorem*) *Let $E \subseteq M$ be a generating set of M and $U \subseteq E$ a linearly independent subset. Then M has a basis B with $U \subseteq B \subseteq E$.*

(ii) (*Exchange Theorem*) *For every finite linearly independent subset $U \subseteq M$ and every generating set E of M, it holds that $|U| \leq |E|$.*

(iii) Any two bases of M have the same cardinality.

Proof.

(i) We argue as in Theorem II.2.2. Let $\mathcal{M}$ be the set of all linearly independent subsets $S \subseteq M$ with $U \subseteq S \subseteq E$. Because of $U \in \mathcal{M}$, $\mathcal{M}$ is non-empty and ordered by $\subseteq$. For a totally ordered subset $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$, $\bigcup_{N \in \mathcal{N}} N \in \mathcal{M}$ is an upper bound of $\mathcal{N}$ (for this, it is not yet required that R is a skew field). By Zorn's Lemma, $\mathcal{M}$ possesses a maximal element B. For $e \in E \setminus B$, $B \cup \{e\}$ is linearly dependent. Thus, there exist $r_b \in R$ $(b \in B)$ and $r_e \in R \setminus \{0\} = R^\times$ with $r_e e + \sum_{b \in B} r_b b = 0$. This yields $e = -r_e^{-1} \sum_{b \in B} r b_b \in \langle B \rangle$. Therefore $M = \langle E \rangle \subseteq \langle B \rangle \subseteq M$ and B is a basis of M.

(ii) Let $U = \{u_1, \ldots, u_n\}$ and wlog. $E = \{e_1, \ldots, e_m\}$ (in the case $|E| = \infty$ there is nothing to do). Since U is linearly independent, $0 \neq u_1 = \sum_{i=1}^{m} \lambda_i e_i$ holds, where not all $\lambda_1, \ldots, \lambda_m \in R$ vanish. So let wlog. $\lambda_1 \in R \setminus \{0\} = R^\times$ and therefore

$$e_1 = \lambda_1^{-1} u_1 - \sum_{i=2}^{m} \lambda_1^{-1} \lambda_i e_i \in \langle u_1, e_2, \ldots, e_m \rangle.$$

Consequently, $\{u_1, e_2, \ldots, e_m\}$ is also a generating system with m elements. Because of $u_2 \notin \langle u_1 \rangle$, one can exchange u_2 in the same way for an e_i, say e_2. Repeating this process, one finally obtains the generating system $\{u_1, \ldots, u_n, e_{n+1}, \ldots, e_m\}$. In particular, $|U| = n \leq m = |E|$.

(iii) Here we argue as in Theorem II.2.4. Let B and C be bases of M. For each $b \in B$ there exists a finite subset $C_b \subseteq C$ with $c \in \sum_{c \in C_b} Rc$. Thus

$$M = \sum_{b \in B} Rb = \sum_{b \in B} \sum_{c \in C_b} Rc.$$

Since C is a minimal generating system of M, it follows that $C = \bigcup_{b \in B} C_b$. Let $B_1 \subseteq B$ be a finite subset and $C_1 := \bigcup_{b \in B_1} C_b$. Then B_1 is a linearly independent subset in the module $\langle C_1 \rangle$ and (ii) shows $|B_1| \leq |C_1|$. By the marriage theorem, there exist pairwise distinct $c_b \in C_b$ for $b \in B$. The map $B \to C$, $b \mapsto c_b$ is thus injective. For reasons of symmetry, there must also be an injective map $C \to B$ and the claim follows from Cantor-Bernstein. □

Remark II.9.12. If $R \subseteq S$ is an extension of skew fields, then one can consider S both as a free R-left module and as a free R-right module. Even in this special situation, the corresponding dimensions do not have to be equal. It is even possible that one dimension is finite and the other is infinite.[1]

Corollary II.9.13. *Let R be a ring and S a simple R-module which has dimension $d < \infty$ over the division ring $Q := \mathrm{End}_R(S)$. Then $R/\mathrm{Ann}_R(S) \cong (Q^o)^{d \times d}$.*

Proof. It holds that

$$R/\mathrm{Ann}_R(S) \overset{\text{II.8.30}}{\cong} \mathrm{End}_Q(S) \cong \mathrm{End}_Q(Q^d) \overset{\text{II.7.20}}{\cong} \mathrm{End}_Q(Q)^{d \times d} \overset{\text{II.7.20}}{\cong} (Q^o)^{d \times d}.$$ □

Remark II.9.14. Let R be an integral domain with quotient field Q and $n \in \mathbb{N}$. One can then regard $R^{n \times n}$ as a subring of $Q^{n \times n}$. Therefore, the usual calculation rules for determinants also hold in $R^{n \times n}$. The Leibniz formula for $A = (a_{ij}) \in R^{n \times n}$ shows

$$\det A = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} \in R.$$

We define $\mathrm{GL}(n, R) := (R^{n \times n})^\times$.

Lemma II.9.15. *For every integral domain R and $n \in \mathbb{N}$, it holds that $\mathrm{GL}(n, R) = \{A \in R^{n \times n} : \det A \in R^\times\}$.*

Proof. For $A \in \mathrm{GL}(n, R)$, it holds that $\det(A)\det(A^{-1}) = \det(AA^{-1}) = \det(1_n) = 1 = \det(A^{-1})\det(A)$ and it follows that $\det A \in R^\times$. Conversely, let $A \in R^{n \times n}$ with $\det A \in R^\times$. In linear algebra, one constructs the matrix *complementary* to A

$$\widetilde{A} := \big((-1)^{i+j} \det A_{ji}\big)_{i,j},$$

where A_{ij} is formed from A by deleting the i-th row and j-th column. In particular, $\widetilde{A} \in R^{n \times n}$. Over the quotient field of R, it holds that $A^{-1} = \det(A)^{-1}\widetilde{A} \in R^{n \times n}$. Therefore, $A \in \mathrm{GL}(n, R)$. □

Example II.9.16. According to Lemma II.9.15, it holds that

$$\mathrm{GL}(n, \mathbb{Z}) = \{A \in \mathbb{Z}^{n \times n} : \det A = \pm 1\},$$
$$\mathrm{GL}(n, K[X]) = \{A \in K[X]^{n \times n} : \det A \in K^\times\}.$$

[1] See Section 5.9 in [P. M. Cohn, *Skew fields*, Cambridge University Press, Cambridge, 1997]

Definition II.9.17. Let R be an integral domain and $n, m \in \mathbb{N}$. Matrices $A, B \in R^{n\times m}$ are called *equivalent*, if there exist $S \in \mathrm{GL}(n, R)$ and $T \in \mathrm{GL}(m, R)$ with $A = SBT$. If applicable, we write $A \sim B$.

Remark II.9.18. The equivalence of matrices is an equivalence relation. If R is a field, then two matrices (of the same format) are equivalent if and only if they have the same rank (Gaussian elimination).

Theorem II.9.19 (Smith normal form)**.** *Let R be a principal ideal domain and $A \in R^{n\times m}$. Then A is equivalent to a matrix of the form*

$$\begin{pmatrix} d_1 & & 0 \\ & d_2 & \\ 0 & & \ddots \end{pmatrix}$$

with $d_1 \mid d_2 \mid \ldots$. Here, $d_1, d_2, \ldots$ are uniquely determined up to associates.

Proof.
Existence: In the following, we fix a system of representatives for the classes of associated prime elements of R (Remark II.5.14). For $a \in R \setminus \{0\}$, let $\pi(a)$ be the number of prime factors of a counted with multiplicities ($\pi(a) = 0 \Leftrightarrow a \in R^\times$). Additionally, let $\pi(0) := \infty$. Let

$$\Pi(A) := \min\{\pi(a_{ij}) : 1 \le i \le n, 1 \le j \le m\},$$

where $A = (a_{ij})_{i,j}$. If $\Pi(A) = \infty$, then $A = 0$ and we are finished. So let $\Pi(A) < \infty$. Obviously, permutation matrices over R are invertible (the inverse is the permutation matrix of the inverse permutation). By multiplication with permutation matrices from the left and right, one can permute rows and columns of A without leaving the equivalence class. We can therefore assume $\Pi(A) = \pi(a_{11})$. In the case $a_{11} \nmid a_{12}$, there exist by Bézout elements $x, y \in R$ with $d := \gcd(a_{11}, a_{12}) = a_{11}x + a_{12}y$. Then

$$M := \begin{pmatrix} x & -\frac{a_{12}}{d} & 0 \\ y & \frac{a_{11}}{d} & 0 \\ 0 & 0 & 1_{m-2} \end{pmatrix} \in \mathrm{GL}(m, R)$$

and the first entry of AM is d. By replacing A with AM, we achieve $\Pi(A) \le \pi(d) < \pi(a_{11})$. Because $\Pi(A) \ge 0$, this process can only be repeated finitely many times. In the end, $a_{11} \mid a_{12}$. One proceeds analogously for the other entries in the first row (and first column). Then $a_{11} \mid a_{1i}$ and $a_{11} \mid a_{i1}$ for all i. By multiplication from the left and right with (invertible) elementary matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \lambda & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

one transforms A into the form

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{pmatrix}$$

without leaving the equivalence class. If now $a_{11} \nmid a_{ij}$ for certain $i, j \ge 2$, then add the i-th row to the first (by means of elementary matrix multiplication) and start from the beginning. In doing so, $\Pi(A)$

decreases further. After finitely many steps, $a_{11} \mid a_{ij}$ thus holds for all i, j. Now apply the procedure to the matrix $A' := (a_{ij})_{i,j\geq 2}$. The above elementary transformations will always preserve the property $a_{11} \mid a_{ij}$. In the end, one obtains an equivalent matrix in the desired form.

Uniqueness: Let $D_k(A)$ be the ideal in R generated by all $k\times k$ subdeterminants of A. Let $T \in \mathrm{GL}(m, R)$. The columns of AT are then R-linear combinations of the columns of A. This also holds for $k \times k$ submatrices. From the multilinearity of the determinant, it follows that

$$D_k(A) \supseteq D_k(AT) \supseteq D_k(ATT^{-1}) = D_k(A).$$

Analogously, $D_k(A) = D_k(SA)$ holds for $S \in \mathrm{GL}(n, R)$. This shows $D_k(A) = D_k(\mathrm{diag}(d_1, \ldots))) = (d_1 \ldots d_k)$. Thus $d_1, d_1d_2, \ldots$ are uniquely determined by A up to associates. From this follows the uniqueness of $d_1, d_2, \ldots$ up to associates. □

Definition II.9.20. The elements $d_1, d_2, \ldots$ in Theorem II.9.19 are called *elementary divisors* of A. For $R = \mathbb{Z}$ (or $K[X]$), one can make the Smith normal form completely unique by choosing $d_i \geq 0$ (or d_i monic).

Corollary II.9.21. *Matrices of the same format are equivalent if and only if they have the same elementary divisors (up to associates).*

Proof. Follows from the uniqueness of the Smith normal form. □

Example II.9.22. The Smith normal form is useful for solving integer linear systems of equations: We seek all $x \in \mathbb{Z}^3$ with

$$Ax := \begin{pmatrix} 21 & -5 & 26 \\ 3 & -1 & 4 \\ -8 & 2 & -10 \end{pmatrix} x = \begin{pmatrix} 47 \\ 7 \\ -18 \end{pmatrix} =: b. \tag{II.9.1}$$

The algorithm in the proof of Theorem II.9.19 (with $R = \mathbb{Z}$) yields:

$$\begin{pmatrix} 21 & -5 & 26 \\ 3 & -1 & 4 \\ -8 & 2 & -10 \end{pmatrix} \sim \begin{pmatrix} -1 & 3 & 4 \\ -5 & 21 & 26 \\ 2 & -8 & -10 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 5 & 6 & 6 \\ -2 & -2 & -2 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 6 \\ 0 & -2 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 6 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} =: D.$$

For

$$S := \begin{pmatrix} -5 & -8 & -2 \\ -1 & -1 & 0 \\ 2 & 3 & 1 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{Z}), \qquad T := \begin{pmatrix} -1 & 1 & -2 \\ -1 & 0 & -1 \\ 2 & -2 & 3 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{Z})$$

it holds that $SDT = A$. Therefore (II.9.1) is equivalent to

$$Dy = S^{-1}b = \begin{pmatrix} -3 \\ -4 \\ 0 \end{pmatrix}$$

with $y := Tx$. This shows $y = (-3, -2, a)$ with $a \in \mathbb{Z}$. Thus $x = T^{-1}y = (a - 4, 5 - a, 6 - a)$ for $a \in \mathbb{Z}$.

Remark II.9.23. The next theorem provides an integer version of the (unique) row echelon form of a real matrix.[2]

Theorem II.9.24 (HERMITE normal form)**.** *For every matrix $A \in \mathbb{Z}^{n\times m}$ there exists exactly one non-negative matrix $H \in \mathbb{Z}^{n\times m}$ with the following properties:*

(i) $H = SA$ *for some* $S \in \mathrm{GL}(n,\mathbb{Z})$.

(ii) Every non-zero row of H "starts" with a positive entry, which is called a pivot.

(iii) The pivot of a row is located to the left of the pivot of the following row (if present).

(iv) The entries above a pivot in the same column are smaller than the pivot.

(v) Zero rows are located at the bottom of H. In particular, H is an upper triangular matrix.

Proof. The following algorithm transforms A into a matrix H with the desired properties. We traverse the columns of A from left to right. Wlog. let the first column be non-zero. By multiplication with a permutation matrix from the left, one can achieve that the first entry a_{11} is not 0. By multiplying with $1_n - 2E_{11}$ if necessary, one can assume $a_{11} > 0$. By multiplication with an elementary matrix (in $\mathrm{GL}(n,\mathbb{Z})$), one can, as in the proof of the Smith normal form, replace a_{11} by $\gcd(a_{11}, a_{21})$. Subsequently, one replaces a_{11} by $\gcd(a_{11}, a_{31})$ etc. In the end, $a_{11} = \gcd(a_{11}, \ldots, a_{n1})$. With elementary matrices, one can then realize $a_{21} = \ldots = a_{n1} = 0$.

In the second column, we can analogously achieve $a_{32} = \ldots = a_{n2} = 0$. In the case $a_{22} = 0$, we proceed to the third column. Otherwise, let wlog. $a_{22} > 0$. In the case $a_{12} < 0$ or $a_{12} > a_{22}$, we add or subtract a_{22} from a_{12} by multiplication with an elementary matrix (thereby the first column of A is not changed). By repeating this step sufficiently many times, one obtains $0 \leq a_{12} < a_{22}$. Once all columns have been traversed in this way, A (or H) has the desired properties.

For the uniqueness of H, we can assume that A itself satisfies the properties of H. Let a_i (or s_i) be the i-th column of A (or S). Then $h_i = Sa_i$ is the i-th column of H. Let $e_1, \ldots, e_m$ be the standard basis of $\mathbb{Z}^m$. Let $a_i \in \langle e_1^{\mathrm{t}}, \ldots, e_k^{\mathrm{t}}\rangle$. We show $a_i = h_i$ and $s_k = e_k^{\mathrm{t}}$ by induction on k. In the case $k = 0$, $a_i = 0$ and $h_i = Sa_i = 0$. Now let the claim be already proven up to $k-1$. The first column (from the left) of A that does not lie in $\langle e_1^{\mathrm{t}}, \ldots, e_{k-1}^{\mathrm{t}}\rangle$ has the form $a_i = (a_{1i}, \ldots, a_{ki}, 0, \ldots, 0)^{\mathrm{t}}$ with the pivot $a_{ki} > 0$. By the induction hypothesis, $h_{ji} = a_{ji} + s_{jk}a_{ki}$ for $j < k$ and $h_{ki} = s_{kk}a_{ki}$. Since S is invertible, $s_{kk} \neq 0$ and $h_{ki} \neq 0$ holds. Therefore $h_{ki} > 0$ must be a pivot of H. It follows that $s_{jk}a_{ki} = h_{ji} = 0$ and $s_{ji} = 0$ for $j > k$. From $\det(S) = 1$, it follows that $s_{kk} = 1$ and $h_{ki} = a_{ki}$. For $j < k$, it holds that

$$0 \leq h_{ji} = a_{ji} + s_{jk}a_{ki} < h_{ki} = a_{ki}.$$

From $0 \leq a_{ji} < a_{ki}$, it follows that $s_{jk} = 0$ and $s_k = e_k$. Furthermore, $a_i = h_i$ as claimed. □

Example II.9.25. One can use the Hermite normal form to construct a canonical basis of a free abelian group. For $A := \langle (0,2,6), (3,3,0), (2,2,1)\rangle$ we calculate:

$$\begin{pmatrix} 0 & 2 & 6 \\ 3 & 3 & 0 \\ 2 & 2 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & -1 \\ 0 & 2 & 6 \\ 2 & 2 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & -1 \\ 0 & 2 & 6 \\ 0 & 0 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 2 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Thus $(1,1,2)$, $(0,2,0)$, $(0,0,3)$ is a basis of A. In the following, we construct bases of submodules with respect to a given basis of the module.

[2] See lecture notes Linear Algebra

Theorem II.9.26. *Let R be a principal ideal domain and M a free R-module with $n := \operatorname{rk} M < \infty$. Every submodule $N \leq M$ is then free with $m := \operatorname{rk} N \leq n$. Furthermore, there exists a basis $b_1, \ldots, b_n$ of M and elements $d_1, \ldots, d_m \in R$ with $d_1 \mid d_2 \mid \ldots \mid d_m$, such that $d_1 b_1, \ldots, d_m b_m$ is a basis of N. Here, $d_1, \ldots, d_m$ are uniquely determined up to associates.*

Proof.
Existence: Let $a_1, \ldots, a_n$ initially be any basis of M. According to Example II.8.3, R is Noetherian and therefore also M according to Lemma II.8.4. In particular, N is finitely generated, say by $c_1, \ldots, c_k$. We write $c_i = \sum_{j=1}^{n} x_{ij} a_j$ with $x_{ij} \in R$ for $i = 1, \ldots, k$ and set $A := (x_{ij})_{i,j} \in R^{k \times n}$. According to Theorem II.9.19, there exist $S = (s_{ij})_{i,j} \in \mathrm{GL}(k, R)$ and $T = (t_{ij})_{i,j} \in \mathrm{GL}(n, R)$ with $A = S \operatorname{diag}(d_1, d_2, \ldots) T$ and $d_1 \mid d_2 \mid \ldots$. Let $b_i := \sum_{j=1}^{n} t_{ij} a_j \in M$ for $i = 1, \ldots, n$. As in linear algebra, one shows that $b_1, \ldots, b_n$ is also a basis of M (keyword: basis transformation). Because of

$$c_i = \sum_{j=1}^{n} x_{ij} a_j = \sum_{j=1}^{n} \sum_{l=1}^{k} s_{il} d_l t_{lj} a_j = \sum_{l=1}^{k} s_{il} d_l b_l$$

$\{d_1 b_1, \ldots, d_k b_k\}$ is a generating system of N. From the linear independence of $b_1, \ldots, b_n$ it follows that $d_i b_i = 0 \Leftrightarrow d_i = 0$. Because of $d_1 \mid d_2 \mid \ldots \mid d_k$, the zeros in the sequence $d_1, \ldots, d_k$ are at the end. By deleting these elements, one obtains the generating system $d_1 b_1, \ldots, d_m b_m$ of N. Let $r_1, \ldots, r_m \in R$ with $r_1 d_1 b_1 + \ldots + r_m d_m b_m = 0$. Since $b_1, \ldots, b_m$ are linearly independent, it follows that $r_1 d_1 = \ldots = r_m d_m = 0$. Since R is an integral domain, $r_1 = \ldots = r_m = 0$ holds. Thus $d_1 b_1, \ldots, d_m b_m$ is indeed a basis of N.

Uniqueness: Let $b'_1, \ldots, b'_n$ be another basis of M and $d'_1 \mid d'_2 \mid \ldots \mid d'_m$, such that $d'_1 b'_1, \ldots, d'_m b'_m$ is a basis of N (note Theorem II.9.7). Then there exist $x_{ij}, y_{ij} \in R$ with $b'_i = \sum_{j=1}^{n} x_{ij} b_j$ and $d'_i b'_i = \sum_{j=1}^{m} y_{ij} d_j b_j$ for all i. Since one can conversely express b_i by b'_j, $X := (x_{ij}) \in \mathrm{GL}(n, R)$ and analogously $Y := (y_{ij}) \in \mathrm{GL}(m, R)$. A comparison of coefficients shows $d'_i x_{ij} = y_{ij} d_j$. Therefore

$$\operatorname{diag}(d'_1, \ldots, d'_m) X = Y \operatorname{diag}(d_1, \ldots, d_m).$$

Thus $\operatorname{diag}(d_1, \ldots, d_m)$ and $\operatorname{diag}(d'_1, \ldots, d'_m)$ are equivalent and the claim follows from Corollary II.9.21. □

Remark II.9.27.

(i) With Zorn's Lemma it can be shown that the first part of Theorem II.9.26 also holds in the case $n = \infty$ (see Theorem A.12.1).

(ii) Theorem II.9.26 becomes false if R is not a principal ideal ring: Every ideal I of R is a submodule of the (free) regular R-module. If I is not a principal ideal, then a basis of I must have at least two elements. On the other hand, any two elements $x, y \in I$ are linearly dependent over R because of $yx + (-x)y = 0$. Therefore, only principal ideals can be free.

Definition II.9.28. Let $R \neq \{0\}$ be an integral domain and M an R-module. Then

$$\mathrm{T}(M) := \{m \in M : \exists r \in R \setminus \{0\} : rm = 0\}$$

is called the *torsion module* of M. In the case $\mathrm{T}(M) = 0$, M is called *torsion-free*.

Remark II.9.29. Certainly $0 \in \mathrm{T}(M)$. For $x, y \in \mathrm{T}(M)$ there exist $r, s \in R \setminus \{0\}$ with $rx = sy = 0$. Since R is an integral domain, $rs \neq 0$ and $rs(x-y) = s(rx) - r(sy) = 0$ holds. This shows $x - y \in \mathrm{T}(M)$. For $t \in R$ likewise $r(tx) = t(rx) = 0$ and $tx \in \mathrm{T}(M)$. Therefore $\mathrm{T}(M) \leq M$.

Theorem II.9.30. *Let R be a principal ideal domain and M a finitely generated R-module. Then:*

(i) $M = \mathrm{T}(M) \oplus F$ *for a free R-module F, whose rank is uniquely determined.*

(ii) $\mathrm{T}(M) \simeq R/(d_1) \times \ldots \times R/(d_n)$ *with uniquely determined ideals* $R \neq (d_1) \supseteq (d_2) \supseteq \ldots \supseteq (d_n) \neq (0)$.

(iii) There exist prime elements $p_1, \ldots, p_k \in R$ *and* $a_1, \ldots, a_k \in \mathbb{N}$ *with*

$$\mathrm{T}(M) \simeq R/(p_1^{a_1}) \times \ldots \times R/(p_k^{a_k}).$$

The ideals $(p_1^{a_1}), \ldots, (p_k^{a_k})$ *are uniquely determined up to their order.*

Proof. Let $m_1, \ldots, m_s$ be a generating system of M and L the kernel of the epimorphism $R^s \to M$, $(r_1, \ldots, r_s) \mapsto \sum_{i=1}^s r_i m_i$. According to Theorem II.9.26, there exists a basis $b_1, \ldots, b_s$ of R^s and $d_1, \ldots, d_n \in R \setminus \{0\}$ with $d_1 \mid \ldots \mid d_n$, such that $d_1 b_1, \ldots, d_n b_n$ is a basis of L. The epimorphism

$$R^s \to R/(d_1) \times \ldots \times R/(d_n) \times R^{s-n},$$
$$\sum_{i=1}^s r_i b_i \mapsto (r_1 + (d_1), \ldots, r_n + (d_n), r_{n+1}, \ldots, r_s)$$

then also has kernel L. The isomorphism theorem yields

$$M \simeq R^s/L \simeq R/(d_1) \times \ldots \times R/(d_n) \times R^{s-n}.$$

For $d_i \in R^\times$, we have $R/(d_i) = 0$. By removing these elements, we achieve $R \neq (d_1) \supseteq (d_2) \supseteq \ldots \supseteq (d_n) \neq (0)$. We now identify M with $R/(d_1) \times \ldots \times R/(d_n) \times R^{s-n}$. Apparently, then $\mathrm{T}(M) = R/(d_1) \times \ldots \times R/(d_n)$ and we can choose $F = R^{s-n}$. According to Theorem II.9.7, the rank of $F \simeq M/\mathrm{T}(M)$ is uniquely determined. In the following, we can therefore assume $M = \mathrm{T}(M)$.

To prove the uniqueness in (ii), we first observe

$$\mathrm{Ann}_R(M) = (d_n) =: I.$$

In particular, (d_n) is uniquely determined. So let $n \geq 2$. According to the second isomorphism theorem for rings, $\overline{R} := R/I$ is also a principal ideal domain. By

$$(r + I)m := rm \qquad (r \in R,\ m \in M)$$

M becomes an $\overline{R}$-module (well-defined), which we denote by $\overline{M}$. According to (i), we have

$$\overline{M} = \mathrm{T}(\overline{M}) \oplus \overline{F} = R/(d_1) \times \ldots \times R/(d_l) \times \overline{R}^{n-l} \simeq \overline{R}/((d_1)/I) \times \ldots \times \overline{R}/((d_l)/I) \times \overline{R}^{n-l},$$

where $(d_l) \supsetneq (d_{l+1}) = (d_{l+2}) = \ldots = (d_n)$. Here, $\mathrm{rk}\,\overline{F} = n - l$ is uniquely determined. By induction on n, $(d_1)/I, \ldots, (d_l)/I$ are uniquely determined. Surely then $(d_1), \ldots, (d_n)$ are also uniquely determined.

In (iii), we can assume $M = R/(d)$. Let $d = p_1^{a_1} \ldots p_k^{a_k}$ be the prime factorization of d (Remark II.5.14). For $i \neq j$, we have $(p_i^{a_i}) + (p_j^{a_j}) = (\gcd(p_i^{a_i}, p_j^{a_j})) = R$. The Chinese remainder theorem for rings (Theorem I.7.30) yields an isomorphism

$$M = R/(d) \cong R/(p_1^{a_1}) \times \ldots \times R/(p_k^{a_k}),$$

which is also an isomorphism of R-modules. Since one can recover the elements $d_1, \ldots, d_n$ in (ii) from the prime elements in (iii) up to associates (cf. Exercise I.29), these prime elements are uniquely determined up to order and associates. Therefore, the ideals $(p_1^{a_1}), \ldots, (p_k^{a_k})$ are uniquely determined up to order. □

Remark II.9.31.

(i) According to Theorem II.9.30, finitely generated modules over principal ideal domains are free if and only if they are torsion-free. For infinitely generated modules, this is false (Exercise II.52).

(ii) In the special case $R = \mathbb{Z}$, Theorem II.9.30 is called the *fundamental theorem of finitely generated abelian groups* (cf. Theorem I.5.9 and Exercise I.29). For example,

$$C_2 \times C_6 \times C_{60} \times \mathbb{Z}^5 \cong C_2^2 \times C_3^2 \times C_4 \times C_5 \times \mathbb{Z}^5.$$

Theorem II.9.32. *Let A be a free abelian group with basis $a_1, \ldots, a_n$. Let $B = \langle b_1, \ldots, b_m \rangle \leq A$ and $b_i = \sum_{j=1}^{n} x_{ij} a_j$ for $i = 1, \ldots, m$ and $x_{ij} \in \mathbb{Z}$. The quotient A/B is finite if and only if the matrix $M := (x_{ij})_{i,j} \in \mathbb{Z}^{m \times n}$ has rank n. In the case $m = n$, it then holds that $|A/B| = |\det M|$.*

Proof. After a change of basis as in Theorem II.9.26, we can assume that $d_1 a_1, \ldots, d_k a_k$ is a basis of B for certain $d_1, \ldots, d_k \in R \setminus \{0\}$. Here $k \leq m$ holds and M is equivalent to $D := \operatorname{diag}(d_1, \ldots, d_k, 0, \ldots, 0)$. In particular, M and D have the same rank. As in Theorem II.9.30, it holds that

$$A/B = \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^{n-k}.$$

This shows

$$|A/B| < \infty \iff k = n \iff \operatorname{rk} D = n \iff \operatorname{rk} M = n.$$

If applicable, $|A/B| = |d_1 \ldots d_n| = |\det D| = |\det M|$ according to Example II.9.16. □

II.10 Frobenius Normal Form

Remark II.10.1. In the following, let K be a field and $n \in \mathbb{N}$. We apply the results of the last chapter to the principal ideal domain $K[X]$ in order to construct a normal form of matrices.

Definition II.10.2.

- Matrices $A, B \in K^{n\times n}$ are called *similar*, if there exists an $S \in \mathrm{GL}(n, K)$ with $A = SBS^{-1}$ (linear algebra).
- For $\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X] \setminus K$, one calls

$$B_\alpha := \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{n-2} \\ 0 & & 1 & -a_{n-1} \end{pmatrix} \in K^{n\times n}$$

  the *companion matrix* of α.

Example II.10.3. The companion matrix of X^n is the $n \times n$ Jordan block for the eigenvalue 0.

Lemma II.10.4. *Every $\alpha \in K[X] \setminus K$ is the characteristic polynomial of B_α.*

Proof. Let $\alpha := X^n + a_{n-1}X^{n-1} + \ldots + a_0$. In the case $n = 1$, $X + a_0 = \alpha$ is the characteristic polynomial. Now let $n \geq 2$ and assume the claim has already been proven for $n - 1$. We expand the $\det(X1_m - B_\alpha)$ along the first row

$$\begin{aligned} \det(X1_m - B_\alpha) &= X \begin{vmatrix} X & & & a_1 \\ -1 & \ddots & & \vdots \\ & \ddots & X & a_{n-2} \\ 0 & & -1 & X + a_{n-1} \end{vmatrix} + (-1)^{n-1}a_0 \begin{vmatrix} -1 & X & & 0 \\ & \ddots & \ddots & \\ & & \ddots & X \\ 0 & & & -1 \end{vmatrix} \\ &= X(X^{n-1} + a_{n-1}X^{n-2} + \ldots + a_1) + a_0 = \alpha. \end{aligned}$$

□

Remark II.10.5 (Review Linear Algebra 2)**.** Let $A \in K^{n\times n}$. It is easy to show that the map

$$\begin{aligned} F_A \colon K[X] &\to K^{n\times n}, \\ \alpha = \sum_{k=0}^{\infty} a_k X^k &\mapsto \alpha(A) := \sum_{k=0}^{\infty} a_k A^k \end{aligned}$$

is a ring homomorphism. Because $\dim_K K^{n\times n} = n^2 < \infty = \dim_K K[X]$, F_A is never injective. Since $K[X]$ is a principal ideal domain, there exists exactly one monic polynomial $\mu_A \in K[X]$ with $\mathrm{Ker}(F_A) = (\mu_A)$. One calls μ_A the *minimal polynomial* of A. In contrast to minimal polynomials of algebraic elements, μ_A is often reducible, because $K^{n\times n}$ has zero divisors.

Theorem II.10.6 (FROBENIUS normal form)**.** *For every $A \in K^{n\times n}$ there exist uniquely determined monic polynomials $\alpha_1, \ldots, \alpha_k \in K[X] \setminus K$ with $\alpha_1 \mid \ldots \mid \alpha_k$, such that A is similar to*

$$\begin{pmatrix} B_{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & B_{\alpha_k} \end{pmatrix}.$$

Proof. Let $R := K[X]$. Through the evaluation homomorphism F_A, the $K^{n\times n}$-module $V := K^{n\times 1}$ becomes an R-module with $\alpha v = \alpha(A)v$ for $\alpha \in R$ and $v \in V$ (Example II.6.4(vii)). Because $\dim_K V = n$, V is finitely generated as an R-module. For the minimal polynomial μ of A, it holds that $\mu V = \mu(A)V = 0V = 0$. In particular, $V = \mathrm{T}(V)$. According to Theorem II.9.30, there exist monic polynomials $\alpha_1, \ldots, \alpha_k \in R \setminus K$ with $\alpha_1 \mid \ldots \mid \alpha_k$ and $V \simeq R/(\alpha_1) \times \ldots \times R/(\alpha_k)$. We therefore identify V with $R/(\alpha_1) \times \ldots \times R/(\alpha_k)$. Let $1 \le i \le k$ be fixed and $\alpha_i = X^{d_i} + a_{d_i-1}X^{d_i-1} + \ldots + a_0$. For $j = 0, \ldots, d_i - 1$ let

$$b_{ij} := (0, \ldots, 0, X^j + (\alpha_i), 0, \ldots, 0) \in V.$$

Then $B := \{b_{ij} : 1 \le i \le k,\ 1 \le j \le d_i\}$ is a K-basis of V and it holds that

$$\begin{aligned} Ab_{ij} = Xb_{ij} &= X(0, \ldots, 0, X^j + (\alpha_i), 0, \ldots, 0) = (0, \ldots, 0, X^{j+1} + (\alpha_i), 0, \ldots, 0) \\ &= \begin{cases} b_{i,j+1} & \text{if } j < d_i - 1, \\ -a_0 b_{i,0} - \ldots - a_{d_i-1} b_{i,d_i-1} & \text{if } j = d_i - 1. \end{cases} \end{aligned}$$

Thus A has the specified form with respect to B.

Now let $\beta_1, \ldots, \beta_l \in R \setminus K$ also be monic with $\beta_1 \mid \ldots \mid \beta_l$, such that A is similar to

$$\begin{pmatrix} B_{\beta_1} & & 0 \\ & \ddots & \\ 0 & & B_{\beta_l} \end{pmatrix}.$$

By choosing a suitable K-basis, one obtains a corresponding decomposition $V = V_1 \oplus \ldots \oplus V_l$. Because $XV_i = AV_i \subseteq V_i$, $V_1, \ldots, V_l$ are R-submodules of V. Let $1 \le i \le l$ be fixed and $\beta_i = X^{e_i} + b_{e_i-1}X^{e_i-1} + \ldots + b_0$. Then V_i possesses a basis $c_{i1}, \ldots, c_{i,e_i}$ with

$$Ac_{ij} = \begin{cases} c_{i,j+1} & \text{if } j < e_i - 1, \\ -b_0 c_{i,0} - \ldots - b_{e_i-1} c_{i,e_i-1} & \text{if } j = e_i - 1. \end{cases}$$

One obtains an isomorphism of vector spaces $f\colon V_i \to R/(\beta_i)$ with $f(c_{ij}) = X^j + (\beta_i)$ for $j = 0, \ldots, e_i - 1$. Because $f(Xc_{ij}) = f(Ac_{ij}) = Xf(c_{ij})$, f is also R-linear. This shows $V_i \simeq R/(\beta_i)$ and

$$V \simeq R/(\beta_1) \times \ldots \times R/(\beta_l).$$

From Theorem II.9.30 it follows that $k = l$ and $(\alpha_i) = (\beta_i)$ for $i = 1, \ldots, k$. Since all α_i and β_i are monic, it even holds that $\alpha_i = \beta_i$ for $i = 1, \ldots, k$. □

Remark II.10.7.

(i) One can also prove Theorem II.10.6 using linear algebra (i. e. without modules).[1]

[1] See lecture notes linear algebra.

(ii) In contrast to the Jordan normal form, the Frobenius normal form exists over arbitrary fields and does not change when the field is "enlarged" (due to uniqueness). Furthermore, the matrix blocks in the Frobenius normal form are uniquely sorted.

(iii) The decomposition $V \simeq R/(\alpha_1) \times \ldots \times R/(\alpha_k)$ in the proof above shows $\mathrm{Ann}_{K[X]}(V) = (\alpha_k)$. Thus $\alpha_k(A) = 0$ with $\deg \alpha_k$ minimal, i. e. α_k is the minimal polynomial of A and also of B_{α_k}. In particular, the Frobenius normal form has diagonal shape only if A is a scalar matrix, i. e. $A \in K1_n$. According to Lemma II.10.4, $\chi := \alpha_1 \ldots \alpha_k$ is the characteristic polynomial of A. This yields the theorem of Cayley-Hamilton from linear algebra: $\chi(A) = 0$.

(iv) If the characteristic polynomial χ of $A \in K^{n\times n}$ has pairwise distinct roots in a splitting field, then B_χ is the Frobenius normal form of A.

(v) If one uses part (iii) instead of (ii) in Theorem II.9.30, one obtains the *Weierstraß normal form* of A:

$$\begin{pmatrix} B_{\rho_1^{a_1}} & & 0 \\ & \ddots & \\ 0 & & B_{\rho_s^{a_s}} \end{pmatrix}$$

with irreducible polynomials $\rho_1, \ldots, \rho_s \in K[X]$ and $a_1, \ldots, a_s \in \mathbb{N}$. Here, the powers $\rho_1^{a_1}, \ldots, \rho_s^{a_s}$ are uniquely determined up to their order (they arise from the prime factorization of $\alpha_1, \ldots, \alpha_k$ and therefore depend on K). If A is diagonalizable over K, then the minimal polynomial α_k splits into pairwise distinct linear factors (linear algebra). In this case, $\deg(\rho_1^{a_1}) = \ldots = \deg(\rho_s^{a_s}) = 1$, i. e. the Weierstraß normal form has diagonal shape.

Example II.10.8. The matrix

$$A := \begin{pmatrix} 7 & -1 & -3 \\ 30 & -4 & -15 \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$$

has characteristic polynomial $((X-7)(X+4)+30)(X-1) = (X^2-3X+2)(X-1) = (X-1)^2(X-2)$. Because of

$$(A - 1_2)(A - 2\cdot 1_2) = \begin{pmatrix} 6 & -1 & -3 \\ 30 & -5 & -15 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 5 & -1 & -3 \\ 30 & -6 & -15 \\ 0 & 0 & -1 \end{pmatrix} = 0$$

$\mu = (X-1)(X-2)$ is the minimal polynomial of A. Thus

$$\begin{pmatrix} B_{X-1} & 0 \\ 0 & B_\mu \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix}$$

is the Frobenius normal form of A. The Weierstraß normal form, however, is $\mathrm{diag}(1, 1, 2)$. The following proof shows that one can calculate the Frobenius normal form of any matrix $A \in K^{n\times n}$ via the Smith normal form of $X1_n - A \in K[X]^{n\times n}$.

Theorem II.10.9. *For $A, B \in K^{n\times n}$, the following are equivalent:*

(1) A and B are similar.

(2) A and B have the same Frobenius normal form.

(3) $X1_n - A$ and $X1_n - B$ are equivalent in $K[X]^{n\times n}$.

Proof. The equivalence of (1) and (2) follows from the uniqueness of the Frobenius normal form. For the equivalence to (3), we analyze how the polynomials $\alpha_1, \ldots, \alpha_k$ in Theorem II.10.6 arise. As there, let $R := K[X]$. Let $e_1, \ldots, e_n$ be the standard basis of $V = K^{n\times 1}$ as a K-vector space. Then

$$F\colon R^n \to V,$$
$$(\gamma_1, \ldots, \gamma_n) \mapsto \sum_{i=1}^{n} \gamma_i(A)e_i$$

is an epimorphism of R-modules. Because of $K \subseteq R$, F is also K-linear. In particular, $\mathrm{Ker}(F)$ is a K-vector space. Let $\widetilde{A} := X1_n - A = (\alpha_{ij})_{i,j} \in R^{n\times n}$. For $i = 1, \ldots, n$, it holds that

$$\sum_{j=1}^{n} \alpha_{ji}(A)e_j = (A - a_{ii}1_n)e_i - \sum_{j\neq i} a_{ji}e_j = Ae_i - \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix} = 0.$$

Therefore, the columns $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_n$ of $\widetilde{A}$ lie in $\mathrm{Ker}(F)$. It follows that $L := \sum_{i=1}^{n} R\widetilde{\alpha}_i \subseteq \mathrm{Ker}(F)$. We show that equality holds. As in the proof of Theorem II.9.26, one expresses $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_n$ in terms of the standard basis of R^n. In doing so, one obtains precisely the coefficient matrix $\widetilde{A}$. Now one transforms $\widetilde{A}$ into the Smith normal form

$$\begin{pmatrix} \beta_1 & & 0 \\ & \ddots & \\ 0 & & \beta_n \end{pmatrix}$$

with $\beta_1, \ldots, \beta_n \in R$ and $\beta_1 \mid \ldots \mid \beta_n$. As in the proof of Theorem II.9.30, it then follows that

$$R^n/L \simeq R/(\beta_1) \times \ldots \times R/(\beta_n).$$

Since $\det \widetilde{A}$ is the characteristic polynomial of A, it holds that

$$\begin{aligned} n &= \deg(\det \widetilde{A}) = \deg(\beta_1 \ldots \beta_n) = \deg(\beta_1) + \ldots + \deg(\beta_n) \\ &= \dim_K(R/(\beta_1)) + \ldots + \dim_K(R/(\beta_n)) = \dim_K(R^n/L) \\ &\geq \dim_K(R^n/\mathrm{Ker}(F)) = \dim_K V = n. \end{aligned}$$

This finally shows $L = \mathrm{Ker}(F)$ and

$$V \simeq R^n/L \simeq R/(\beta_1) \times \ldots \times R/(\beta_n).$$

Because of $\mathrm{T}(V) = V$, we have $\beta_1, \ldots, \beta_n \in R \setminus \{0\}$. After normalization, it then holds that $\beta_1 = \ldots = \beta_{n-k} = 1$ and $\beta_{n-k+i} = \alpha_i$ for $i = 1, \ldots, k$ with the α_i from Theorem II.10.6. The Frobenius normal form of A therefore determines the Smith normal form of $\widetilde{A} = X1_n - A$ and vice versa. The equivalence of (2) and (3) now follows from Corollary II.9.21. □

Corollary II.10.10. *Every matrix $A \in K^{n\times n}$ is similar to A^{t}.*

Proof. Let D be the Smith normal form of $X1_n - A$ and $S, T \in \mathrm{GL}(n, K[X])$ with $D = S(X1_n - A)T$. Then

$$T^{\mathrm{t}}(X1_n - A^{\mathrm{t}})S^{\mathrm{t}} = D^{\mathrm{t}} = D = S(X1_n - A)T.$$

Thus $X1_n - A$ and $X1_n - A^{\mathrm{t}}$ are equivalent and the claim follows from Theorem II.10.9.[2] □

[2] See also Exercise II.56

Remark II.10.11. The Frobenius normal form finds application in Galois theory: According to Artin, every Galois extension $K \subseteq L$ possesses a *power basis* $1, x, \ldots, x^d$ for some $x \in L$. The elements $\sigma(x)$ with $\sigma \in G := \mathrm{Gal}(L|K)$ are then pairwise distinct, but not necessarily linearly independent over K. We show that there always exists a *normal basis* of the form $\{\sigma(y) : \sigma \in G\}$ with $y \in L$. This simplifies the calculation of intermediate fields, because for $H \leq G$,

$$\Big\{ \sum_{\tau \in H\sigma} \tau(y) : \sigma \in R \Big\}$$

is a K-basis of L^H, where R is a system of representatives for the right cosets of H in G (note $|L^H : K| = |G : H| = |R|$). This finds application, for example, in cryptography.

Theorem II.10.12 (Normal Basis Theorem)**.** *For every Galois extension $K \subseteq L$, there exists an $a \in L$ such that $\{\Gamma(a) : \Gamma \in \mathrm{Gal}(L|K)\}$ is a K-basis of L.*

Proof. Let $n := |L : K|$ and $G := \mathrm{Gal}(L|K)$.

Case 1: $|K| < \infty$.
Let $p := \operatorname{char} K$. According to Theorem I.11.14, $\mathbb{F}_p \subseteq L$ is a Galois extension and $G \leq \mathrm{Gal}(L|\mathbb{F}_p)$ is cyclic. Let $G = \langle \Gamma \rangle$. Then $\Gamma \in \mathrm{End}_K(L)$ and according to Dedekind, the powers $1, \Gamma, \ldots, \Gamma^{n-1}$ are linearly independent over K. On the other hand, $\Gamma^n - 1 = 0$ in $\mathrm{End}_K(L)$. Thus $X^n - 1$ is the minimal polynomial of Γ. The Frobenius normal form of Γ is therefore

$$B_{X^n-1} = \begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{pmatrix}.$$

In particular, L possesses a K-basis of the form $\{\Gamma^i(a) : i = 0, \ldots, n-1\} = \{\Gamma(a) : \Gamma \in G\}$.

Case 2: $|K| = \infty$.
According to Artin, there exists an $x \in L$ with $L = K(x)$, such that the minimal polynomial $\mu \in K[X]$ of x has pairwise distinct roots $x = x_1, \ldots, x_n \in L$. Let $G = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_n\}$ with $\Gamma_i(x) = x_i$ for $i = 1, \ldots, n$. Let

$$\varphi := \prod_{j=2}^{n} \frac{X - x_j}{x - x_j} \in L[X].$$

For the Lagrange polynomial

$$\alpha := \sum_{i=1}^{n} \Gamma_i(\varphi) = \sum_{i=1}^{n} \prod_{j \neq i} \frac{X - x_j}{x_i - x_j} \in L[X]$$

it holds that $\alpha(x_k) = 1$ for $k = 1, \ldots, n$. According to Example I.8.30, $\alpha = 1$. It follows that

$$\Gamma_i(\varphi)\Gamma_j(\varphi) \equiv \begin{cases} 0 \pmod{\mu} & \text{if } i \neq j. \\ \sum_{k=1}^{n} \Gamma_i(\varphi)\Gamma_k(\varphi) = \Gamma_i(\varphi) \pmod{\mu} & \text{if } i = j. \end{cases} \tag{II.10.1}$$

We now consider the matrix $M := (\Gamma_i\Gamma_j(\varphi))_{i,j=1}^n \in L[X]^{n\times n}$. It holds that

$$M^{\mathrm{t}}M = \Big(\sum_{k=1}^n \Gamma_k\Gamma_i(\varphi)\Gamma_k\Gamma_j(\varphi)\Big)_{i,j} = \Big(\sum_{k=1}^n \Gamma_k(\Gamma_i(\varphi)\Gamma_j(\varphi))\Big)_{i,j}$$
$$\overset{\text{(II.10.1)}}{\equiv} \Big(\delta_{ij}\sum_{k=1}^n \Gamma_k(\Gamma_i(\varphi))\Big)_{i,j} \equiv \Big(\delta_{i,j}\sum_{k=1}^n \Gamma_k(\varphi)\Big)_{i,j} \equiv 1_n \pmod{\mu}.$$

In particular, $(\det M)^2 = \det(M^{\mathrm{t}}M) \equiv 1 \pmod{\mu}$ and $\gamma := \det M \in K[X]\setminus\{0\}$. Since γ has only finitely many roots (Theorem I.8.29), but K is infinitely large, there exists a $y \in K$ with $\gamma(y) \neq 0$. Finally, let $a := \varphi(y)$ and $A := (\Gamma_i\Gamma_j(a))_{i,j} \in L^{n\times n}$. Then

$$\det A = \det(\Gamma_i\Gamma_j(\varphi)(y)) = \gamma(y) \neq 0.$$

Let $\sum_{j=1}^n \lambda_j\Gamma_j(a) = 0$ with $\lambda_1,\ldots,\lambda_n \in K$. Applying Γ_i to both sides, it follows that $\sum_j \lambda_j\Gamma_i\Gamma_j(a) = 0$, i. e. $(\lambda_1,\ldots,\lambda_n)$ is a solution to the system of linear equations $Az = 0$. From $\det A \neq 0$ it follows that $\lambda_1 = \ldots = \lambda_n = 0$. Thus $\{\Gamma_1(a),\ldots,\Gamma_n(a)\}$ is linearly independent and therefore a K-basis of L. □

Example II.10.13.

(i) Obviously $1+\sqrt{2}$, $1-\sqrt{2}$ is a normal basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. In contrast, 1, $\sqrt{2}$ or $\sqrt{2}$, $-\sqrt{2}$ are *not* normal bases.

(ii) We already know that $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is a $\mathbb{Q}$-basis of $L := \mathbb{Q}(\sqrt{2},\sqrt{3})$ (Example I.10.12). From this it follows easily that the four elements $(1\pm\sqrt{2})(1\pm\sqrt{3})$ form a normal basis of L.

II.11 Prime Ideal Decomposition in Dedekind Domains

Remark II.11.1. In this chapter, we generalize algebraic field extensions to commutative rings. Subsequently, we develop an alternative to prime factorization in non-factorial rings.

Definition II.11.2. Let S be a commutative ring with subring R.

- An element $x \in S$ is called *integral* over R if there exists a monic polynomial $\alpha \in R[X]$ with $\alpha(x) = 0$. If all $x \in S$ are integral over R, then $R \subseteq S$ is called an *integral ring extension*.
- For a subset $T \subseteq S$, let $R[T]$ be the intersection of all subrings of S that contain R and T. As always, $R[T]$ is then the "smallest" subring containing R and T. Furthermore, $R[T]$ is the image of the evaluation homomorphism $R[X_t : t \in T] \to S$ (cf. Remark II.3.14). In particular, $R[t] := R[\{t\}] = \sum_{n=0}^{\infty} Rt^n$.

Example II.11.3.

(i) Every $x \in R$ is integral over R as a root of $X - x$.

(ii) If R is a field, then $x \in S$ is integral if and only if x is algebraic over R, because the minimal polynomial of x is always monic.

(iii) For $R = \mathbb{Z}$ and $S = \mathbb{C}$, the integral elements are also called *algebraic integers*. For example, i and $\sqrt[3]{2}$ are algebraic integers. According to Remark I.8.53, all rational algebraic integers are already integers.

Remark II.11.4. We had already seen in Remark II.9.14 that the rules for determinants from linear algebra also hold in arbitrary integral domains (by embedding into the quotient field). Now let R be an arbitrary commutative ring. Then the polynomial ring

$$\widehat{R} := \mathbb{Z}[X_r : r \in R]$$

is an integral domain and the evaluation homomorphism $F\colon \widehat{R} \to R$, $X_r \mapsto r$ is surjective. Componentwise, F extends to a ring epimorphism $F\colon \widehat{R}^{n\times n} \to R^{n\times n}$. Thus, the calculation rules transfer from $\widehat{R}^{n\times n}$ to $R^{n\times n}$. For example, let $A \in R^{n\times n}$ and $\widehat{A} \in \widehat{R}^{n\times n}$ be a preimage of A under F. Let $C \in \widehat{R}^{n\times n}$ be the adjugate matrix to $\widehat{A}$ and $\widetilde{A} := F(C)$. Then it holds that

$$\widetilde{A}A = F(C)F(\widehat{A}) = F(C\widehat{A}) = F(\det(\widehat{A})1_n) = \det(F(\widehat{A}))1_n = \det(A)1_n.$$

As a first application, we prove a theorem about bases in free modules.

Theorem II.11.5. *Let R be a commutative ring and M a free R-module with rank $n < \infty$. Then every generating set of M with n elements is a basis of M.*

Proof. Wlog. let $M = R^n$ and $E \subseteq M$ be a generating set with $|E| = n$. We must show that E is linearly independent. Let $A \in R^{n\times n}$ be the matrix whose columns are formed from E. Since E is a generating set, there exists a $B \in R^{n\times n}$ with $AB = 1_n$. Applying the determinant yields $\det(A) \in R^\times$. For the adjugate matrix $\widetilde{A}$ to A, it holds that $\det(A)^{-1}\widetilde{A}A = 1_n$. For $v \in R^n \setminus \{0\}$, it therefore holds that $Av \neq 0$. The claim follows. □

Lemma II.11.6. *For every commutative ring S with subring R and $x \in S$, the following statements are equivalent:*

(1) x is integral over R.

(2) $R[x]$ is a finitely generated R-module.

(3) There exists a finitely generated R-submodule M of S with $1 \in M$ and $xM \subseteq M$.

Proof.

(1) ⇒ (2): By assumption, there exist $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in R$ with $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. In particular,

$$\begin{aligned} x^n &= -a_{n-1}x^{n-1} - \ldots - a_0 \in R + Rx + \ldots + Rx^{n-1} =: M, \\ x^{n+1} &= -a_{n-1}x^n - \ldots - a_0 x \in M, \\ &\vdots \end{aligned}$$

This shows $R[x] = \sum_{k=0}^{\infty} Rx^k = M$.

(2) ⇒ (3): Choose $M := R[x]$.

(3) ⇒ (1): Let $M = Rs_1 + \ldots + Rs_n$ with $s_1, \ldots, s_n \in S \setminus \{0\}$. Because of $xM \subseteq M$, there exist $a_{ij} \in R$ with $xs_i = \sum_{j=1}^n a_{ij}s_j$ for $i = 1, \ldots, n$. For $A := (a_{ij})_{i,j} \in R^{n\times n}$ and $v := (s_1, \ldots, s_n) \in S^n$, it holds that

$$Av = \Big(\sum_{j=1}^n a_{ij}s_j\Big)_{i=1}^n = xv.$$

Let $B := x1_n - A \in S^{n\times n}$ and $\widetilde{B} \in S^{n\times n}$ with $\widetilde{B}B = \det(B)1_n$ as in Remark II.11.4. Then $\det(B)v = \widetilde{B}Bv = \widetilde{B}0 = 0$, thus $\det(B)s_i = 0$ for $i = 1, \ldots, n$. Because of $1 \in M$, it follows that $\det(B) = \det(B)1 = 0$. Finally, $\det(B) = \det(x1_n - A)$ is a monic polynomial in x (of degree n) with coefficients in R. Thus x is integral over R. □

Example II.11.7. Let $R \subseteq S$ be a ring extension such that S is finitely generated as an R-module. Then $R \subseteq S$ is integral according to Lemma II.11.6 with $M = S$.

Theorem II.11.8. *Let S be a commutative ring with subring R. Then the elements in S that are integral over R form a subring T of S with $R \subseteq T$. Furthermore, every element of S that is integral over T already lies in T.*

Proof. According to Example II.11.3, $R \subseteq T$. Now let $a, b \in T$. By Lemma II.11.6, there exist finitely generated R-modules $M, N \subseteq S$ with $1 \in M \cap N$, $aM \subseteq M$ and $bN \subseteq N$. We write $M = Rx_1 + \ldots + Rx_m$ and $N = Ry_1 + \ldots + Ry_n$. Then $L := MN = \sum_{i,j} Rx_iy_j$ is also a finitely generated R-module with $1 \in L$, $(a-b)L \subseteq aMN + bNM \subseteq MN = L$ and $abL \subseteq aMbN \subseteq MN = L$. By Lemma II.11.6, it follows that $a - b, ab \in T$ and T is a subring of S.

Now let $x \in S$ be integral over T. Then there exist $a_0, \ldots, a_{n-1} \in T$ with $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. Consequently, x is also integral over $R[a_0, \ldots, a_{n-1}]$. By Lemma II.11.6, there exist $k_0, \ldots, k_n \in \mathbb{N}$ with $R[a_0] = R + Ra_0 + \ldots + Ra_0^{k_0}$, $R[a_0, a_1] = R[a_0] + R[a_0]a_1 + \ldots + R[a_0]a_1^{k_1}$, $\ldots$,

$$R[a_0, \ldots, a_{n-1}, x] = \sum_{i_0=0}^{k_0} \ldots \sum_{i_n=0}^{k_n} Ra_0^{i_0} \ldots a_{n-1}^{i_{n-1}} x^{i_n}.$$

Therefore $M := R[a_0, \ldots, a_{n-1}, x]$ is a finitely generated R-module with $1 \in M$ and $xM \subseteq M$. By Lemma II.11.6, x is integral over R, i. e. $x \in T$. □

Definition II.11.9. In the situation of Theorem II.11.8, T is called the *integral closure* of R in S. In the case $T = R$, R is called *integrally closed* in S. An integral domain R is called *integrally closed* if it is integrally closed in its field of fractions.

Example II.11.10. According to Example II.11.3, $\mathbb{Z}$ is integrally closed. We generalize this.

Theorem II.11.11. *Every factorial ring is integrally closed.*

Proof. Let R be factorial with field of fractions Q. Let $x \in Q$ be integral over R. Then there exist coprime $a, b \in R$ with $x = \frac{a}{b}$. Furthermore, there exist $a_0, \ldots, a_{n-1} \in R$ with $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. Multiplication by b^n yields

$$a^n + a_{n-1}ba^{n-1} + \ldots + a_0 b^n = 0.$$

This shows $b \mid a^n$. Because $\gcd(a, b) = 1$, $b \in R^\times$ and $x = ab^{-1} \in R$. □

Remark II.11.12. The integral closure of $\mathbb{Z}$ in a number field K is called the *ring of integers*[1] of K and is usually denoted by $\mathbb{Z}_K$. Every quadratic number field K is known to have the form $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Q}$ (see proof of Theorem I.12.23). Because $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(e^2\sqrt{d}) = \mathbb{Q}(\sqrt{de})$ for $e \in \mathbb{Z}$, we can assume that d is a square-free integer and $0 \neq d \neq 1$.

Theorem II.11.13. *Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be square-free and $K = \mathbb{Q}(\sqrt{d})$. Then*

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4, \\ \mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{otherwise.} \end{cases}$$

Proof. Since $\sqrt{d}$ is algebraic-integral as a root of $X^2 - d$, $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Z}_K$ holds in any case according to Theorem II.11.8. In the case $d \equiv 1 \pmod 4$, $X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X]$ with root $\omega := \frac{1+\sqrt{d}}{2}$. Then $\mathbb{Z}[\omega] \subseteq \mathbb{Z}_K$ also holds.

Conversely, let $x \in \mathbb{Z}_K$. Then there exist $a, b \in \mathbb{Q}$ such that $x = a + b\sqrt{d}$. Let $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ with $\sigma(\sqrt{d}) = -\sqrt{d}$. Along with x, $\sigma(x)$ is also algebraic-integral (root of the same integer polynomial). Therefore $x + \sigma(x) = 2a \in \mathbb{Q}$ is algebraic-integral, hence $2a \in \mathbb{Z}$. Analogously, $x\sigma(x) = a^2 - b^2 d \in \mathbb{Q} \cap \mathbb{Z}_K = \mathbb{Z}$. Because $(2b)^2 d = (2a)^2 - 4(a^2 - b^2 d) \in \mathbb{Z}$, it follows that $2b \in \mathbb{Z}$, since d is square-free. For $\widetilde{a} := 2a$ and $\widetilde{b} := 2b$, we have

$$\frac{\widetilde{a}^2 - \widetilde{b}^2 d}{4} = a^2 - b^2 d \in \mathbb{Z}.$$

[1] or *maximal order*

This shows $\widetilde{a}^2 \equiv \widetilde{b}^2 d \pmod 4$, where $d \not\equiv 0 \pmod 4$. Therefore $\widetilde{a}$ is even if and only if $\widetilde{b}$ is even. If applicable, $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. In the case $\widetilde{a} \equiv \widetilde{b} \equiv 1 \pmod 2$, we have $1 \equiv \widetilde{a}^2 \equiv \widetilde{b}^2 d \equiv d \pmod 4$. Then

$$x = \frac{\widetilde{a} + \widetilde{b}\sqrt{d}}{2} = \frac{\widetilde{a} - \widetilde{b}}{2} + \widetilde{b}\frac{1 + \sqrt{d}}{2} \in \mathbb{Z}[\omega]. \qquad \square$$

Remark II.11.14.

(i) We had already seen in Example II.5.31 and Exercise II.29 that the rings of integers of $K := \mathbb{Q}(\sqrt{d})$ for $d \in \{-3, -2, -1, 2, 3\}$ are Euclidean, but for $d = -5$ they are not. It is conjectured that $\mathbb{Z}_K$ is Euclidean for infinitely many positive d. For negative d, however, $\mathbb{Z}_K$ is Euclidean if and only if $-d \in \{1, 2, 3, 7, 11\}$ (without proof). More generally, Heegner showed that for negative d, $\mathbb{Z}_K$ is a principal ideal domain if and only if $-d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ (*Heegner numbers*). This can be used to explain why

$$e^{\pi\sqrt{163}} = 262537412640768743{,}99999999999925\ldots$$

is almost an integer (without proof).

(ii) The rings of integers of $K := \mathbb{Q}(\sqrt{-2})$ and $L := \mathbb{Q}(\sqrt{-7})$ are Euclidean according to (i). Let P_K and P_L be systems of representatives for the non-associated prime elements in $\mathbb{Z}_K$ and $\mathbb{Z}_L$, respectively. One easily shows $\mathbb{Z}_K^\times = \{\pm 1\} = \mathbb{Z}_L^\times$. Therefore, the map $K^\times \to L^\times$, $\pm\prod_{p\in P_K} p^{a_p} \mapsto \pm\prod_{p\in P_L} p^{a_p}$ is an isomorphism. Obviously, $(K, +) \cong \mathbb{Q}^2 \cong (L, +)$ also holds. On the other hand, according to Exercise I.67, $K \ncong L$.

Theorem II.11.15. *Let R be an integral domain with quotient field Q. Let $Q \subseteq K$ be a finite field extension and S the integral closure of R in K. For every $x \in K$, there then exists an $r \in R \setminus \{0\}$ with $rx \in S$. In particular, K is isomorphic to the quotient field of S.*

Proof. Let $\mu = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in Q[X]$ be the minimal polynomial of x over Q. Then there exists an $r \in R \setminus \{0\}$ with $ra_i \in R$ for $i = 0, \ldots, n-1$. Consequently, rx is integral over R as a root of the monic polynomial $X^n + a_{n-1}rX^{n-1} + \ldots + a_0 r^n \in R[X]$. Thus $rx \in S$. According to the universal property of the quotient field (Exercise I.40), the inclusion map $S \hookrightarrow K$ can be extended to a field homomorphism $\sigma\colon Q(S) \to K$. With the above notation, $\sigma(rx/r) = x$ then holds. Thus σ is surjective and therefore an isomorphism. $\square$

Theorem II.11.16. *The ring of integers of a number field K is a free abelian group of rank $|K : \mathbb{Q}|$.*

Proof. Let $x \in K$ be a primitive element ($K = \mathbb{Q}(x)$). According to Theorem II.11.15 (with $R = \mathbb{Z}$), there exists an $a \in \mathbb{Z} \setminus \{0\}$ with $ax \in \mathbb{Z}_K$. Because of $\mathbb{Q}(x) = \mathbb{Q}(ax)$, we can assume $x \in \mathbb{Z}_K$. Let $\alpha \in \mathbb{Z}[X]$ be monic with root x. Then the minimal polynomial $\mu \in \mathbb{Q}[X]$ is a divisor of α. From Corollary I.8.51 it follows that $\mu \in \mathbb{Z}[X]$. Therefore, all roots $x = x_0, \ldots, x_{n-1}$ of μ in a splitting field are algebraic integers. Because of $|K : \mathbb{Q}| = |\mathbb{Q}(x) : \mathbb{Q}| = \deg \mu = n$, $1, x, \ldots, x^{n-1}$ is a $\mathbb{Q}$-basis of K. For $z \in \mathbb{Z}_K$, there therefore exist $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ with

$$z = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}.$$

Let $\mathrm{Gal}(\mu) = \{\sigma_0, \ldots, \sigma_{n-1}\}$ with $\sigma_i(x) = x_i$ for $i = 0, \ldots, n-1$. With z, $z_i := \sigma_i(z) = a_0 + a_1 x_i + \ldots + a_{n-1}x_i^{n-1}$ is then also an algebraic integer (root of the same polynomial). This yields a system of equations

$Av = w$, where $A := (x_i^j)_{i,j=0}^{n-1} \in \mathbb{Z}_K^{n\times n}$, $v := (a_0, \ldots, a_{n-1}) \in \mathbb{Q}^n$ and $w := (z_0, \ldots, z_{n-1}) \in \mathbb{Z}_K^n$. Since A is a Vandermonde matrix,

$$d := \det A = \prod_{i<j}(x_j - x_i) \in \mathbb{Z}_K \setminus \{0\}$$

holds (linear algebra). Furthermore, $d^2 = D_\mu \in \mathbb{Q}$ (discriminant). Multiplication with the complementary matrix $\widetilde{A} \in \mathbb{Z}_K^{n\times n}$ yields $dv = \widetilde{A}Av = \widetilde{A}w$ and

$$d^2 v = d\widetilde{A}w \in \mathbb{Q}^n \cap \mathbb{Z}_K^n = \mathbb{Z}^n.$$

This shows

$$z = a_0 + \ldots + a_{n-1}x^{n-1} \in \mathbb{Z}\frac{1}{d^2} + \mathbb{Z}\frac{x}{d^2} + \ldots + \mathbb{Z}\frac{x^{n-1}}{d^2} =: M.$$

Obviously, M is a free abelian group with basis $1/d^2, \ldots, x^{n-1}/d^2$. According to Theorem II.9.26, $\mathbb{Z}_K$ is also a free abelian group of rank at most n. Conversely, $\mathbb{Z}_K$ contains the free abelian group $\mathbb{Z}[x]$ of rank n. Therefore, $\mathbb{Z}_K$ also has rank $n = |K : \mathbb{Q}|$. □

Remark II.11.17. A $\mathbb{Z}$-basis of $\mathbb{Z}_K$ for a number field K is called an *integral basis* of K. For quadratic number fields, we determined integral bases in Theorem II.11.13 ($1, \sqrt{d}$ or $1, \frac{1+\sqrt{d}}{2}$). For the n-th cyclotomic field $\mathbb{Q}_n$, $1, \zeta, \ldots, \zeta^{\varphi(n)-1}$ is an integral basis, where ζ is a primitive n-th root of unity (Theorem A.3.17). In general, however, not every ring of integers possesses a basis consisting of powers of one element (i. e. there are no primitive elements for rings of integers).

Theorem II.11.18. *Let $R \subseteq S$ be an integral ring extension and $P \subsetneq Q$ prime ideals in S. Then $P \cap R \subsetneq Q \cap R$ are prime ideals in R.*

Proof. Obviously $P \cap R$ and $Q \cap R$ are prime ideals in R. Let us assume $Q \cap R \subseteq P$. Let $x \in Q \setminus P$. Since x is integral over R, there exist $a_0, \ldots, a_{n-1} \in R$ with $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$. In the case $a_i \in P$ for all i, we would have $x^n \in P$ and therefore also $x \in P$. Thus there exists an $i \in \{0, \ldots, n-1\}$ with $a_i \notin P$ and $a_0, \ldots, a_{i-1} \in P$. Then

$$x^i(x^{n-i} + \ldots + a_i) = -(a_{i-1}x^{i-1} + \ldots + a_1 x + a_0) \in P$$

and $x^{n-i} + \ldots + a_i \in P \subseteq Q$. Because of $x^{n-i} + \ldots + a_{i+1}x \in Q$, the contradiction $a_i \in Q \cap R \subseteq P$ follows. Thus $P \cap R \subsetneq Q \cap R$. □

Definition II.11.19. Let R be an integral domain with quotient field $Q(R)$. A *fractional ideal* of R is an R-submodule $I \neq 0$ of $Q(R)$ with $rI \subseteq R$ for some $r \in R \setminus \{0\}$.

Example II.11.20. Obviously every non-trivial ideal of R is a fractional ideal. On the other hand, $\mathbb{Z}\frac{1}{2}$ is a fractional ideal of $\mathbb{Z}$, but not an ideal. For fractional ideals I, J, one defines IJ (as for ideals) as the R-span of $\{xy : x \in I, y \in J\}$.

Lemma II.11.21. *For every integral domain R, the following holds:*

(i) Every non-trivial finitely generated R-submodule of $Q(R)$ is a fractional ideal. In particular, Rx for $x \in Q(R)^\times$ is a fractional principal ideal.

(ii) If I and J are fractional ideals of R, then so are $I + J$, IJ and $I \cap J$.

(iii) For every fractional ideal I of R, $I^{-1} := \{x \in Q(R) : xI \subseteq R\}$ is also a fractional ideal of R.

(iv) If I, J are fractional ideals with $IJ = R$, then $J = I^{-1}$.

Proof.

(i) Let $I = R\frac{r_1}{s_1} + \ldots + R\frac{r_n}{s_n} \subseteq Q(R)$ with $r_1, \ldots, r_n, s_1, \ldots, s_n \in R$. Then $(s_1 \ldots s_n)I \subseteq R$.

(ii) By definition, $IJ \subseteq I \cap J \subseteq I + J$ are non-trivial R-modules. Let $r, s \in R$ with $rI, sI \subseteq R$. Then $rsIJ \subseteq rs(I \cap J) \subseteq rs(I + J) \subseteq s(rI) + r(sI) \subseteq R$.

(iii) Let $r \in R \setminus \{0\}$ with $rI \subseteq R$. Then $r \in I^{-1} \neq 0$. Obviously, I^{-1} is an R-module and $xI^{-1} \subseteq R$ for $x \in I \setminus \{0\}$.

(iv) Obviously, $J \subseteq I^{-1} = I^{-1}IJ \subseteq J$. □

Definition II.11.22. An integrally closed, Noetherian integral domain R is called a *Dedekind domain*, if every non-trivial prime ideal of R is maximal.

Theorem II.11.23. *Every principal ideal domain is a Dedekind domain.*

Proof. According to Theorem II.5.19, every principal ideal domain R is factorial and therefore integrally closed according to Theorem II.11.11. Obviously, R is also Noetherian. According to Lemma II.5.18, the non-trivial prime ideals are maximal. □

Example II.11.24. Not every factorial ring is a Dedekind domain. For example, the prime ideal (X) in $\mathbb{Z}[X]$ is not maximal. However, we show in Corollary II.11.37 that Dedekind domains are not far removed from principal ideal domains.

Theorem II.11.25. *The ring of integers $\mathbb{Z}_K$ of every number field K is a Dedekind domain.*

Proof. According to Theorem II.11.15 with $R = \mathbb{Z}$, $\mathbb{Z}_K$ is an integrally closed integral domain with $Q(\mathbb{Z}_K) = K$. According to Theorem II.11.16, $\mathbb{Z}_K$ is a free abelian group with rank $|K : \mathbb{Q}| < \infty$. According to Theorem II.9.26, every ideal (even every subgroup) of $\mathbb{Z}_K$ is finitely generated as a $\mathbb{Z}$-module and therefore also as an R-module. Thus R is Noetherian. Let $P, Q \trianglelefteq \mathbb{Z}_K$ be prime ideals with $(0) \subsetneq P \subseteq Q$. According to Theorem II.11.18, $(0) \subsetneq P \cap \mathbb{Z} \subseteq Q \cap \mathbb{Z}$ are prime ideals in $\mathbb{Z}$. This shows $P \cap \mathbb{Z} = Q \cap \mathbb{Z}$ and $P = Q$. Thus every non-trivial prime ideal of $\mathbb{Z}_K$ is maximal. □

Definition II.11.26. A fractional ideal I of R is called *invertible*, if $II^{-1} = R$.

Lemma II.11.27. *Let R be a Dedekind domain and $0 \neq I \lhd R$. Then there exist prime ideals $P_1, \ldots, P_n \trianglelefteq R$ with $P_1 \ldots P_n \subseteq I \subseteq P_1 \cap \ldots \cap P_n$.*

Proof. Let $I \lhd R$ be a maximal counterexample (exists because R is Noetherian). Then I is not a prime ideal. Thus there exist $J_1, J_2 \trianglelefteq R$ with $J_1J_2 \subseteq I$, but $J_1, J_2 \nsubseteq I$. Because of

$$(I + J_1)(I + J_2) \subseteq I + J_1J_2 = I \subseteq (I + J_1) \cap (I + J_2)$$

we have $I + J_1 \neq R \neq I + J_2$. Consequently, the statement holds for $I + J_1$ and $I + J_2$ and thus also for I. Contradiction. □

Lemma II.11.28. *In every Dedekind domain, the non-trivial prime ideals are invertible.*

Proof. Let $0 \neq P \trianglelefteq R$ be a prime ideal and $a \in P \setminus \{0\}$. According to Lemma II.11.27, there exist non-trivial prime ideals $P_1, \ldots, P_n \trianglelefteq R$ with $P_1 \ldots P_n \subseteq (a) \subseteq P$. Let n be chosen minimally. From the prime ideal property, it follows that $P_i \subseteq P$ for some $i \in \{1, \ldots, n\}$; wlog. $i = 1$. Since every non-trivial prime ideal is maximal in R, it holds that $P = P_1$. Because $P_2 \ldots P_n \nsubseteq (a)$, there exists a $b \in P_2 \ldots P_n \setminus (a)$ (in the case $n = 1$, let $b \in R \setminus (a)$). Then $Pb = P_1 b \subseteq P_1 \ldots P_n \subseteq (a)$ and $a^{-1}bP \subseteq R$, thus $x := a^{-1}b \in P^{-1}$. In the case $x \in R$, it would follow that $b \in x(a) \subseteq (a)$.

Because $P \subseteq R$, we have $1 \in P^{-1}$ and $P \subseteq PP^{-1} \trianglelefteq R$. Since P is maximal, we can assume $PP^{-1} = P$. It follows that $PP^{-n} = P$ and $ax^n \in P \subseteq R$ for $n \geq 0$. Thus $aR[x] \trianglelefteq R$. Since R is Noetherian, there exist $a_1, \ldots, a_k \in R$ with $aR[x] = Ra_1 + \ldots + Ra_k$. Then $R[x] = R\frac{a_1}{a} + \ldots + R\frac{a_n}{a}$ is also a finitely generated R-module. According to Lemma II.11.6, x is integral over R and one obtains the contradiction $x \in R$, since R is integrally closed. □

Theorem II.11.29 (Prime ideal factorization)**.** *Every non-trivial ideal of a Dedekind domain is a product of* (*up to the order*) *uniquely determined prime ideals.*

Proof. Let R be a Dedekind domain and $0 \neq I \trianglelefteq R$. In the case $I = R$, I is the empty product of prime ideals. So let $I \neq R$. According to Lemma II.11.27, there are non-trivial prime ideals $P_1, \ldots, P_n$ with $P_1 \ldots P_n \subseteq I$. Let n be minimal. In the case $n = 1$, $I = P_1$ because P_1 is maximal. So let $n \geq 2$. Let M be a maximal ideal with $I \subseteq M$. As usual, $P_i \subseteq M$ for some $i \in \{1, \ldots, n\}$; say $i = 1$. Then even $P_1 = M$ holds and

$$P_2 \ldots P_n = M^{-1}P_1 \ldots P_n \subseteq M^{-1}I \subseteq M^{-1}M = R$$

according to Lemma II.11.28. By induction on n, $M^{-1}I$ is a product of prime ideals, thus also $M(M^{-1}I) = I$.

Now let $P_1 \ldots P_n = Q_1 \ldots Q_m$ with non-trivial prime ideals $P_1, \ldots, P_n, Q_1, \ldots, Q_m \trianglelefteq R$. Then $Q_1 \ldots Q_m \subseteq P_1$, so $Q_i \subseteq P_1$ for some $i \in \{1, \ldots, m\}$. Wlog. let $i = 1$. From the maximality of Q_1, it follows that $Q_1 = P_1$ and $Q_2 \ldots Q_m = Q_1^{-1}Q_1 \ldots Q_m = P_1^{-1}P_1 \ldots P_n = P_2 \ldots P_n$ according to Lemma II.11.28. The claim now follows by induction on n. □

Remark II.11.30.

(i) As a prime ideal, (0) is also a product of prime ideals, although the factors are no longer uniquely determined, because $(0)^2 = (0)$.

(ii) The proof of Theorem II.11.29 shows that a prime ideal P occurs in the decomposition of $I \trianglelefteq R$ if and only if $I \subseteq P$.

Example II.11.31. We had seen in Example II.5.9 that $R := \mathbb{Z}[\sqrt{-5}]$ is not factorial, because

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

are two different "prime factorizations". On the other hand, according to Theorem II.11.13, R is the ring of integers of the number field $\mathbb{Q}(\sqrt{-5})$ and therefore a Dedekind domain according to Theorem II.11.25. Let $P := (2, 1 + \sqrt{-5}) \trianglelefteq R$. In the case $1 \in P$, there exist $a, b, c, d \in \mathbb{Z}$ with

$$1 = 2(a + b\sqrt{-5}) + (1 + \sqrt{-5})(c + d\sqrt{-5}) = 2a + c - 5d + (2b + c + d)\sqrt{-5}.$$

Then

$$1 = 2a + c - 5d \equiv c + d \equiv 2b + c + d \equiv 0 \pmod 2$$

would hold. Thus $P \lhd R$ and $R/P \cong \mathbb{F}_2$. Consequently, P is a maximal ideal and a prime ideal. Because of

$$\begin{aligned} 2 &= 2(1+\sqrt{-5}) - 2^2 - (1+\sqrt{-5})^2 \in P^2 \\ (1+\sqrt{-5})^2 &= 2(-2+\sqrt{-5}) \in (2) \end{aligned}$$

we have $(2) = P^2$. Analogously, one shows $(3) = Q\overline{Q}$ with the prime ideals $Q := (3, 1+\sqrt{-5})$ and $\overline{Q} := (3, 1-\sqrt{-5})$ of R. Altogether, $(6) = P^2 Q\overline{Q}$ is the unique prime ideal factorization of (6) in R. In the following, we investigate such factorizations systematically.

Theorem II.11.32. *The fractional ideals of a Dedekind domain R form a free abelian group I_R with respect to multiplication with identity element R. The fractional principal ideals form a normal subgroup $H_R \trianglelefteq I_R$.*

Proof. Let I be a fractional ideal of R and $rI \subseteq R$ for some $r \in R \setminus \{0\}$. Then $rI, rR \trianglelefteq R$. According to Theorem II.11.29, there exist prime ideals $P_1, \ldots, P_n, Q_1, \ldots, Q_m$ with $rI = P_1 \ldots P_n$ and $rR = Q_1 \ldots Q_m$. From $(rR)(r^{-1}R) = R = Q_1 \ldots Q_m Q_1^{-1} \ldots Q_m^{-1}$ it follows that $r^{-1}R = Q_1^{-1} \ldots Q_m^{-1}$ according to Lemma II.11.21(iv). This shows

$$I = (rI)(r^{-1}R) = P_1 \ldots P_n Q_1^{-1} \ldots Q_m^{-1}$$

and $I^{-1} = P_1^{-1} \ldots P_n^{-1} Q_1 \ldots Q_m$. Consequently, every fractional ideal is invertible and the abelian group I_R is generated by the prime ideals. The uniqueness in Theorem II.11.29 shows that the prime ideals even form a basis of I_R. Obviously $H_R \leq I_R$. Since I_R is abelian, $H_R \trianglelefteq I_R$ also holds. □

Definition II.11.33. One calls I_R the *ideal group* and I_R/H_R the *class group* of R. Furthermore, $|I_R/H_R|$ is the *class number* of R.

Remark II.11.34.

(i) The Dedekind domains with class number 1 are obviously exactly the principal ideal domains. The class number thus measures how far a Dedekind domain is from being a principal ideal domain. One can show that $\mathbb{Z}[\sqrt{-5}]$ has class number 2. More generally, the rings of integers of number fields always have finite class number (without proof).

(ii) In the following, we summarize the unique factorization of a fractional ideal I in the form $I = \prod_{i=1}^{n} P_i^{a_i}$, where $P_1, \ldots, P_n$ are pairwise distinct prime ideals and $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$.

(iii) The next theorem shows that each of the requirements of a Dedekind domain is indeed necessary for the existence of a prime ideal decomposition.

Theorem II.11.35. *An integral domain is a Dedekind domain if and only if every fractional ideal is invertible.*

Proof. According to Theorem II.11.32, every Dedekind domain satisfies the specified condition. Conversely, let R be an integral domain in which every fractional ideal is invertible. Let $0 \neq I \trianglelefteq R$. Then there exist $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in I^{-1}$ with $1 = a_1b_1 + \ldots + a_nb_n$. For $x \in I$, it holds that $x = (xb_1)a_1 + \ldots + (xb_n)a_n \in Ra_1 + \ldots + Ra_n$. Thus $I = (a_1, \ldots, a_n)$ and R is Noetherian.

Now let $\{0 \neq P \trianglelefteq R$ be a prime ideal and $M \trianglelefteq R$ maximal with $P \subseteq M$. Because of $M^{-1}P \subseteq M^{-1}M = R$, $M^{-1}P \trianglelefteq R$ holds. From $M(M^{-1}P) = RP = P$ it follows that $M = P$ or $M^{-1}P \subseteq P$. In the second case, one obtains the contradiction $R = MM^{-1}PP^{-1} \subseteq MPP^{-1} \subseteq M$. Therefore, every non-trivial prime ideal is maximal.

Finally, let $x \in Q(R)^\times$ be integral over R. Then $R[x] \neq 0$ is finitely generated, thus a fractional ideal according to Lemma II.11.21. By assumption, $x \in R[x] = R[x]R[x]R[x]^{-1} = R[x]R[x]^{-1} = R$. Thus R is integrally closed and therefore a Dedekind domain. □

Theorem II.11.36. *Let R be a Dedekind domain and $I = \prod_{i=1}^n P_i^{a_i}$ and $J = \prod_{i=1}^n P_i^{b_i}$ be prime ideal decompositions with $a_1, b_1, \ldots, a_n, b_n \in \mathbb{N}_0$. Then*

$$I + J = \prod_{i=1}^{n} P_i^{\min\{a_i, b_i\}}.$$

In particular,

(i) $I \subseteq J \iff \forall i : a_i \geq b_i$.

(ii) $I + J = R \iff \forall i : a_i b_i = 0$.

Proof. Let $c_i := \min\{a_i, b_i\}$ for $i = 1, \ldots, n$. Since $\prod P_i^{c_i}$ is a factor in $\prod P_i^{a_i}$, it holds that $I \subseteq \prod P_i^{c_i}$ and analogously $J \subseteq \prod P_i^{c_i}$. Since the product is an ideal, it follows that $I + J \subseteq \prod P_i^{c_i}$. Suppose $I + J \subseteq P_i^{c_i+1}$ for some i. Wlog. let $a_i = c_i$. From $I \subseteq I + J \subseteq P_i^{c_i+1}$ it follows that $\prod_{j \neq i} P_j^{a_j} \subseteq P_i$. This contradicts the prime ideal property. Therefore, $\prod P_i^{c_i}$ is the prime ideal decomposition of $I + J$. The last two statements follow immediately. □

Corollary II.11.37. *Let R be a Dedekind domain and $0 \neq x \in I \trianglelefteq R$. Then there exists $y \in I$ such that $I = (x, y)$.*

Proof. Let $I = \prod_{i=1}^n P_i^{a_i}$ and $(x) = \prod_{i=1}^n P_i^{b_i}$ be the prime ideal factorizations of I and (x). Because of $(x) \subseteq I$, it holds that $a_i \leq b_i$ for $i = 1, \ldots, n$. Let $x_i \in P_i^{a_i} \setminus P_i^{a_i+1}$. According to Theorem II.11.36, $P_i^{a_i+1} + P_j^{a_j+1} = R$ for $i \neq j$. By the Chinese Remainder Theorem I.7.30, there exists $y \in R$ with $y \equiv x_i \pmod{P_i^{a_i+1}}$ for $i = 1, \ldots, n$. Then $y \in P_i^{a_i} \setminus P_i^{a_i+1}$, i. e. a_i is the exponent of P_i in the prime ideal factorization of (y). With Theorem II.11.36 it follows that $I = (x) + (y) = (x, y)$. □

Lemma II.11.38. *Let $R \subseteq S$ be Dedekind domains and S be integral over R. For $I \lhd R$, $SI \lhd S$ holds, and for $0 \neq J \trianglelefteq S$, $0 \neq J \cap R \trianglelefteq R$ holds.*

Proof. We consider R, S and $Q(R)$ as subrings of $Q(S)$. Since R is integrally closed, $S \cap Q(R) = R$ holds. Certainly $SI \trianglelefteq S$ and it suffices to show $SI \neq S$. For this we can assume that I is maximal. For $x \in I \setminus I^2$, $Rx = II'$ holds, where $I' \trianglelefteq R$ is a product of prime ideals $\neq I$. In particular, $I + I' = R$ holds according to Theorem II.11.36. Let $1 = y + a$ with $y \in I$ and $a \in I'$. Then $a \notin I$ and $aI \subseteq II' = Rx$. In the case $SI = S$, we would have $aS = aIS \subseteq xS$ and $a = xz$ with $z = \frac{a}{x} \in S \cap Q(R) = R$, i. e. $a \in I$. Contradiction.

Certainly $J \cap R \trianglelefteq R$ and it suffices to show $J \cap R \neq 0$. Let $x \in J \setminus \{0\}$. Since S is integral over R, there exist $a_0, \ldots, a_n \in R$ with $x^{n+1} + a_n x^n + \ldots + a_0 = 0$. Wlog. let $a_0 \neq 0$. Then $a_0 = -x^{n+1} - a_n x^n - \ldots - a_1 x \in J \cap R$. □

Definition II.11.39. Let K be a number field and $P \trianglelefteq \mathbb{Z}_K$ a non-trivial prime ideal. Lemma II.11.38 with $R = \mathbb{Z}$ shows $P \cap \mathbb{Z} = (p)$ for a prime number $p \in \mathbb{N}$.

- The exponent $e_p(P)$ of P in the prime ideal factorization of $\mathbb{Z}_K p$ is called the *ramification index* of P with respect to p.
- Because of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong (\mathbb{Z} + P)/P \subseteq \mathbb{Z}_K/P$, one can view $\mathbb{Z}_K/P$ as a field extension of $\mathbb{F}_p$. One calls $f_p(P) := |\mathbb{Z}_K/P : \mathbb{F}_p|$ the *inertia degree* of P with respect to p. According to Theorem II.11.16, $f_p(P) < \infty$, i. e. $\mathbb{Z}_K/P \cong \mathbb{F}_{p^{f_p(P)}}$.

Theorem II.11.40 (Fundamental Equation)**.** *Let K be a number field and $p \in \mathbb{N}$ a prime number. Let $P_1, \ldots, P_n$ be the prime ideals of $\mathbb{Z}_K$ that contain p. Then*

$$\boxed{|K : \mathbb{Q}| = \sum_{i=1}^{n} e_p(P_i) f_p(P_i).}$$

Proof. Let $d := |K : \mathbb{Q}|$. According to Theorem II.11.16, $\mathbb{Z}_K$ is a free abelian group with basis $b_1, \ldots, b_d$. Obviously, $pb_1, \ldots, pb_d$ is a basis of $\mathbb{Z}_K p$. This shows $|\mathbb{Z}_K/\mathbb{Z}_K p| = p^d$ (Theorem II.9.32). Let $e_i := e_p(P_i)$ and $f_i := f_p(P_i)$ for $i = 1, \ldots, n$. For $i \neq j$, $P_i^{e_i} + P_j^{e_j} = \mathbb{Z}_K$ holds by Theorem II.11.36. With the Chinese Remainder Theorem, it follows that

$$\mathbb{Z}_K/\mathbb{Z}_K p = \mathbb{Z}_K/P_1^{e_1} \ldots P_n^{e_n} \cong (\mathbb{Z}_K/P_1^{e_1}) \times \ldots \times (\mathbb{Z}_K/P_n^{e_n}).$$

It is therefore sufficient to prove $|\mathbb{Z}_K/P_i^{e_i}| = p^{e_i f_i}$ for $i = 1, \ldots, n$. More precisely, we show $|P_i^k/P_i^{k+1}| = p^{f_i}$ for $k \in \mathbb{N}_0$. For $a \in P_i^k \setminus P_i^{k+1}$, the map

$$\begin{aligned} \varphi \colon \mathbb{Z}_K &\to P_i^k/P_i^{k+1}, \\ x &\mapsto xa + P_i^{k+1} \end{aligned}$$

is a homomorphism of $\mathbb{Z}_K$-modules with $P_i \subseteq \operatorname{Ker}(\varphi)$. Because $a \notin P_i^{k+1}$, $\operatorname{Ker}(\varphi) \lhd \mathbb{Z}_K$. The maximality of P_i shows $\operatorname{Ker}(\varphi) = P_i$. Let $\varphi(\mathbb{Z}_K) = Q/P_i^{k+1}$ with $Q = \mathbb{Z}_K a + P_i^{k+1} \trianglelefteq \mathbb{Z}_K$. Because $P_i^{k+1} \subsetneq Q$, P_i is the only prime ideal containing Q. The unique prime ideal factorization yields $Q = P_i^k$, i. e. φ is surjective. This shows

$$|P_i^k/P_i^{k+1}| = |\varphi(\mathbb{Z}_K)| = |\mathbb{Z}_K/\operatorname{Ker}(\varphi)| = |\mathbb{Z}_K/P_i| = p^{f_i}$$

as claimed. □

Theorem II.11.41. *Let $p \in \mathbb{P}$, $\mathbb{Q} \subseteq K$ be a Galois extension and $P \trianglelefteq \mathbb{Z}_K$ a prime ideal with $p \in P$. Then $\{\alpha(P) : \alpha \in \operatorname{Gal}(K|\mathbb{Q})\}$ is the set of prime ideals of $\mathbb{Z}_K$ that contain p. In particular, $e_p(P)$ and $f_p(P)$ do not depend on the choice of P. Furthermore, $e_p(P) f_p(P)$ is a divisor of $|K : \mathbb{Q}|$.*

Proof. For $\sigma \in G := \operatorname{Gal}(K|\mathbb{Q})$ and $x \in \mathbb{Z}_K$, we also have $\sigma(x) \in \mathbb{Z}_K$ (same minimal polynomial). The same argument with σ^{-1} yields $\sigma(\mathbb{Z}_K) \subseteq \mathbb{Z}_K = \sigma(\sigma^{-1}(\mathbb{Z}_K)) \subseteq \sigma(\mathbb{Z}_K)$, i. e. σ is a ring automorphism of $\mathbb{Z}_K$. With P, $\sigma(P)$ is also a prime ideal with $p = \sigma(p) \in \sigma(P)$. Suppose there exists a prime ideal

$Q \trianglelefteq \mathbb{Z}_K$ with $p \in Q$ outside the orbit of P under G. By the Chinese Remainder Theorem for rings, there exists $x \in P$ with $x \equiv 1 \pmod{\sigma(Q)}$ for all $\sigma \in G$. Then on the one hand

$$\prod_{\sigma \in G} \sigma(x) \in P \cap \mathbb{Q} = P \cap \mathbb{Z}_K \cap \mathbb{Q} = P \cap \mathbb{Z} = (p)$$

and on the other hand

$$\prod_{\sigma \in G} \sigma(x) \in (1+Q)^{|G|} \cap \mathbb{Z} \subseteq (1+Q) \cap \mathbb{Z} = 1 + (p).$$

This contradiction shows the first claim. The second claim is obtained by applying $\sigma \in G$ to the prime ideal factorization of $\mathbb{Z}_K p$. The last claim follows from Theorem II.11.40. □

Remark II.11.42. In the situation of Theorem II.11.41, p is called

- *inert*, if $f_p(P) = |K : \mathbb{Q}|$ (then p is a prime element in $\mathbb{Z}_K$).
- *ramified*, if $e_p(P) > 1$.
- *split*, if $e_p(P) = f_p(P) = 1$.

(cf. Example II.5.33).

Theorem II.11.43. *Let $\mathbb{Q} \subseteq K$ be a Galois extension with primitive element $x \in \mathbb{Z}_K$. Let μ be the minimal polynomial of x. Then every ramified prime number is a divisor of the discriminant D_μ. In particular, there exist only finitely many ramified prime numbers with respect to K.*

Proof. Let $p \in \mathbb{P}$ not be a divisor of D_μ and $P \trianglelefteq \mathbb{Z}_K$ be a prime ideal with $p \in P$. Let $G := \mathrm{Gal}(K|\mathbb{Q})$ and $G_P := \{\sigma \in G : \sigma(P) = P\}$ be the stabilizer of P. According to Theorem II.11.41 and Theorem I.4.7, it holds that

$$|G| = |K : \mathbb{Q}| = |G : G_P| e_p(P) f_p(P)$$

and $|G_P| = e_p(P) f_p(P)$. Since x is integral, $\mu \in \mathbb{Z}[X]$ and $\mu = (X - x_1) \dots (X - x_n)$ with $x_1, \dots, x_n \in \mathbb{Z}_K$. The reduction $\bar{\mu} \in \mathbb{F}_p[X]$ splits in $\overline{K} := \mathbb{Z}_K / P$ in the form $\bar{\mu} = (X - \overline{x_1}) \dots (X - \overline{x_n})$, where $\overline{x_i} := x_i + P$. By assumption, $D_{\bar{\mu}} = \overline{D_\mu} \neq 0$. Therefore, $\overline{x_1}, \dots \overline{x_n}$ are pairwise distinct. As in the proof of Theorem II.11.41, $g(\mathbb{Z}_K) = \mathbb{Z}_K$ holds for all $g \in G$. For $g \in G_P$, $\overline{K} \to \overline{K}$, $\lambda + P \mapsto g(\lambda) + P$ is a field automorphism. This yields a homomorphism $\varphi \colon G_P \to \mathrm{Gal}(\overline{K}|\mathbb{F}_p)$. Since G acts faithfully on $\{x_1, \dots, x_n\}$, the action of G_P on $\{\overline{x_1}, \dots, \overline{x_n}\}$ is also faithful. In particular, φ is injective and

$$e_p(P) f_p(P) = |G_P| \leq |\mathrm{Gal}(\overline{K}|\mathbb{F}_p)| = |\overline{K} : \mathbb{F}_p| = f_p(P). \tag{II.11.1}$$

It follows that $e_p(P) = 1$ and p is unramified. □

Theorem II.11.44 (Dedekind)**.** *Let $\alpha \in \mathbb{Z}[X]$ and $p \in \mathbb{P}$ not be a divisor of D_α. Let the leading coefficient of α not be divisible by p. Let the reduction $\bar{\alpha} \in \mathbb{F}_p[X]$ be a product of irreducible polynomials with degrees $d_1, \dots, d_k$. Then* $\mathrm{Gal}(\alpha)$ *possesses an element of cycle type $(d_1, \dots, d_k)$ with respect to the action on the roots of α.*

Proof. Let K be a splitting field of α and $G := \mathrm{Gal}(\alpha) = \mathrm{Gal}(K|\mathbb{Q})$. Let $P \trianglelefteq \mathbb{Z}_K$ be a prime ideal with $p \in P$. We argue as in the proof of Theorem II.11.43 (the irreducibility of α is not required). The assumption on the leading coefficient of α guarantees $\deg \alpha = \deg \overline{\alpha}$. Because of $p \nmid D_\alpha$ and (II.11.1), $\varphi\colon G_P \to \overline{G} := \mathrm{Gal}(\overline{K}|\mathbb{F}_p)$ is an isomorphism. According to Theorem I.11.14, $\overline{G} = \langle F \rangle$ is cyclic, where F is the Frobenius automorphism. Let $\overline{\alpha} = \overline{\alpha}_1 \dots \overline{\alpha}_k$ with $d_k = \deg \overline{\alpha}_i$ for $i = 1, \dots, k$. Since the roots of $\overline{\alpha}$ are pairwise distinct, $\overline{\alpha}_i \neq \overline{\alpha}_j$ for $i \neq j$. Since $\overline{\alpha}_i$ is irreducible, F must permute the roots of $\overline{\alpha}_i$ transitively. Thus F has the cycle type $(d_1, \dots, d_k)$ on the roots of $\overline{\alpha}$. Now choose $\varphi^{-1}(F) \in G$. □

Remark II.11.45. The Galois automorphism $\gamma := \varphi^{-1}(F)$ constructed in the proof of Theorem II.11.44 satisfies $\gamma(x) \equiv F(x) \equiv x^p \pmod{P}$ for all $x \in \mathbb{Z}_K$ and is therefore called the *Frobenius element* of K with respect to P. Since the prime ideals of $\mathbb{Z}_K$ containing p are conjugate under G, every unramified prime p determines exactly one conjugacy class of Frobenius elements. According to the deep *density theorem* of Chebotarev, the unramified primes are distributed "uniformly" among the conjugacy classes of G: For $g \in G$, the proportion of primes whose Frobenius element is conjugate to g is exactly $\frac{1}{|C_G(g)|}$. In particular, for every cycle type of elements of G, one finds infinitely many corresponding primes. The proportion of split primes (i.e., the Frobenius element is 1) is $\frac{1}{|G|} = \frac{1}{|K:\mathbb{Q}|}$.

Example II.11.46.

(i) Let $n \in \mathbb{N}$, $K = \mathbb{Q}_n$ and $\zeta \in K$ be a primitive n-th root of unity. Then $G := \mathrm{Gal}(K|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian. According to Remark A.3.18, the prime divisors of n and D_{Φ_n} coincide. Let $p \in \mathbb{P}$ with $p \nmid n$ and $P \trianglelefteq \mathbb{Z}_K$ be a prime ideal with $p \in P$. Let $\sigma \in G_P$ with $\sigma(\zeta) = \zeta^a$. According to Theorem A.3.17, $\mathbb{Z}_K = \mathbb{Z}[\zeta]$ holds. Therefore, σ is the Frobenius element with respect to P if and only if $\zeta^a \equiv \zeta^p \pmod{P}$ holds. Because of $D_{\overline{\Phi_n}} = \overline{D_{\Phi_n}} \neq 0$, the primitive roots of unity modulo P are pairwise distinct. Thus, it holds that

$$\zeta^a \equiv \zeta^p \pmod{P} \iff \zeta^a = \zeta^p \iff p \equiv a \pmod{n}.$$

According to the density theorem, the proportion of prime numbers $p \in a + n\mathbb{Z}$ is exactly $\frac{1}{\varphi(n)}$. In particular, there are infinitely many such prime numbers for each $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, i. e. Dirichlet's prime number theorem holds.

(ii) There is a simple method for the construction of Galois groups with prescribed cycle types. For $p \in \mathbb{P}$ and $d \in \mathbb{N}$, there are $\varphi(p^d - 1)$ generators of the cyclic group $\mathbb{F}_{p^d}^\times$. The minimal polynomial of each generator over $\mathbb{F}_p$ is irreducible of degree d. Each d such generators thus determine an irreducible polynomial in $\mathbb{F}_p[X]$ of degree d. Since $\varphi(p^d - 1)/d$ tends to infinity as p goes to infinity, one finds for sufficiently large p arbitrarily many pairwise distinct irreducible polynomials of degree d (cf. Exercise I.61).

Now let $(d_1, \dots, d_k)$ be a partition of $n \in \mathbb{N}$, i. e. $d_1 + \dots + d_k = n$. Then for "large" p there exists a monic polynomial $\beta_p \in \mathbb{F}_p[X]$ of degree n with pairwise distinct prime factors with degrees $d_1, \dots, d_k$. If another partition $(e_1, \dots, e_l)$ of n is given, one finds a prime number $q \neq p$ and $\beta_q \in \mathbb{F}_q[X]$ monic with pairwise distinct prime factors with degrees $e_1, \dots, e_l$. In the same way, one can add arbitrarily many further cycle types. According to the Chinese Remainder Theorem, there exists $\alpha \in \mathbb{Z}[X]$ with $\alpha \equiv \beta_p \pmod{p}$ and $\alpha \equiv \beta_q \pmod{q}$. Since β_p and β_q are monic of degree n, one can also choose α monic of degree n. Since β_p and β_q have pairwise distinct roots, D_α is divisible neither by p nor by q. Theorem II.11.44 provides elements in $\mathrm{Gal}(\alpha)$ with cycle type $(d_1, \dots, d_k)$ and $(e_1, \dots, e_l)$.

(iii) Let $\alpha \in \mathbb{Z}[X]$ be monic of degree n and $p \in \mathbb{P}$ split with respect to the splitting field of α. Then the reduction $\overline{\alpha} \in \mathbb{F}_p[X]$ splits into pairwise distinct linear factors. In particular, $p \geq n$.

Lemma II.11.47. *Let $G \leq S_n$ be a transitive permutation group containing a transposition. If $n \in \mathbb{P}$ or G possesses an $(n-1)$-cycle, then $G = S_n$.*

Proof.

(i) First let $n \in \mathbb{P}$. Then there exists an n-cycle $\sigma \in G$. Wlog. let $(1,2) \in G$. By replacing σ with a suitable power, one can assume $\sigma = (1, 2, a_3, \ldots, a_n)$. After conjugation, $\sigma = (1, 2, \ldots, n)$. Now one obtains $\sigma(1,2)\sigma^{-1} = (2,3) \in G$, $(3,4) \in G$ etc. As is well known, S_n is generated by these transpositions.

(ii) Let n be arbitrary and $\sigma \in G$ an $(n-1)$-cycle. Wlog. let $\sigma = (2, \ldots, n) \in G$. Let $\tau := (a, b) \in G$ be a transposition. Since G is transitive, there exists $\rho \in G$ with $\rho(a) = 1$. By replacing τ with $\rho\tau\rho^{-1} = (\rho(a), \rho(b))$, we can assume $a = 1$. Conjugation of τ with the powers of σ yields the transpositions $(1,2), (1,3), \ldots, (1,n) \in G$. As is well known, S_n is generated by these transpositions. □

Theorem II.11.48 (Hilbert)**.** *For every $n \in \mathbb{N}$ there exists a polynomial $\alpha \in \mathbb{Q}[X]$ with Galois group S_n.*

Proof. Wlog. let $n \geq 2$. According to Example II.11.46 there exists a monic polynomial $\alpha \in \mathbb{Z}[X]$ such that $G := \mathrm{Gal}(\alpha)$ possesses cycles of length 2, $n-1$ and n. In particular, G operates transitively on the set of roots of α. From Lemma II.11.47 it follows that $G \cong S_n$. □

Example II.11.49 (Schur)**.** Let $p \geq 5$ be a prime number and

$$\alpha = X^3(X-2)(X-4)\ldots(X-2p+6) - 2 \in \mathbb{Z}[X].$$

According to the Eisenstein criterion for $p = 2$, α is irreducible. Therefore $\mathrm{Gal}(\alpha)$ is transitive. Because of

$$\alpha(0) < 0, \qquad \alpha(1) > 0, \qquad \alpha(3) < 0, \qquad \ldots \qquad \alpha(2p-5) > 0$$

α has at least $p-2$ real roots. Because of $\alpha(x) < 0$ for $x \leq 0$, α possesses no negative real roots. If all roots $x_1, \ldots, x_p$ of α were real (and positive), then $\sigma_{p-1}(x_1, \ldots, x_p) > 0$ would be the coefficient of X in α. This contradiction shows that α possesses exactly two non-real roots. Complex conjugation yields a transposition in $\mathrm{Gal}(\alpha)$. According to Lemma II.11.47, $\mathrm{Gal}(\alpha) \cong S_p$.

II.12 Finite-dimensional algebras

Remark II.12.1. Many of the rings considered so far also possess a vector space structure (e. g. $K[X]$ or $K^{n\times n}$). Using methods of linear algebra, we will improve earlier structural statements.

Definition II.12.2. An *algebra* over a field K (briefly a *K-algebra*) is a ring A and at the same time a K-vector space, such that the scalar multiplication and the ring multiplication are compatible, i. e.

$$\lambda(ab) = (\lambda a)b = a(\lambda b)$$

for all $\lambda \in K$ and $a, b \in A$. One calls A *finite-dimensional*, if $\dim_K A < \infty$. An algebra that is a division ring as a ring is called a *division algebra*.

Remark II.12.3.

(i) A *subalgebra* of a K-algebra A is a subring of A which is at the same time a K-vector space. One can identify K with the subring $K1_A$ of A.

(ii) Unless stated otherwise, we always assume in the following that A is a finite-dimensional K-algebra and that every A-module M is finitely generated. By

$$\lambda m := (\lambda 1_A)m \qquad (\lambda \in K,\ m \in M)$$

M becomes a K-vector space. Let $b_1, \ldots, b_s \in A$ be a K-basis of A and $M = Am_1 + \ldots + Am_t$ with $m_1, \ldots, m_t \in M$. Then

$$M = \sum_{i=1}^{s} \sum_{j=1}^{t} Kb_i m_j,$$

i. e. $\{b_i m_j : 1 \le i \le s,\ 1 \le j \le t\}$ is a generating system of M as a K-vector space. In particular, $\dim_K M < \infty$. Since all submodules of M are also subspaces, M is Noetherian and Artinian. The choice $M = A$ shows that A is also Artinian (and Noetherian). We can therefore apply the theorems from chapter II.8. In particular, A possesses a Peirce decomposition into blocks, which are themselves algebras (since they are ideals).

(iii) Let $f\colon M \to N$ be a homomorphism of A-modules. Because of

$$f(\lambda m) = f((\lambda 1_A)m) = (\lambda 1_A)f(m) = \lambda f(m)$$

for $\lambda \in K$ and $m \in M$, f is also K-linear. Thus $\mathrm{Hom}_A(M, N) \subseteq \mathrm{Hom}_K(M, N)$ and $\mathrm{End}_A(M) \subseteq \mathrm{End}_K(M)$ hold. For $f \in \mathrm{End}_A(M)$ and $\lambda \in K$, $\lambda f := (\lambda 1_A)f \in \mathrm{End}_A(M)$ holds. In this way, $\mathrm{End}_A(M)$ becomes a K-algebra. According to Schur's Lemma, $\mathrm{End}_A(M)$ is a division algebra if M is simple.

(iv) A *homomorphism* of K-algebras A and B is a ring homomorphism $A \to B$ which is at the same time K-linear. As usual, one defines epi-, mono-, iso- and automorphisms of algebras. The homomorphism theorem, the isomorphism theorems and the Chinese remainder theorem then also hold for algebras (all maps are K-linear).

(v) If A is a semisimple algebra, then there exist division algebras $D_1, \ldots, D_k$ with $A \cong D_1^{d_1 \times d_1} \times \ldots \times D_k^{d_k \times d_k}$. Since the maps used in the proof of Artin-Wedderburn are all K-linear, this is an isomorphism of algebras. Furthermore, d_i is the multiplicity of the simple A-module $M_i := D_i^{d_i \times 1}$ as a composition factor of the regular module. At the same time, d_i is the dimension of M_i over $\mathrm{End}_A(M_i) \cong D_i^o$.

(vi) Let $e_1, \ldots, e_n$ be a K-basis of an algebra A. Then there exist $\lambda_{ijk} \in K$ with $e_i e_j = \sum_{k=1}^n \lambda_{ijk} e_k$. Obviously, the isomorphism type of A is uniquely determined by the λ_{ijk}. The λ_{ijk} are called the *structure constants* of A (with respect to a basis).

Example II.12.4.

(i) For every field K and $n \in \mathbb{N}$, $K^{n \times n}$ is a finite-dimensional K-algebra. In contrast, $K[X]$ and $K[[X]]$ (Exercise II.30) are infinite-dimensional K-algebras.

(ii) For every K-algebra A, $\mathrm{Z}(A)$ is also a K-algebra.

(iii) If $A_1, \ldots, A_n$ are algebras over K, then so is the direct product $A_1 \times \ldots \times A_n$.

(iv) If $K \subseteq L$ is a field extension, then L is a K-algebra.

(v) Every division ring Q is a $\mathrm{Z}(Q)$-algebra.

Lemma II.12.5. *For every algebra A and $n \in \mathbb{N}$, the following holds:*

(i) $\boxed{\mathrm{Z}(A^{n \times n}) = \mathrm{Z}(A)1_n \cong \mathrm{Z}(A).}$

(ii) $\boxed{\mathrm{J}(A^{n \times n}) = \mathrm{J}(A)^{n \times n}.}$

Proof.

(i) Certainly $\mathrm{Z}(A)1_n \subseteq \mathrm{Z}(A^{n \times n})$. Conversely, let $M = (a_{ij}) \in \mathrm{Z}(A^{n \times n})$. For $s \neq t$, let $E_{st} := (\delta_{is}\delta_{jt})_{i,j}$ be the matrix with a 1 at position (s,t) and zeros elsewhere. Then

$$(\delta_{jt}a_{is})_{i,j} = \Big(\sum_{k=1}^n a_{ik}\delta_{ks}\delta_{jt}\Big)_{i,j} = ME_{st} = E_{st}M = \Big(\sum_{k=1}^n \delta_{is}\delta_{kt}a_{kj}\Big)_{i,j} = (\delta_{is}a_{tj})_{i,j}$$

and it follows that $M \in A1_n$. Certainly $M \in \mathrm{Z}(A1_n) = \mathrm{Z}(A)1_n$ also holds.

(ii) Let $J := \mathrm{J}(A)$. An induction on k shows $(J^{n \times n})^k \subseteq (J^k)^{n \times n}$. Since J is nilpotent by Lemma II.8.15, $J^{n \times n}$ is also nilpotent. This shows $J^{n \times n} \subseteq \mathrm{J}(A^{n \times n})$. Conversely, let $a = (a_{ij})_{ij} \in \mathrm{J}(A^{n \times n})$ and $E_{st} = (\delta_{is}\delta_{jt}) \in A^{n \times n}$. Let $I \trianglelefteq A$ be the ideal generated by a_{st}. Then

$$IE_{11} \subseteq (E_{1s}aE_{t1}) \subseteq \mathrm{J}(A^{n \times n}).$$

Since $\mathrm{J}(A^{n \times n})$ is nilpotent, I must also be nilpotent. This shows $a_{st} \in I \subseteq J$ and $\mathrm{J}(A^{n \times n}) \subseteq J^{n \times n}$. □

Lemma II.12.6. *Every division algebra over an algebraically closed field K is isomorphic to K.*

Proof. Let D be a K-division algebra and $x \in D$. Then the powers $1_D, x, x^2, \ldots$ are linearly dependent over K. Therefore, there exists a monic $\alpha \in K[X] \setminus K$ with $\alpha(x) = 0$. Since K is algebraically closed, α splits into linear factors, say $\alpha = (X - \lambda_1 1_D) \ldots (X - \lambda_n 1_D)$ with $\lambda_1, \ldots, \lambda_n \in K$. As a division algebra, D has no zero divisors. From $\alpha(x) = 0$ it thus follows that $x - \lambda_i 1_D = 0$ for some $i \in \{1, \ldots, n\}$. Therefore $x = \lambda_i 1_D$ and $D = K1_D \cong K$. □

Remark II.12.7. Frobenius showed that $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$ (Exercise I.50) are the only finite-dimensional division algebras over $\mathbb{R}$ (see Theorem III.7.27).

Definition II.12.8. A ring R is called *local*, if R has only one maximal left ideal.

Example II.12.9.

(i) Every division ring is a local ring with maximal left ideal 0.

(ii) Let R be a Dedekind domain with a non-trivial prime ideal P. Then R/P^n is local for all $n \in \mathbb{N}$ with maximal (left) ideal P/P^n. In particular, one obtains the local rings $K[X]/(X^n)$ and $\mathbb{Z}/2^n\mathbb{Z}$.

(iii) The ring of formal power series $K[[X]]$ (Exercise II.30) is local with maximal ideal (X), because $K[[X]]^\times = K[[X]] \setminus (X)$.

(iv) Let R be a local principal ideal domain (e. g. $K[[X]]$). Then the powers of $\mathrm{J}(R)$ are the only proper ideals of R. One then speaks of a *discrete valuation ring* (see chapter III.10).

Lemma II.12.10 (Lifting of units/idempotents)**.** *Let R be a ring and $I \trianglelefteq R$ nilpotent. Then:*

(i) From $e + I \in (R/I)^\times$ it follows that $e \in R^\times$.

(ii) For every idempotent $\bar{e} \in R/I$ there exists an idempotent $e \in R$ with $e + I = \bar{e}$.

Proof (Koh).

(i) Let $f \in R$ with $ef \equiv 1 \pmod{I}$ and $x := 1 - ef \in I$. Since I is nilpotent, there exists an $n \in \mathbb{N}$ with $x^n = 0$. This shows

$$e \cdot f \sum_{k=0}^{n-1} x^k = (1 - x) \sum_{k=0}^{n-1} x^k = 1 - x^n = 1.$$

An analogous calculation with $1 - fe$ yields $e \in R^\times$.

(ii) Let $a \in R$ be arbitrary with $a + I = \bar{e}$. Then $(1 - a)a = a - a^2 \in I$. Since I is nilpotent, there exists an $n \in \mathbb{N}$ with $(1 - a)^n a^n = ((1 - a)a)^n = 0$. Let

$$e := \sum_{i=0}^{n} \binom{2n}{i} (1 - a)^i a^{2n-i}, \qquad f := \sum_{i=n+1}^{2n} \binom{2n}{i} (1 - a)^i a^{2n-i}.$$

Then

$$e + f = \sum_{i=0}^{2n} \binom{2n}{i} (1 - a)^i a^{2n-i} = ((1 - a) + a)^{2n} = 1.$$

Because of $a^{2n-i}(1 - a)^j = 0$ for $0 \leq i \leq n$ and $n + 1 \leq j \leq 2n$, it holds that $ef = 0$. This shows $e = e(e + f) = e^2 + ef = e^2$ and $e \equiv a^{2n} \equiv a \pmod{I}$. □

Theorem II.12.11. *For every algebra A, the following statements are equivalent:*

(1) A is local.

(2) $A/\mathrm{J}(A)$ is a division algebra.

(3) Every element in A is invertible or nilpotent.

(4) 0 and 1 are the only idempotents of A.

(5) The regular A-module is indecomposable.

Proof.

(1) $\Rightarrow$ (2): Apparently $\mathrm{J}(A)$ is the only maximal left ideal. In particular, $A/\mathrm{J}(A)$ is a simple algebra, thus of the form $A/\mathrm{J}(A) = D^{n\times n}$ for a division algebra D. In the case $n > 1$, $D^{n\times 1}$ would be a proper left ideal in $A/\mathrm{J}(A)$. According to the correspondence theorem, this is excluded.

(2) $\Rightarrow$ (3): According to Lemma II.8.15, $\mathrm{J}(A)$ is nilpotent and therefore consists only of nilpotent elements. Let $a \in A \setminus \mathrm{J}(A)$. By assumption, there exists $b \in A$ with $ab \equiv 1 \pmod{\mathrm{J}(A)}$ and $c := 1 - ab \in \mathrm{J}(A)$. Then there exists an $n \in \mathbb{N}$ with $c^n = 0$. This shows

$$a \cdot b \sum_{k=0}^{n-1} c^k = (1-c) \sum_{k=0}^{n-1} c^k = 1.$$

An analogous calculation with $1 - ba$ yields $a \in A^\times$.

(3) $\Rightarrow$ (4): Let $e = e^2 \in A$. In the case $e \in A^\times$, $e = 1$. Otherwise, $e^n = 0$ for some $n \in \mathbb{N}$. Then it follows that $e = e^2 = \ldots = e^n = 0$.

(4) $\Leftrightarrow$ (5): Follows from $A \cong \mathrm{End}_A(A)^o$ (Lemma II.7.20) and Theorem II.8.22.

(4) $\Rightarrow$ (1): According to Lemma II.12.10, the semisimple algebra $A/\mathrm{J}(A)$ (Lemma II.8.13) possesses only the idempotents 0 and 1. However, each component $D^{n\times n}$ in the Artin-Wedderburn decomposition of $A/\mathrm{J}(A)$ provides (at least) n idempotents $E_{11}, \ldots, E_{nn}$ according to Example II.8.19. Therefore, $A/\mathrm{J}(A)$ itself must be a division algebra. □

Remark II.12.12.

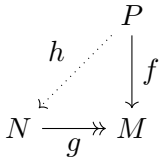
(i) A simple local algebra is a division algebra.

(ii) An A-module M is indecomposable if and only if $\mathrm{End}_A(M)$ is local (Theorem II.8.22).

Theorem II.12.13. *For every ring R and every R-module P, the following statements are equivalent:*

(1) P is a direct summand of a free R-module.

(2) For every homomorphism $f\colon P \to M$ and every epimorphism $g\colon N \to M$, there exists a homomorphism $h\colon P \to N$ with $g \circ h = f$.



(3) For every epimorphism $g\colon M \to P$, there exists a submodule $N \leq M$ with $M = \mathrm{Ker}(g) \oplus N$.

If applicable, P is called projective.

Proof.

(1) ⇒ (2): Let F be a free R-module with basis B and $F = P \oplus Q$. Let $\pi\colon F \to P$ be the projection. For $b \in B$ there exists $x_b \in N$ with $g(x_b) = f(\pi(b))$, since g is surjective. We define $h\colon F \to N$ by $h(b) := x_b$. For $x = \sum_{b\in B} \lambda_b b \in P$ with $\lambda_b \in A$ it holds that

$$g(h(x)) = \sum_{b\in B} \lambda_b g(h(b)) = \sum_{b\in B} \lambda_b g(x_b) = \sum_{b\in B} \lambda_b f(\pi(b)) = f\Big(\pi\Big(\sum_{b\in B} \lambda_b b\Big)\Big) = f(\pi(x)) = f(x).$$

(2) ⇒ (3): For $f = \mathrm{id}_P$ there exists $h\colon P \to M$ with $g \circ h = f$. Let $N := h(P) \leq M$. For $m \in M$ and $x := h(g(m)) \in N$ it holds that $g(m) = f(g(m)) = g(x)$ and $m - x \in \mathrm{Ker}(g)$. This shows $M = \mathrm{Ker}(g) + N$. For $h(x) \in \mathrm{Ker}(g) \cap N$ it holds that $x = f(x) = g(h(x)) = 0$ and $h(x) = 0$. Thus $M = \mathrm{Ker}(g) \oplus N$.

(3) ⇒ (1): By Theorem II.9.4 there exists a free module F and an epimorphism $g\colon F \to P$. By assumption $F = \mathrm{Ker}(g) \oplus N$ with $N \simeq F/\mathrm{Ker}(g) \simeq g(F) = P$. □

Example II.12.14.

(i) Every free A-module is projective. Conversely, if every projective module is free, then the regular module is indecomposable and A is local by Theorem II.12.11. Kaplansky has proven that in a local algebra every projective module is free (for finite-dimensional modules this follows from Krull-Schmidt). Quillen has proven that every finitely generated projective module over $K[X_1, \ldots, X_n]$ (for a field K) is free.

(ii) If P and Q are projective, then so is $P \times Q$, because if P (resp. Q) is a direct summand of the free module F_P (resp. F_Q), then $P \times Q$ is a direct summand of the free module $F_P \times F_Q$. More generally, the coproduct of projective modules is projective.

(iii) If A is semisimple, then every simple module is projective. By Lemma II.8.13 and (ii) even all A-modules are projective.

(iv) Every direct summand of a projective module is projective. Therefore, the projective, indecomposable (short *projective-indecomposable*) modules play a special role.

Lemma II.12.15 (Schanuel)**.** *Let P_1 and P_2 be projective A-modules. Let $U_i \leq P_i$ with $P_1/U_1 \simeq P_2/U_2$. Then $U_1 \times P_2 \simeq U_2 \times P_1$ holds.*

Proof. Let $\varphi\colon P_1/U_1 \to P_2/U_2$ be an isomorphism.

$$M := \big\{(x, y) \in P_1 \times P_2 : \varphi(x + U_1) = y + U_2\big\} \leq P_1 \times P_2.$$

The projections $\pi_i\colon M \to P_i$ are clearly surjective. Since P_i is projective, it follows that $M = \mathrm{Ker}(\pi_1) \oplus N_1 = \mathrm{Ker}(\pi_2) \oplus N_2$ with $N_i \simeq M/\mathrm{Ker}(\pi_i) \simeq P_i$, $\mathrm{Ker}(\pi_1) = \{0\} \times U_2 \simeq U_2$ and $\mathrm{Ker}(\pi_2) = U_1 \times \{0\} \simeq U_1$. □

Theorem II.12.16. *For every algebra A, the following holds:*

(i) The projective-indecomposable modules P are the indecomposable summands of the regular A-module. In particular, P is generated by one element.

(ii) The map $P \mapsto P/\mathrm{J}(P)$ induces a bijection between the set of isomorphism classes of projective-indecomposable A-modules and the set of isomorphism classes of simple A-modules.

Proof.

(ii) We first prove the statement only for finitely generated projective-indecomposable modules P. Let $\overline{P} := P/\mathrm{J}(P)$. For $f \in \mathrm{End}_A(P)$, it holds that

$$f(\mathrm{J}(P)) \overset{\text{II.8.13}}{=} f(\mathrm{J}(R)P) = \mathrm{J}(R)f(P) \subseteq \mathrm{J}(R)P \subseteq \mathrm{J}(P).$$

One obtains a well-defined map $\overline{f} \in \mathrm{End}_A(\overline{P})$ with $\overline{f}(x + \mathrm{J}(P)) := f(x) + \mathrm{J}(P)$ for $x \in P$.

Conversely, let $\varphi \in \mathrm{End}_A(\overline{P})$ be given. Then $f\colon P \to \overline{P}$, $x \mapsto \varphi(x + \mathrm{J}(P))$ is a homomorphism and $g\colon P \to \overline{P}$, $x \mapsto x + \mathrm{J}(P)$ is an epimorphism of A-modules. According to Theorem II.12.13, there exists $h \in \mathrm{End}_A(P)$ with $g \circ h = f$. This shows $\overline{h} = \varphi$. Thus $\mathrm{End}_A(P) \to \mathrm{End}_A(\overline{P})$, $f \mapsto \overline{f}$ is an epimorphism of algebras. According to Remark II.12.12, $\mathrm{End}_A(P)$ is local. If f is invertible (resp. nilpotent), then so is $\overline{f}$. Theorem II.12.11 shows that $\mathrm{End}_A(\overline{P})$ is local, i. e. $\overline{P}$ is indecomposable. On the other hand, $\overline{P}$ is semisimple according to Example II.8.9. Overall, $\overline{P}$ is simple.

If P and Q are isomorphic projective-indecomposable modules, then certainly $\overline{P} \simeq \overline{Q}$. Conversely, let $\varphi\colon \overline{P} \to \overline{Q}$ be an isomorphism. For the homomorphism $f\colon P \to \overline{Q}$, $x \mapsto \varphi(x + \mathrm{J}(P))$, there exists according to Theorem II.12.13 a homomorphism $h\colon P \to Q$ with

$$h(x) + \mathrm{J}(Q) = f(x) = \varphi(x + \mathrm{J}(P))$$

for all $x \in P$. This shows $h(P) + \mathrm{J}(Q) = Q$. From Nakayama's Lemma, it follows that $h(P) = Q$. According to Theorem II.12.13, there exists $N \leq P$ with $P = \mathrm{Ker}(h) \oplus N$. Since P is indecomposable, $\mathrm{Ker}(h) = 0$ must hold. Thus $h\colon P \to Q$ is an isomorphism.

Finally, let S be any simple A-module and $s \in S \setminus \{0\}$. Let $A = P_1 \oplus \ldots \oplus P_k$ be a decomposition into projective-indecomposable modules. As usual, there exists an epimorphism $f\colon A \to S$. Let $f(P_i) \neq 0$. Since S is simple, $P_i/\mathrm{Ker}(f) \simeq f(P_i) = S$ holds. In particular, $\mathrm{Ker}(f)$ is a maximal submodule of P_i and $\mathrm{J}(P_i) \leq \mathrm{Ker}(P_i)$. According to the first part of the proof, $P_i/\mathrm{J}(P_i)$ is simple and it follows that $\mathrm{J}(P_i) = \mathrm{Ker}(f)$. Overall, $S \simeq P_i/\mathrm{J}(P_i)$.

(i) Let P be a projective-indecomposable A-module (not necessarily finitely generated). Since $\mathrm{J}(A)$ is nilpotent, $\mathrm{J}(A)P < P$ holds and $P/\mathrm{J}(A)P$ is semisimple. Thus there exists a maximal submodule $M < P$. According to the first part of the proof, there exists an indecomposable summand Q of A and an isomorphism $\varphi\colon Q/\mathrm{J}(Q) \simeq P/M$. From the projectivity of P, one obtains a homomorphism $f\colon P \to Q$ with $\varphi(f(x) + \mathrm{J}(Q)) = x + M$ for $x \in P$. By Nakayama, f is surjective. The projectivity of Q, on the other hand, shows $P = \mathrm{Ker}(f) \oplus N$. Since P is indecomposable, $\mathrm{Ker}(f) = 0$ and $P \simeq Q$ must hold. This completes the proof of (ii). Since $Q/\mathrm{J}(Q)$ is simple, there exists an $x \in Q$ with $Rx + \mathrm{J}(Q) = Q$. By Nakayama, $Q = Rx$ already holds. □

Theorem II.12.17. *Let K be algebraically closed and P a projectively indecomposable A-module. Then $\dim_K(P/\mathrm{J}(P))$ is the multiplicity of P in the Krull-Schmidt decomposition of the regular A-module.*

Proof. Let $A = P_1 \oplus \ldots \oplus P_n$ be a decomposition into projectively indecomposable A-modules. According to Theorem II.12.16, $\overline{P_i} := P_i/\mathrm{J}(P_i)$ is a simple A-module and a simple $A/\mathrm{J}(A)$-module (Remark II.8.12). On the other hand, $A/\mathrm{J}(A) \simeq \overline{P_1} \oplus \ldots \oplus \overline{P_n}$ is semisimple. Since K is algebraically closed, $\mathrm{End}_A(\overline{P_i}) \cong K$ holds. According to Remark II.12.3, $\dim_K \overline{P_i}$ is the multiplicity of $\overline{P_i}$ as a composition factor of $A/\mathrm{J}(A)$. Theorem II.12.16 yields

$$\dim \overline{P} = \big|\{1 \leq i \leq n : \overline{P_i} \simeq \overline{P}\}\big| = \big|\{1 \leq i \leq n : P_i \simeq P\}\big|. \qquad \square$$

Lemma II.12.18. *Let P be a projectively indecomposable A-module, $E := \mathrm{End}_A(P)^o$ and $S := P/\mathrm{J}(P)$. For an arbitrary A-module M, the following hold:*

(i) $E/\mathrm{J}(E) \cong \mathrm{End}_A(S)^o =: D$.

(ii) By $f \cdot \varphi := \varphi \circ f$ *for* $f \in E$ *and* $\varphi \in \mathrm{Hom}_A(P, M)$, $\mathrm{Hom}_A(P, M)$ *becomes an* E*-module.*

(iii) The multiplicity of S *as a composition factor of* M *is* $\dim_K \mathrm{Hom}_A(P, M)/\dim_K D$.

Proof.

(i) Since P is indecomposable, E is local. Since $\mathrm{J}(P)$ is the unique maximal submodule of P, $f(\mathrm{J}(P)) \subseteq \mathrm{J}(P)$ holds for all $f \in E$. In particular, $\overline{f} \in D$ with $\overline{f}(x + \mathrm{J}(E)) = f(x) + \mathrm{J}(P)$ for $x \in P$ is well-defined. Since P is projective, conversely for all $\varphi \in D$ there exists an $f \in E$ with $\overline{f} = \varphi$ (see proof of Theorem II.12.16). Consequently, $E \to D$, $f \mapsto \overline{f}$ is an epimorphism with kernel $\mathrm{J}(E) = \mathrm{Hom}_A(P, \mathrm{J}(P))$.

(ii) For $f, g \in E$ we have $(fg)\varphi = \varphi \circ (g \circ f) = f(g\varphi)$. The other axioms are obvious.

(iii) Let $0 = M_0 < \ldots < M_k = M$ be a composition series of M. Then

$$0 = \mathrm{Hom}_A(P, M_0) \leq \ldots \leq \mathrm{Hom}_A(P, M_k) = \mathrm{Hom}_A(P, M)$$

is a sequence of E-modules according to (ii). For $i \geq 1$, the canonical homomorphism $\mathrm{Hom}_A(P, M_i) \to \mathrm{Hom}_A(P, M_i/M_{i-1})$ has kernel $\mathrm{Hom}_A(P, M_{i-1})$. Since M_i/M_{i-1} is simple, $\mathrm{Hom}_A(P, M_i/M_{i-1}) = 0$ if $M_i/M_{i-1} \not\simeq S$ according to Theorem II.12.16. If applicable, $\mathrm{Hom}_A(P, M_i) = \mathrm{Hom}_A(P, M_{i-1})$. Now let $M_i/M_{i-1} \simeq S$ and $f, g \in \mathrm{Hom}_A(P, S) \setminus \{0\}$. Since P is projective, there exists $\hat{f} \in E$ with $\hat{f}(x) + \mathrm{J}(P) = f(x)$ for all $x \in P$ (cf. proof of Theorem II.12.16). Since $\mathrm{J}(P)$ is the unique maximal submodule of P, $\hat{f}(P) = P$ and $\hat{f} \in E^\times$ holds. Analogously, there exists $\hat{g} \in E$ with $\hat{g}(x) + \mathrm{J}(P) = g(x)$. Finally,

$$\hat{g}\hat{f}^{-1} \cdot f = f \circ \hat{f}^{-1} \circ \hat{g} = g.$$

This shows that $\mathrm{Hom}_A(P, S)$ is a simple E-module. Since E is local, $\mathrm{Hom}_A(P, S) \simeq E/\mathrm{J}(E)$ holds. From (i) it follows that $\dim_K \mathrm{Hom}_A(P, S) = \dim_K D$. The existence of the canonical epimorphism $P \to S$ yields $\mathrm{Hom}_A(P, M_i)/\mathrm{Hom}_A(P, M_{i-1}) \simeq \mathrm{Hom}_A(P, S)$. The multiplicity of S as a composition factor of M is therefore the number of simple factors of $\mathrm{Hom}_A(P, M_0) \leq \ldots \leq \mathrm{Hom}_A(P, M)$. Since all other factors are trivial, the claim follows. □

Definition II.12.19. Let $P_1, \ldots, P_k$ be the projective-indecomposable A-modules up to isomorphism.

- One calls $A^b := \mathrm{End}_A(P_1 \times \ldots \times P_k)^o$ the *basic algebra* of A. In the case $A \cong A^b$, one calls A a *basic algebra*.
- Let c_{ij} be the multiplicity of $P_i/\mathrm{J}(P_i)$ as a composition factor of P_j. One calls $C(A) := (c_{ij})_{i,j} \in \mathbb{N}_0^{k \times k}$ the *Cartan matrix* of A.

Theorem II.12.20. *Let $e_1, \ldots, e_k \in A$ be pairwise orthogonal primitive idempotents, such that $Ae_1, \ldots, Ae_k$ represent the isomorphism classes of projective-indecomposable A-modules.*

(i) For $e := e_1 + \ldots + e_k$, *it holds that* $A^b \cong eAe$.

(ii) Let $D_i := \mathrm{End}_A(Ae_i/\mathrm{J}(Ae_i))$ *and* $C(A) = (c_{ij})$. *Then* $c_{ij} \dim_K D_i = \dim_K e_i A e_j$.

Proof.

(i) Because of $Ae = Ae_1 \oplus \ldots \oplus Ae_k$, the claim follows from Lemma II.7.20.

(ii) As in Lemma II.7.20, one shows that

$$\begin{aligned}\mathrm{Hom}_A(Ae_i, Ae_j) &\to e_iAe_j,\\ \varphi &\mapsto \varphi(e_i) = \varphi(e_i^2) = e_i\varphi(e_i)\end{aligned}$$

is a vector space isomorphism. Therefore, the claim follows from Lemma II.12.18. □

Remark II.12.21.

(i) In the situation of Theorem II.12.20, $e = e_1 + \ldots + e_k$ is called a *basic idempotent* for A (not uniquely determined).

(ii) The next theorems show that many questions about the module structure of A can be answered by the "smaller" basic algebra. It is often sufficient to only consider the basic algebras of the blocks of A (Theorem II.12.29).

(iii) If K is algebraically closed, then $D_i = K$ and $c_{ij} = \dim_K e_iAe_j$. From $A^b = \bigoplus_{i,j=1}^k e_iAe_j$ it then follows that $\dim A^b = \sum_{i,j=1}^k c_{ij}$.

Example II.12.22.

(i) If A is semisimple, then the projective-indecomposable modules $P_1, \ldots, P_k$ are exactly the simple A-modules (up to isomorphism) and one obtains $C(A) = 1_k$ and $A^b \cong \mathrm{End}_A(P_1)^o \times \ldots \times \mathrm{End}_A(P_k)^o = D_1 \times \ldots \times D_k$ with division algebras $D_1, \ldots, D_k$ (Lemma II.7.20). In particular, $(D^{n\times n})^b \cong D$ for every division algebra D.

(ii) Let $A/\mathrm{J}(A)$ be a direct sum of division algebras. According to Remark II.12.3, every projective-indecomposable module then occurs with multiplicity 1 in the regular A-module. This shows

$$A^b = \mathrm{End}_A(P_1 \times \ldots \times P_k)^o \cong \mathrm{End}_A(A)^o \cong A.$$

In particular, all commutative algebras are basic algebras.

(iii) Let $A \subseteq K^{n\times n}$ be the algebra of upper triangular matrices. The strict upper triangular matrices (i. e. zeros on the main diagonal) clearly form a nilpotent ideal $J \trianglelefteq A$ with $A/J \cong K^n$. This shows $J = \mathrm{J}(A)$. From (ii) it follows that $A \cong A^b$. For the primitive idempotents, one can choose $e_i := E_{ii} = (\delta_{si}\delta_{ti})_{st} \in A$. Then $e_iAe_j = KE_{ij}$ if $i \le j$ and $e_iAe_j = 0$ otherwise. This shows

$$C(A) = \begin{pmatrix} 1 & \cdots & 1 \\ & \ddots & \vdots \\ 0 & & 1 \end{pmatrix}.$$

Lemma II.12.23. *For every idempotent e of an algebra A, it holds that $\mathrm{J}(eAe) = e\mathrm{J}(A)e$.*

Proof. Since $\mathrm{J}(A)$ is nilpotent, $e\mathrm{J}(A)e \subseteq \mathrm{J}(A)$ is a nilpotent ideal of eAe. By Lemma II.8.15 it follows that $e\mathrm{J}(A)e \subseteq \mathrm{J}(eAe) =: J$. Conversely, J is also nilpotent, say $J^n = 0$. Then $AJA \trianglelefteq A$ with

$$(AJA)^{n+1} = A(JeAe)^nJA = AJ^{n+1}A = 0.$$

This shows $AJA \subseteq \mathrm{J}(A)$ and $J \subseteq eAeJeAe \subseteq e\mathrm{J}(A)e$. □

Theorem II.12.24. *For every algebra A, $C(A) = C(A^b)$ holds for a suitable ordering. In particular, A and A^b have the same number of simple modules up to isomorphism. If K is algebraically closed, then every simple A^b-module has dimension 1.*

Proof. With the notation from Theorem II.12.20, we have

$$A^b = eAe = eAe_1 \oplus \ldots \oplus eAe_k = A^be_1 \oplus \ldots \oplus A^be_k$$

with $E_i := \mathrm{End}_{A^b}(A^be_i)^o \cong e_iA^be_i = e_iAe_i \cong \mathrm{End}_A(Ae_i)^o$. According to Remark II.12.3 and Lemma II.12.18, $\overline{A} := A/\mathrm{J}(A) \cong D_1^{n_1\times n_1} \times \ldots \times D_k^{n_k\times n_k}$ with division algebras $D_i \cong E_i/\mathrm{J}(E_i)$. Wlog. let $\overline{e_i} := e_i + \mathrm{J}(A) = (0, \ldots, E_{11}, \ldots, 0)$, where $E_{11} = (\delta_{i1}\delta_{j1})_{ij} \in D^{n_i\times n_i}$. By Lemma II.12.23 it holds that

$$A^b/\mathrm{J}(A^b) = eAe/e\mathrm{J}(A)e = \bar{e}\overline{A}\bar{e} \cong D_1 \times \ldots \times D_k.$$

Therefore, $A^be_1, \ldots, A^be_k$ are exactly the projective-indecomposable A^b-modules up to isomorphism. From Lemma II.12.18 it follows that

$$C(A) = \Big(\frac{\dim_K \mathrm{Hom}_A(Ae_i, Ae_j)}{\dim_K D_i}\Big)_{ij} = \Big(\frac{\dim_K e_iAe_j}{\dim_K D_i}\Big)_{ij} = \Big(\frac{\dim_K e_iA^be_j}{\dim_K D_i}\Big)_{ij} = C(A^b).$$

If K is algebraically closed, then $D_1 = \ldots = D_k = K$ and the last claim follows from Remark II.12.3. □

Theorem II.12.25. *For every algebra A there exists an $n \in \mathbb{N}$ with $A \cong e(A^b)^{n\times n}e$, where e is an idempotent of $(A^b)^{n\times n}$.*

Proof. Let $P_1, \ldots, P_k$ be, as before, the projective-indecomposable A-modules up to isomorphism. Let $P := P_1 \times \ldots \times P_k$. Let n be the maximum multiplicity of a P_i in the regular A-module. Then A is a direct summand of P^n, say $P^n = A \oplus Q$. Let $\varphi \in \mathrm{End}_A(P^n)$ be the projection onto A. Then $\varphi\mathrm{End}_A(P^n)\varphi \to \mathrm{End}_A(A)$, $\varphi f\varphi \mapsto \varphi f\varphi_A$ is an isomorphism of algebras. Under the well-known isomorphism

$$\mathrm{End}_A(P^n)^o \cong (\mathrm{End}_A(P)^{n\times n})^o \cong (\mathrm{End}_A(P)^o)^{n\times n} = (A^b)^{n\times n}$$

(cf. proof of Artin-Wedderburn and Lemma II.7.20), φ is mapped to an idempotent $e \in (A^b)^{n\times n}$. It now holds that $A \cong \mathrm{End}_A(A)^o \cong e(A^b)^{n\times n}e$. □

Lemma II.12.26. *For algebras A, B and $n, m \in \mathbb{N}$ it holds that*

$$\boxed{(A \times B)^{n\times n} \cong A^{n\times n} \times B^{n\times n}} \qquad \boxed{(A^{n\times n})^{m\times m} \cong A^{nm\times nm}.}$$

Proof. Apparently, the map

$$\begin{aligned}(A \times B)^{n\times n} &\to A^{n\times n} \times B^{n\times n},\\ (a_{ij}, b_{ij})_{ij} &\mapsto \big((a_{ij})_{ij}, (b_{ij})_{ij}\big)\end{aligned}$$

is an isomorphism. The second isomorphism is obtained by partitioning matrices in $A^{nm\times nm}$ into $n \times n$-blocks (thus there is only a formal difference between the algebras). □

Theorem II.12.27. *For every algebra A with basic idempotent e, we have $\mathrm{Z}(A^b) \cong \mathrm{Z}(eAe) = e\mathrm{Z}(A)e \cong \mathrm{Z}(A)$.*

Proof. Apparently,

$$\Gamma\colon \mathrm{Z}(A) \to \mathrm{Z}(eAe) \cong \mathrm{Z}(A^b), \qquad z \mapsto ez = eze$$

is a ring homomorphism. Let $e = e_1 + \ldots + e_k$ with primitive idempotents $e_1, \ldots, e_k$. We can refine $1 = e + (1-e)$ to a decomposition $1 = e_1 + \ldots + e_n$ into primitive idempotents. Let $z \in \mathrm{Z}(A)$ with $ez = 0$. For each $i \leq n$, there exists a $j \leq k$ with $Ae_j \simeq Ae_i$. According to Theorem II.8.22, there exists an $x \in A^\times$ with $xe_jx^{-1} = e_i$. It follows that

$$e_iz = xe_jx^{-1}z = xe_jzx^{-1} = xe_jezx^{-1} = 0.$$

In total, $z = (e_1 + \ldots + e_n)z = 0$. Therefore, Γ is injective and $\dim \mathrm{Z}(A) \leq \dim \mathrm{Z}(A^b)$.

Now let $A \cong f(A^b)^{m\times m}f$ for an idempotent $f \in (A^b)^{m\times m} =: \hat{A}$ as in Theorem II.12.25. We decompose $f = f_1 + \ldots + f_l$ into pairwise orthogonal primitive idempotents. Let $A^b/\mathrm{J}(A^b) \cong D_1 \times \ldots \times D_k$. According to Lemma II.12.5 and Lemma II.12.26, we have

$$\hat{A}/\mathrm{J}(\hat{A}) = \hat{A}/\mathrm{J}(A^b)^{m\times m} \cong (A^b/\mathrm{J}(A^b))^{m\times m} \cong D_1^{m\times m} \times \ldots \times D_k^{m\times m}.$$

In particular, $\hat{A}$ has as many simple modules as A. Consequently, every indecomposable projective $\hat{A}$-module must be isomorphic to some $\hat{A}f_i$ (otherwise $A \cong f\hat{A}f$ would have fewer simple modules, cf. proof of Theorem II.12.24). We can now apply the argument from the first part of the proof to $\hat{A}$ and obtain $\dim \mathrm{Z}(A^b) \overset{\text{II.12.5}}{=} \dim \mathrm{Z}(\hat{A}) \leq \dim \mathrm{Z}(A)$. Thus Γ is an isomorphism. □

Remark II.12.28.

(i) For an arbitrary idempotent $e \in A$, it is not necessarily true that $\mathrm{Z}(eAe) = e\mathrm{Z}(A)e$ (Exercise II.64).

(ii) In the following, we call an $n \times n$-matrix $M = (m_{ij})$ *indecomposable*, if there exists no non-empty subset $I \subsetneq \{1, \ldots, n\}$ with $a_{ij} = 0 = a_{ji}$ for all $i \in I$ and $j \notin I$.

Theorem II.12.29. *Let $A = B_1 \oplus \ldots \oplus B_s$ be the Peirce decomposition of the algebra A. Then*

$$C(A) = \begin{pmatrix} C(B_1) & & 0 \\ & \ddots & \\ 0 & & C(B_s) \end{pmatrix}$$

holds for a suitable ordering. Furthermore, the matrices $C(B_i)$ are indecomposable.

Proof. Let $1 = z_1 + \ldots + z_s$ be the decomposition into central primitive idempotents with $B_i = Az_i$. We decompose $z_i = e_{i1} + \ldots + e_{ik_i}$ into pairwise orthogonal primitive idempotents. Then

$$\mathrm{Hom}_{B_i}(B_ie_{ij}, B_ie_{ik}) \simeq_K e_{ij}B_ie_{ik} = e_{ij}Ae_{ik} \simeq_K \mathrm{Hom}_A(Ae_{ij}, Ae_{ik})$$

and $\mathrm{End}_{B_i}(B_ie_{ij})^o \cong \mathrm{End}_A(Ae_{ij})$. According to Lemma II.12.18, the entries of $C(B_i)$ coincide with the corresponding entries from $C(A)$. Now let $i \neq j$. Then

$$e_{is}Ae_{jt} = z_ie_{is}Ae_{jt}z_j = e_{is}Ae_{jt}z_iz_j = 0.$$

The block diagonal form of $C(A)$ follows from Theorem II.12.20.

Now assume $C(B_i)$ is decomposable. Wlog. let $i = 1$ and $\varnothing \neq I \subsetneq \{1, \ldots, k_1\}$ with $e_{1i}Ae_{1j} = 0 = e_{1j}Ae_{1i}$ for all $i \in I$ and $j \notin I$. Let $e := \sum_{i\in I} e_{1i}$ and $a \in A$. Then

$$ea = ez_1a\sum_{i=1}^{s} z_i = eaz_1 = \sum_{i\in I} e_{1i}a\sum_{j=1}^{k} e_{1j} = eae = \ldots = ae$$

and $a \in \mathrm{Z}(A)$. The decomposition $z_1 = e + (z_1 - e)$ contradicts the primitivity of z_1 in $\mathrm{Z}(A)$. Thus $C(B_i)$ is indecomposable. □

Remark II.12.30. The non-negative, indecomposable Cartan matrices $C = C(B_i)$ in Theorem II.12.29 satisfy the requirements of the Perron-Frobenius theorem: The *spectral radius*

$$\rho(C) := \max\{|\lambda| : \lambda \in \mathbb{C} \text{ eigenvalue of } C\}$$

is an eigenvalue with algebraic multiplicity 1 and the corresponding eigenspace is spanned by a vector with positive entries. However, this theorem has not yet found application for algebras.

Corollary II.12.31. *Two simple A-modules S, T belong to the same block if and only if there exist projective-indecomposable A-modules $P_1, \ldots, P_k$ with the following properties:*

(i) $S \simeq P_1/\mathrm{J}(P_1)$ *and* $T \simeq P_k/\mathrm{J}(P_k)$.

(ii) For $i = 1, \ldots, k-1$, P_i *and* P_{i+1} *have a common composition factor.*

Proof. Suppose $P_1, \ldots, P_k$ exist and S belongs to the block B. Because of $S \simeq P_1/\mathrm{J}(P_1)$, P_1 also belongs to B. By induction, assume it has already been shown that P_i belongs to B. Let S_i be a common composition factor of P_i and P_{i+1}. Then the entry in $C(A)$ with respect to S_i and P_i is non-zero. From Theorem II.12.29 it follows that S_i belongs to B. For the same reason, P_{i+1} also belongs to B. In this way, it finally follows that T belongs to B.

Conversely, suppose that S and T belong to B. Let $P_1, \ldots, P_n$ be the projective-indecomposable B-modules with $S \simeq P_1/\mathrm{J}(P_1)$ and $T \simeq P_n/\mathrm{J}(P_n)$. Let Γ be the graph with vertices $P_1, \ldots, P_n$, such that P_i and P_j are connected by an edge if and only if they have a common composition factor. Let $\{P_i : i \in I\}$ be the connected component of P_1. For $C(B) = (c_{ij})$, it now holds that $c_{ij} = 0 = c_{ji}$ for all $i \in I$ and $j \notin I$. From Theorem II.12.29 it follows that $I = \{1, \ldots, n\}$. In particular, P_1 and P_n are connected. □

Definition II.12.32. For a K-algebra A, let $\gamma(A) := K\{ab - ba : a, b \in A\}$ be the *commutator space* of A.

Remark II.12.33. Attention: $\gamma(A)$ is neither an ideal nor a subring of A.

Lemma II.12.34.

(i) For K-algebras A, B, we have $\gamma(A \times B) = \gamma(A) \times \gamma(B)$.

(ii) For every K-algebra A and $I \trianglelefteq A$, we have $\gamma(A/I) = (\gamma(A) + I)/I$.

(iii) For $n \in \mathbb{N}$, we have $\gamma(K^{n\times n}) = \{M \in K^{n\times n} : \operatorname{tr} M = 0\}$. *In particular,* $\dim_K(K^{n\times n}/\gamma(K^{n\times n})) = 1$.

Proof.

(i) For $a_1, a_2 \in A$ and $b_1, b_2 \in B$, we have

$$(a_1, b_1)(a_2, b_2) - (a_2, b_2)(a_1, b_1) = (a_1a_2 - a_2a_1, b_1b_2 - b_2b_1) \in \gamma(A) \times \gamma(B).$$

(ii) For $a, b \in A$, we have $(a + I)(b + I) - (b + I)(a + I) = ab - ba + I \in \gamma(A) + I$.

(iii) For $a, b \in K^{n\times n}$, it is well known that $\mathrm{tr}(ab - ba) = \mathrm{tr}(ab) - \mathrm{tr}(ba) = 0$, i. e. $\gamma(K^{n\times n}) \subseteq \mathrm{Ker}(\mathrm{tr})$. Let, as usual, $E_{st} = (\delta_{is}\delta_{jt})_{i,j} \in K^{n\times n}$. For $s \neq t$, we have

$$E_{st} = E_{s1}E_{1t} - E_{1t}E_{s1} \in \gamma(K^{n\times n}),$$
$$E_{ss} - E_{tt} = E_{st}E_{ts} - E_{ts}E_{st} \in \gamma(K^{n\times n}).$$

Obviously, the matrices E_{st} $(s \neq t)$ and $E_{11} - E_{ss}$ $(2 \leq s \leq n)$ form a basis of $\mathrm{Ker}(\mathrm{tr})$. Therefore, $\mathrm{Ker}(\mathrm{tr}) \subseteq \gamma(K^{n\times n})$ holds. The second assertion follows from the isomorphism theorem for tr. $\square$

II.13 Symmetric Algebras and Group Algebras

Remark II.13.1. We give an introduction to the theory of symmetric algebras with the goal of proving the Wedderburn-Malcev Theorem. Subsequently, we assign a symmetric algebra to every finite group and investigate its properties. As in the last chapter, A is always a finite-dimensional K-algebra.

Definition II.13.2. We call A *symmetric*, if a bilinear form $\beta\colon A \times A \to K$ exists with the following properties:

- $\forall a, b \in A : \beta(a, b) = \beta(b, a)$ (symmetric),
- $\forall a, b, c \in A : \beta(ab, c) = \beta(a, bc)$ (associative),
- $\forall a \in A \setminus \{0\} : \beta(a, A) \neq 0$ (non-degenerate).

Example II.13.3.

(i) If $A_1, \ldots, A_n$ are symmetric algebras with bilinear forms $\beta_1, \ldots, \beta_n$, then $A := A_1 \times \ldots \times A_n$ is symmetric with respect to

$$\beta(a_1 \ldots a_n, b_1 \ldots b_n) := \beta_1(a_1, b_1) + \ldots + \beta_n(a_n, b_n)$$

for $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in A$.

(ii) Let A be symmetric with bilinear form β and $e \in A$ an idempotent. Then the restriction β' of β to $eAe \times eAe$ is obviously a symmetric, associative bilinear form. For every $a \in eAe \setminus \{0\}$ there exists a $b \in A$ with $\beta(a, b) \neq 0$. It follows

$$0 \neq \beta(ae, b) = \beta(a, eb) = \beta(eb, ea) = \beta(ebe, a).$$

Thus β' is non-degenerate and eAe is symmetric. In particular, every block of A is symmetric.

(iii) Let $A = K^{n\times n}$ and $\beta(a, b) := \mathrm{tr}(ab)$ for $a, b \in A$. Obviously β is a symmetric, associative bilinear form. For $a = (a_{ij})$ with $a_{st} \neq 0$ we have $\mathrm{tr}(E_{ts}a) = a_{st}$. Therefore β is non-degenerate and A is symmetric. If K is algebraically closed, then by Artin-Wedderburn and (i) every semisimple K-algebra is symmetric. This even holds for every field K (see Theorem III.7.31).

(iv) Let $K \subseteq L$ be a finite field extension. Obviously there exists a K-linear map $\lambda\colon L \to K$ with $\lambda(1) = 1$. One easily shows that $\beta\colon L \times L \to K$, $(x, y) \mapsto \lambda(xy)$ defines a symmetric, associative, non-degenerate bilinear form. Thus L is a symmetric K-algebra.

(v) The next theorem shows that the algebra $A \subseteq K^{n\times n}$ of upper triangular matrices for $n \geq 2$ is not symmetric (Example II.12.22).

Theorem II.13.4. *Let K be algebraically closed and A symmetric. Then the Cartan matrix of A is symmetric.*

Proof. Let A be symmetric with respect to the bilinear form β. Let $e, f \in A$ be idempotents and $a \in eAf \setminus \{0\}$. Since β is non-degenerate, there exists a $b \in A$ with $\beta(a,b) \neq 0$. It follows

$$0 \neq \beta(af,b) = \beta(a,fb) = \beta(fb,ea) = \beta(fbe,a).$$

Therefore, the linear map $eAf \to \mathrm{Hom}_K(fAe,K)$, $a \mapsto \beta(a,.)$ is injective and $\dim eAf \leq \dim fAe$. For reasons of symmetry, $\dim eAf = \dim fAe$ holds. The assertion follows from Remark II.12.21. □

Remark II.13.5. Let A be a symmetric algebra with bilinear form β.

(i) For $a \in A$, $\beta_a \colon A \to K$, $b \mapsto \beta(a,b)$ is an element of the dual space $A^* := \mathrm{Hom}(A,K)$. Since β is non-degenerate and $\dim A = \dim A^*$ (linear algebra), $A \to A^*$, $a \mapsto \beta_a$ is an isomorphism.

(ii) For a K-basis $e_1, \ldots, e_n$ of A, it is well known that there exists a dual basis $f_1, \ldots, f_n \in A$ with respect to β, i. e. $\beta(e_i, f_j) = \delta_{ij}$ holds for $1 \leq i,j \leq n$ (linear algebra; the associativity of β is not needed for this). For $a = \sum_{i=1}^n a_i e_i \in A$, we have $\beta(a,f_i) = a_i$ and

$$a = \sum_{i=1}^n \beta(a,f_i)e_i = \sum_{i=1}^n \beta(f_i,a)e_i = \sum_{i=1}^n \beta(e_i,a)f_i = \sum_{i=1}^n \beta(a,e_i)f_i. \tag{II.13.1}$$

We consider the linear map $\Gamma \colon A \to A$, $a \mapsto \sum_{i=1}^n e_i a f_i$. For every other pair of dual bases (e_i'), (f_i') of A, we have

$$\sum_{i=1}^n e_i' a f_i' = \sum_{i=1}^n \Big(\sum_{j=1}^n \beta(e_i', f_j)e_j\Big) a f_i' = \sum_{j=1}^n e_j a \sum_{i=1}^n \beta(e_i', f_j) f_i' = \sum_{j=1}^n e_j a f_j.$$

Thus, Γ does not depend on the choice of the bases (but on β). For $b \in A$, we have

$$\Gamma(a)b = \sum_{i=1}^n e_i a \sum_{j=1}^n \beta(f_i b, e_j) f_j = \sum_{j=1}^n \sum_{i=1}^n \beta(f_i, be_j) e_i a f_j = \sum_{j=1}^n be_j a f_j = b\Gamma(a).$$

It follows $\Gamma \colon A \to \mathrm{Z}(A)$. For $z \in \mathrm{Z}(A)$, $z\Gamma(a) = \Gamma(za)$ holds. Therefore, $\Gamma(A) \trianglelefteq \mathrm{Z}(A)$.

Suppose A is also symmetric with respect to a bilinear form β'. According to (i), there exists an $x \in A$ with $\beta(1,a) = \beta'(x,a)$ for all $a \in A$. Because of

$$\beta'(xa - ax, b) = \beta'(x,ab) - \beta'(x,ba) = \beta(a,b) - \beta(b,a) = 0$$

for all $a, b \in A$, we have $x \in \mathrm{Z}(A)$. Furthermore, $\beta'(xe_i, f_j) = \beta'(x, e_i f_j) = \beta(1, e_i f_j) = \beta(e_i, f_j)$, i. e. (xe_i) and (f_i) are dual bases to each other with respect to β'. This shows $\Gamma'(a) := \sum_{i=1}^n xe_i a f_i = \Gamma(xa)$ and $\Gamma'(A) \subseteq \Gamma(A)$. For reasons of symmetry, $\Gamma'(A) = \Gamma(A)$ holds, i. e. $\Gamma(A)$ does not depend on the choice of β.

Definition II.13.6. In the situation of Remark II.13.5, $\Gamma(A)$ is called the *Higman ideal* of $\mathrm{Z}(A)$ (or *projective center* of A). A symmetric algebra A is called *strongly symmetric*, if $\Gamma(A) = \mathrm{Z}(A)$ holds.

Theorem II.13.7. *For every symmetric algebra A, $\mathrm{J}(A)\Gamma(A) = 0$ holds. In particular, every strongly symmetric algebra is semisimple.*

Proof. Let A be symmetric with respect to β. Let $l \geq 1$ with $\mathrm{J}(A)^l = 0$. We choose a K-basis of $\mathrm{J}(A)^{l-1}$ and extend it to a basis of $\mathrm{J}(A)^{l-2}$. We extend this further to a basis of $\mathrm{J}(A)^{l-3}$ etc. In the end, one obtains a basis $e_1, \ldots, e_n$ of $A = \mathrm{J}(A)^0$. Let $f_1, \ldots, f_n$ be the corresponding dual basis with respect to β. Let $x \in \mathrm{J}(A)$ and $1 \leq i \leq n$ be fixed. Then $e_i \in \mathrm{J}(A)^k \setminus \mathrm{J}(A)^{k+1}$ for some $k \geq 0$. For all $a, b \in A$, $axe_ib \in \mathrm{J}(A)^{k+1}$ can be written as a linear combination of e_j with $j < i$. It follows that

$$\beta(xe_ibf_i, a) = \beta(axe_ib, f_i) = 0$$

and $xe_ibf_i = 0$ for $i = 1, \ldots, n$. This shows $x\Gamma(b) = 0$ for all $x \in \mathrm{J}(A)$ and $b \in A$. If A is strongly symmetric, then $\mathrm{J}(A) = \mathrm{J}(A)\mathrm{Z}(A) = \mathrm{J}(A)\Gamma(A) = 0$ holds. □

Remark II.13.8. Every semisimple algebra is symmetric (Theorem III.7.31), but not every symmetric algebra is semisimple (Remark II.13.20).

Lemma II.13.9. *Let $K \subseteq L$ be a finite, separable field extension. Then L is a strongly symmetric K-algebra.*

Proof. According to Theorem II.3.21, $\beta\colon L \times L \to K$, $(a, b) \mapsto S_K^L(ab)$ is a symmetric, associative, non-degenerate bilinear form. According to the primitive element theorem, L has a basis of the form $1, x, \ldots, x^{n-1}$ with $x \in L$. Let

$$\mu = (X - x)\rho = \prod_{i=1}^{d}(X - x_i) \in K[X]$$

be the minimal polynomial of x and $\rho := X^{n-1} + r_{n-1} + \ldots + r_0 \in L[X]$. Let

$$\alpha_k := X^k - \sum_{i=1}^{d} \frac{\mu}{X - x_i} \frac{x_i^k}{\mu'(x_i)} \in \overline{K}[X]$$

for $1 \leq k \leq n-1$ (note $\mu'(x_i) = \prod_{j \neq i}(x_i - x_j) \neq 0$). Obviously, α_k has the roots $x_1, \ldots, x_n$ and $\deg \alpha_k \leq n - 1$. This shows

$$S_K^L\Big(\rho \frac{x^k}{\mu'(x)}\Big) = \sum_{i=1}^{d} \frac{\mu}{X - x_i} \frac{x_i^k}{\mu'(x_i)} = X^k.$$

For the coefficient of X^l on the left side, it therefore holds that

$$S_K^L\Big(r_l \frac{x^k}{\mu'(x)}\Big) = \delta_{kl}$$

for $1 \leq k, l \leq n$. Thus $1, x, \ldots, x^{n-1}$ and $\frac{r_0}{\mu'(x)}, \ldots \frac{r_{n-1}}{\mu'(x)}$ are dual bases to each other with respect to β with

$$\Gamma(1) = \sum_{i=0}^{n-1} \frac{r_i x^i}{\mu'(x)} = \frac{\rho(x)}{\rho(x)} = 1.$$ □

Example II.13.10.

(i) We consider $L := \mathbb{F}_2(X)$ as a 2-dimensional semisimple algebra over $K := \mathbb{F}_2(X^2)$ with basis $\{1, X\}$. Let $\lambda(a + bX) = a$ for $a, b \in K$. Then A is symmetric with respect to $\beta(x, y) = \lambda(xy)$ for $x, y \in L$. Furthermore, $\{1, X^{-1}\}$ is dual to $\{1, X\}$ and $\Gamma(x) = x + XxX^{-1} = 0$ for all $x \in L$. Therefore L is not strongly symmetric.

(ii) Let A be strongly symmetric with respect to β and $B := A^{n\times n}$. For $x, y \in B$, $\hat{\beta}(x,y) := \beta(\mathrm{tr}(xy), 1)$ defines an associative bilinear form on B. Because of

$$\hat{\beta}(x,y) = \beta\Big(\sum_{i,j=1}^{n} x_{ij}y_{ji}, 1\Big) = \sum_{i,j=1}^{n} \beta(x_{ij}, y_{ji}) = \sum_{i,j=1}^{n} \beta(y_{ji}, x_{ij}) = \hat{\beta}(y,x)$$

$\hat{\beta}$ is symmetric. Let $x_{ij} \neq 0$. Then there exists an $a \in A$ with $\beta(x_{ij}, a) \neq 0$. It follows that $\hat{\beta}(x, E_{ji}a) = \beta(\mathrm{tr}(xE_{ji}a), 1) = \beta(x_{ij}, a) \neq 0$. Therefore $\hat{\beta}$ is non-degenerate and B is symmetric. Let $(e_1, \ldots, e_d)$ and $(f_1, \ldots, f_d)$ be dual bases of A with respect to β. Then $(e_iE_{st} : 1 \leq i \leq d,\ 1 \leq s, t \leq n)$ and (f_iE_{ts}) are dual bases with respect to $\hat{\beta}$, because

$$\begin{aligned}\hat{\beta}(e_iE_{st}, f_{i'}E_{t's'}) &= \beta(e_if_{i'}\,\mathrm{tr}(E_{st}E_{t's'}), 1) = \delta_{tt'}\beta(e_if_{i'}\,\mathrm{tr}(E_{ss'}), 1)\\ &= \delta_{ss'}\delta_{tt'}\beta(e_i, f_{i'}) = \delta_{ii'}\delta_{ss'}\delta_{tt'}.\end{aligned}$$

For $a \in A$ we have

$$\hat{\Gamma}(aE_{11}) = \sum_{i=1}^{d}\sum_{s,t=1}^{n} e_iaf_iE_{st}E_{11}E_{ts} = \sum_{i=1}^{d}\sum_{s=1}^{n} e_iaf_iE_{ss} = \Gamma(a)1_n.$$

Thus B is strongly symmetric.

(iii) Let $A_1, \ldots, A_n$ be strongly symmetric algebras and $(e_{ik})_{k=1}^{n_i}$, $(f_{ik})_{k=1}^{n_i}$ a pair of dual bases of A_i. Then

$$\bigcup_{i=1}^{n}\big\{(0, \ldots, e_{ik}, \ldots, 0) : 1 \leq k \leq n_i\big\}, \qquad \bigcup_{i=1}^{n}\big\{(0, \ldots, f_{ik}, \ldots, 0) : 1 \leq k \leq n_i\big\}$$

is a pair of dual bases of $A := A_1 \times \ldots \times A_n$. Let $\Gamma_i \colon A_i \to \mathrm{Z}(A_i)$ be the map from Remark II.13.5. Then $\Gamma \colon A \to \mathrm{Z}(A)$, $(a_1, \ldots, a_n) \mapsto (\Gamma_1(a_1), \ldots, \Gamma(a_n))$ is the corresponding map for A. Consequently $A_1 \times \ldots \times A_n$ is strongly symmetric.

(iv) Let K be finite or algebraically closed and A a semisimple K-algebra. According to Artin-Wedderburn, Lemma II.12.6, Theorem II.8.7, Example II.3.3, (ii) and (iii), A is strongly symmetric.

Lemma II.13.11. *Let S be a strongly symmetric algebra. Let $I \trianglelefteq A$ with $I^2 = 0$ and $\varphi \colon S \to A/I$ be a homomorphism of algebras. Then there exists a homomorphism $\hat{\varphi} \colon S \to A$ with $\hat{\varphi}(s) + I = \varphi(s)$ for all $s \in S$. If $\hat{\psi} \colon S \to A$ is also a homomorphism with $\hat{\psi}(s) + I = \varphi(s)$ for $s \in S$, then there exists an $x \in \mathrm{J}(A)$ with $\hat{\varphi}(s) = (1+x)\hat{\psi}(s)(1+x)^{-1}$ for all $s \in S$.*

Proof. Let $s, t, u \in S$. Obviously there exists a K-linear map $\varphi_0 \colon S \to A$ with $\varphi_0(1) = 1$ and $\varphi_0(s) + I = \varphi(s)$ for all $s \in S$. We define the bilinear map $\tau(s,t) := \varphi_0(st) - \varphi_0(s)\varphi_0(t) \in I$. Then

$$\begin{aligned}\tau(st,u) - \varphi_0(s)\tau(t,u) &= \varphi_0(stu) - \varphi_0(st)\varphi_0(u) - \varphi_0(s)\varphi_0(tu) + \varphi_0(s)\varphi_0(t)\varphi_0(u)\\ &= \tau(s,tu) - \tau(s,t)\varphi_0(u).\end{aligned} \tag{II.13.2}$$

By assumption, S is strongly symmetric with respect to a bilinear form β and there exists a pair of dual bases $(e_1, \ldots, e_n)$, $(f_1, \ldots, f_n)$ with respect to β. Furthermore, there exists a $c \in S$ with $\Gamma(c) = \sum_{i=1}^{n} e_icf_i = 1$. We define

$$\hat{\varphi}(s) := \varphi_0(s) + \sum_{i=1}^{n} \tau(s, e_ic)\varphi_0(f_i) \equiv \varphi_0(s) \pmod{I}.$$

Obviously φ_0 is linear and $\hat{\varphi}(1) = \varphi_0(1) = 1$. One calculates

$$\begin{aligned}
\hat{\varphi}(st) - \hat{\varphi}(s)\hat{\varphi}(t) &= \varphi_0(st) - \varphi_0(s)\varphi_0(t) + \sum_{i=1}^{n} \big(\tau(st, e_ic) - \varphi_0(s)\tau(t, e_ic)\big)\varphi_0(f_i) \\
&\quad - \sum_{i=1}^{n} \overbrace{\tau(s, e_ic)}^{\in I} \overbrace{\varphi_0(f_i)\varphi_0(t)}^{\equiv \varphi_0(f_it) \,(\mathrm{mod}\ I)} \\
&\overset{\text{(II.13.2)}}{=} \tau(s,t) + \sum_{i=1}^{n} \tau(s, te_ic)\varphi_0(f_i) - \sum_{i=1}^{n} \tau(s,t)\varphi_0(e_ic)\varphi_0(f_i) - \sum_{i=1}^{n} \tau(s, e_ic)\varphi_0(f_it) \\
&\overset{\text{(II.13.1)}}{=} \tau(s,t) + \sum_{i,j=1}^{n} \tau\big(s, \beta(f_j, te_i)e_jc\big)\varphi_0(f_i) - \sum_{i=1}^{n} \tau(s,t)\varphi_0(e_icf_i) \\
&\quad - \sum_{i,j=1}^{n} \tau(s, e_ic)\varphi_0\big(\beta(f_it, e_j)f_j\big) \\
&\overset{i \leftrightarrow j}{=} \tau(s,t) - \tau(s,t)\varphi_0(1).
\end{aligned}$$

Thus $\hat{\varphi}\colon S \to A$ is a homomorphism of algebras which coincides with φ on A/I.

For the second statement, let $\hat{\varphi}, \hat{\psi}\colon S \to A$ be homomorphisms with $\eta(s) := \hat{\varphi}(s) - \hat{\psi}(s) \in I$. Obviously η is linear and

$$\eta(st) = \hat{\varphi}(s)\big(\hat{\varphi}(t) - \hat{\psi}(t)\big) + \big(\hat{\varphi}(s) - \hat{\psi}(s)\big)\hat{\psi}(t) = \hat{\varphi}(s)\eta(t) + \eta(s)\hat{\psi}(t). \tag{II.13.3}$$

We define

$$x := \sum_{i=1}^{n} \hat{\varphi}(e_ic)\eta(f_i) \in I$$

and $a := 1 - x \in A$. Because of $(1-x)(1+x) = 1 - x^2 = 1$, we have $a \in A^\times$. One calculates

$$\begin{aligned}
\hat{\varphi}(s)x - x\hat{\psi}(s) &= \sum_{i=1}^{n} \hat{\varphi}(se_ic)\eta(f_i) - \sum_{i=1}^{n} \hat{\varphi}(e_ic)\eta(f_i)\hat{\psi}(s) \\
&\overset{\text{(II.13.3)}}{=} \sum_{i,j=1}^{n} \hat{\varphi}\big(\beta(f_j, se_i)e_jc\big)\eta(f_i) - \sum_{i=1}^{n} \eta(e_icf_i)\hat{\psi}(s) + \sum_{i=1}^{n} \eta(e_ic)\hat{\psi}(f_is) \\
&= \sum_{i,j=1}^{n} \hat{\varphi}(e_jc)\eta\big(\beta(f_js, e_i)f_i\big) - \eta(1)\hat{\psi}(s) + \sum_{i=1}^{n} \eta(e_ic)\hat{\psi}(f_is) \\
&= \sum_{j=1}^{n} \hat{\varphi}(e_jc)\eta(f_js) + \sum_{i=1}^{n} \eta(e_ic)\hat{\psi}(f_is) \overset{\text{(II.13.3)}}{=} \sum_{i=1}^{n} \eta(e_icf_is) = \eta(s) = \hat{\varphi}(s) - \hat{\psi}(s).
\end{aligned}$$

This shows $a\hat{\psi}(s) = \hat{\varphi}(s)a$ for all $s \in S$. □

Theorem II.13.12 (Wedderburn-Malcev)**.** *Let $A/\mathrm{J}(A)$ be strongly symmetric. Then there exists a semisimple subalgebra $B \subseteq A$ with $A = B \oplus \mathrm{J}(A)$. If B' is also a subalgebra with $A = B' \oplus \mathrm{J}(A)$, then there exists an $x \in \mathrm{J}(A)$ such that $B = (1+x)B'(1+x)^{-1}$.*

Proof. Induction on $\dim A$. Let $J := \mathrm{J}(A)$.

Existence: First, assume $J^2 \neq 0$. By induction, there exists a subalgebra $B/J^2 \subseteq A/J^2$ with $A/J^2 = B/J^2 + J/J^2$. Because of $B/J^2 \cong (A/J^2)/(J/J^2) \cong A/J$, B/J^2 is semisimple. In particular, $\mathrm{J}(B) \subseteq J^2$. Since $J^2 \trianglelefteq B$ is nilpotent, $\mathrm{J}(B) = J^2$ holds. Applying induction again yields a subalgebra $B_1 \subseteq B$ with $B = B_1 \oplus J^2$. Overall, $A = B + J = B_1 + J$ and $B_1 \cap J \subseteq \mathrm{J}(B_1) = 0$. Thus, we can assume $J^2 = 0$. We apply Lemma II.13.11 to $\mathrm{id}\colon S \to A/J$. This yields a homomorphism $\varphi\colon S \to A$ with $\varphi(s) + J = s$ for $s \in S$. Now $B := \varphi(S)$ is a subalgebra of A with $A = B + J$. For $\varphi(a+J) \in B \cap J$, it follows that $a \in J$ and $\varphi(a + J) = 0$. Thus $A = B \oplus J$ and $B \cong A/J = S$ is semisimple.

Uniqueness: As above, let first $J^2 \neq 0$. Then

$$A/J^2 = (B + J^2)/J^2 \oplus J/J^2 = (B' + J^2) \oplus J/J^2.$$

By induction, there exists $\overline{x} = x + J^2 \in (1 + J)/J^2$ with $\overline{x}((B + J^2)/J^2)\overline{x}^{-1} = (B' + J^2)/J^2$. Then $xBx^{-1} \oplus J^2 = B' \oplus J^2$ holds. By induction, there exists $y \in 1 + J^2$ such that $yxB(yx)^{-1} = B'$ and $yx \in 1 + J$. Thus, we can assume $J^2 = 0$. From the isomorphisms $\varphi\colon B \to S$, $b \mapsto b + J$ and $\psi\colon B' \to S$, $b' \mapsto b' + J$, one obtains homomorphisms

$$\hat{\varphi}\colon S \xrightarrow{\varphi^{-1}} B \hookrightarrow A,$$
$$\hat{\psi}\colon S \xrightarrow{\psi^{-1}} B' \hookrightarrow A$$

with $\hat{\varphi}(s) + J = s + J = \hat{\psi}(s) + I$. By Lemma II.13.11, there exists an $x \in J$ with $\hat{\varphi}(s) = (1+x)\hat{\psi}(s)(1+x)^{-1}$ for all $s \in S$. This shows $B = \varphi^{-1}(S) = (1 + x)\psi^{-1}(S)(1 + x)^{-1} = (1 + x)B'(1 + x)^{-1}$. □

Example II.13.13.

(i) The Wedderburn-Malcev Theorem holds for all algebras if K is finite or algebraically closed (Example II.13.10). One can show that the theorem also holds for all perfect fields (see Corollary A.8.11).

(ii) We construct counterexamples for imperfect fields. For this, let $K := \mathbb{F}_2(X)$, $I := (Y^4 + X^2) \trianglelefteq K[Y]$ and $A := K[Y]/I$. According to the correspondence theorem, $\mathrm{J}(A) = (\varphi)/I$ for some $\varphi \in K[Y]$. From $\varphi \mid Y^4 + X^2 = (Y^2 + X)^2$ it follows that $\varphi = Y^2 + X$ and $\varphi^2 \equiv 0 \pmod{I}$. Suppose there exists a subalgebra $B \subseteq A$ with $A = B \oplus \mathrm{J}(A)$. Then there exist $b \in B$ and $c \in \mathrm{J}(A)$ with $Y + I = b + c$. Thus $Y^2 + I = b^2 \in B$ holds. Because of $X + I = X1 + I \in B$, it now follows that $\varphi + I \in B \cap \mathrm{J}(A) = 0$. This contradicts $\dim_K A = 4$.

(iii) Now let $K := \mathbb{F}_2(X^2)$, $L := \mathbb{F}_2(X)$ and $A := L[Y]/(Y^2)$ as a 4-dimensional K-algebra. Obviously $\mathrm{J}(A) = (Y)/(Y^2)$ and $A/\mathrm{J}(A) \cong L$. Certainly $B := (L + (Y^2))/(Y^2) \subseteq A$ is a subalgebra with $A = B \oplus \mathrm{J}(A)$. Because of $(X + Y)^2 = X^2 + Y^2 \in K + (Y^2)$,

$$B' := \big(K + K(X + Y) + (Y^2)\big)/(Y^2) \subseteq A$$

is also a subalgebra with $A = B' \oplus \mathrm{J}(A)$ and $B \neq B'$. Since A is abelian, B and B' cannot be conjugate.

(iv) Let K be algebraically closed. If A is local, then $K1$ is the only subalgebra with $A = K1 \oplus \mathrm{J}(A)$ (Theorem II.12.11).

(v) Let K be algebraically closed. Let A be a basic algebra and $1 = e_1 + \ldots + e_n$ a decomposition into pairwise primitive idempotents. Then $B := Ke_1 + \ldots + Ke_n$ is a subalgebra with $A = B \oplus \mathrm{J}(A)$.

Remark II.13.14. In contrast to subalgebras, by Nakayama's Lemma there exists *no* left ideal $I \lhd A$ with $A = I \oplus \mathrm{J}(A)$. For subalgebras, however, the following weaker statement holds.

Theorem II.13.15. *Let B be a subalgebra of A with $A = B + \mathrm{J}(A)^2$. Then $B = A$ holds.*

Proof. According to Dedekind (for vector spaces), $\mathrm{J}(A) = (B + \mathrm{J}(A)^2) \cap \mathrm{J}(A) = (B \cap \mathrm{J}(A)) + \mathrm{J}(A)^2$ holds. Suppose inductively that $\mathrm{J}(A)^n = (B \cap \mathrm{J}(A))^n + \mathrm{J}(A)^{n+1}$ has already been shown for some $n \in \mathbb{N}$. Then it follows that

$$\begin{aligned}\mathrm{J}(A)^{n+1} &= \big((B \cap \mathrm{J}(A)) \cap \mathrm{J}(A)\big)\big((B \cap \mathrm{J}(A))^n + \mathrm{J}(A)^{n+1}\big) \\ &= (B \cap \mathrm{J}(A))^{n+1} + (B \cap \mathrm{J}(A))\mathrm{J}(A)^{n+1} + \mathrm{J}(A)(B \cap \mathrm{J}(A))^n + \mathrm{J}(A)^{n+2} \\ &= (B \cap \mathrm{J}(A))^{n+1} + \mathrm{J}(A)^{n+2}.\end{aligned}$$

This equation thus holds for all $n \in \mathbb{N}$. Since $\mathrm{J}(A)$ is nilpotent, there exists an $n \in \mathbb{N}$ with $\mathrm{J}(A)^n = 0$. It follows that

$$A = B + \mathrm{J}(A)^2 = B + (B \cap \mathrm{J}(A))^2 + \mathrm{J}(A)^3 = B + \mathrm{J}(A)^3 = \ldots = B + \mathrm{J}(A)^n = B. \qquad \square$$

Remark II.13.16. Let A be symmetric with respect to a bilinear form β.

(i) For $B \subseteq A$ let

$$B^\perp := \{a \in A : \beta(a, B) = 0\} \subseteq A$$

(a subspace). Since β is non-degenerate, for all subspaces $B, C \subseteq A$ (linear algebra) the following holds:

$$(B^\perp)^\perp = B, \qquad B^\perp + C^\perp = (B \cap B)^\perp, \qquad (B + C)^\perp = B^\perp \cap C^\perp,$$
$$B \subseteq C \iff C^\perp \subseteq B^\perp, \qquad \dim B + \dim B^\perp = \dim A.$$

(ii) If $I \trianglelefteq A$, then also $I^\perp \trianglelefteq A$, because

$$\beta(I^\perp A, I) = \beta(I^\perp, AI) = \beta(I^\perp, I) = 0 = \beta(I^\perp, IA) = \beta(AI^\perp, I).$$

(iii) For $I \trianglelefteq A$ and $B \subseteq A$ it holds that

$$B \subseteq I^\perp \iff \beta(BI, A) = \beta(B, IA) = \beta(B, I) = 0 \iff BI = 0 \iff IB = 0.$$

(iv) According to Exercise II.38, $\mathrm{Soc}(A)$ is the largest semisimple submodule of the regular A-module.

Theorem II.13.17 (Nakayama)**.** *For every symmetric algebra A the following holds:*

(i) $\mathrm{Z}(A) = \gamma(A)^\perp$.

(ii) $\mathrm{Soc}(A) = \mathrm{J}(A)^\perp$.

(iii) There exists a $z \in \mathrm{Z}(A)$ *with* $\mathrm{J}(A)^\perp = Az$.

(iv) $\mathrm{J}(A) = \big\{a \in A : a(\gamma(A) + \mathrm{J}(A))^\perp = 0\big\}$.

Proof.

(i) It holds that

$$\begin{aligned}z \in \mathrm{Z}(A) &\iff \forall a, b \in A : \beta(az - za, b) = 0 \iff \forall a, b \in A : \beta(z, ba) = \beta(z, ab) \\ &\iff \forall a, b \in A : \beta(z, ba - ab) = 0 \iff z \in \gamma(A)^\perp.\end{aligned}$$

(ii) From Lemma II.8.13 it follows that $\mathrm{J}(A)\,\mathrm{Soc}(A) = \mathrm{J}(\mathrm{Soc}(A)) = 0$, since $\mathrm{Soc}(A)$ is semisimple. Thus $\mathrm{Soc}(A) \subseteq J(A)^\perp$ holds by Remark II.13.16. Conversely, $\mathrm{J}(\mathrm{J}(A)^\perp) = \mathrm{J}(A)^\perp \mathrm{J}(A) = 0$, i. e. $\mathrm{J}(A)^\perp$ is a semisimple submodule of the regular A-module. This shows $\mathrm{J}(A)^\perp \subseteq \mathrm{Soc}(A)$.

(iii) According to Theorem III.7.31, $\overline{A} := A/\mathrm{J}(A)$ is symmetric with respect to a bilinear form $\overline{\beta}$.[1] Since the map $A \to K$, $a \mapsto \overline{\beta}(\overline{a}, 1)$ is linear, there exists by Remark II.13.5 a $z \in A$ with $\overline{\beta}(\overline{a}, 1) = \beta(a, z)$ for all $a \in A$. Because of $\beta(\mathrm{J}(A), Az) = \beta(\mathrm{J}(A), z) = \overline{\beta}(0, 1) = 0$, we have $Az \subseteq \mathrm{J}(A)^\perp$. For $x \in (Az)^\perp$ and $a \in A$ it holds that

$$\overline{\beta}(\overline{x}, \overline{a}) = \overline{\beta}(\overline{x}\overline{a}, 1) = \beta(xa, z) = \beta(x, az) = 0.$$

Since $\overline{\beta}$ is non-degenerate, it follows that $x \in \mathrm{J}(A)$ and $\mathrm{J}(A)^\perp \subseteq Az$. For all $a, b \in A$ it holds that

$$\beta(ab - ba, z) = \overline{\beta}(\overline{ab}, 1) - \overline{\beta}(\overline{ba}, 1) = \overline{\beta}(\overline{a}, \overline{b}) - \overline{\beta}(\overline{b}, \overline{a}) = 0$$

and $z \in \gamma(A)^\perp = \mathrm{Z}(A)$.

(iv) From $(\gamma(A) + \mathrm{J}(A))^\perp \subseteq \mathrm{J}(A)^\perp$ it follows that $\mathrm{J}(A) \subseteq \{a \in A : a(\gamma(A) + \mathrm{J}(A))^\perp = 0\} =: T$ by Remark II.13.16. According to (iii) there exists a $z \in \mathrm{Z}(A)$ with $\mathrm{J}(A)^\perp = Az$. According to (i) it holds that $z \in \gamma(A)^\perp \cap \mathrm{J}(A)^\perp = (\gamma(A) + \mathrm{J}(A))^\perp$. This shows $\beta(T, Az) = \beta(zT, A) = 0$ and $T \subseteq (Az)^\perp = \mathrm{J}(A)$. □

Remark II.13.18.

(i) For symmetric algebras A, one calls

$$R(A) := (\gamma(A) + \mathrm{J}(A))^\perp = \mathrm{Z}(A) \cap \mathrm{Soc}(A) \trianglelefteq \mathrm{Z}(A)$$

the *Reynolds ideal* of $\mathrm{Z}(A)$. According to Theorem II.13.7 it holds that $\mathrm{J}(A)\Gamma(A) = 0$. From Remark II.13.16 it follows that $\Gamma(A) \subseteq \mathrm{J}(A)^\perp \cap \mathrm{Z}(A) = R(A)$.

(ii) The equation $\dim \mathrm{Soc}(A) = \dim A/\mathrm{J}(A)$ following from Theorem II.13.17 is in general false for non-symmetric algebras. For

$$A := \left\{ \begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} : a, b, c \in K \right\} \subseteq K^{3\times 3}$$

it holds for example that $\mathrm{Soc}(A) = \mathrm{J}(A) = KE_{12} + KE_{13}$, thus $\dim \mathrm{Soc}(A) = 2 > 1 = \dim A/\mathrm{J}(A)$.

(iii) We now define a particularly important class of symmetric algebras.

Definition II.13.19. For a finite group G, let KG be the set of all mappings $G \to K$. By

$$\begin{aligned} (\alpha + \beta)(g) &:= \alpha(g) + \beta(g) \qquad (\alpha, \beta \in KG,\ g \in G), \\ (\alpha\beta)(g) &:= \sum_{h \in G} \alpha(h)\beta(h^{-1}g) \qquad (\textit{convolution}), \\ (\lambda\alpha)(g) &:= \lambda\alpha(g) \qquad (\lambda \in K) \end{aligned}$$

[1] Since the theorem is proven only later, one could assume at this point that K is algebraically closed and refer to Example II.13.3. This special case is sufficient for the application in Theorem III.3.10.

KG becomes a K-algebra. The associativity of multiplication follows from

$$\begin{aligned}((\alpha\beta)\gamma)(g) &= \sum_{h\in G}(\alpha\beta)(h)\gamma(h^{-1}g) = \sum_{h\in G}\sum_{k\in G}\alpha(k)\beta(k^{-1}h)\gamma(h^{-1}g)\\ &= \sum_{\substack{x,y,z\in G\\ xyz=g}}\alpha(x)\beta(y)\gamma(z) = \ldots = (\alpha(\beta\gamma))(g)\end{aligned}$$

for $\alpha, \beta, \gamma \in KG$ and $g \in G$ (the other axioms are easy). KG is called the *group algebra* of G over K. Its elements are usually written as formal linear combinations $\alpha = \sum_{g\in G}\alpha_g g$, where $\alpha_g = \alpha(g) \in K$. The multiplication then works as with polynomials (cf. Exercise II.66):

$$\sum_{g\in G}\alpha_g g \cdot \sum_{g\in G}\beta_g g = \sum_{g,h\in G}\alpha_g\beta_h gh = \sum_{g\in G}\Big(\sum_{h\in G}\alpha_h\beta_{h^{-1}g}\Big)g.$$

Remark II.13.20.

(i) By identifying $g \in G$ with $1_K g$, we can view G as a subset of KG. Then 1_G is the identity element of KG and G is a K-basis of KG. In particular, $\dim_K KG = |G|$. Furthermore, KG is commutative if and only if G is abelian.

(ii) Let $A := KG$. For $a := \sum \alpha_g g \in A$ and $b := \sum_g \beta_g g \in A$ let

$$\beta(a,b) := \sum_{g\in G}\alpha_g\beta_{g^{-1}}.$$

Then $\beta\colon A \times A \to K$ is a symmetric, non-degenerate bilinear form. For $c := \sum_g \gamma_g g \in A$ it holds that

$$\beta(ab,c) = \sum_{g\in G}\Big(\sum_{h\in G}\alpha_h\beta_{h^{-1}g}\Big)\gamma_{g^{-1}} = \sum_{h\in G}\alpha_h\Big(\sum_{g\in G}\beta_{h^{-1}g}\gamma_{g^{-1}}\Big) = \beta(a,bc).$$

Therefore β is associative and A is a symmetric algebra. Obviously $(g)_{g\in G}$, $(g^{-1})_{g\in G}$ is a pair of dual bases with respect to β. For the mapping γ from Remark II.13.5, $\gamma(1) = |G|$ holds. If $\operatorname{char} K \nmid |G|$, then A is strongly symmetric.

Example II.13.21. For $x := (1,2) + (1,3) \in \mathbb{F}_2 S_3$ it holds that

$$x^2 = (1,2)^2 + (1,2)(1,3) + (1,3)(1,2) + (1,3)^2 = 1 + (1,3,2) + (1,2,3) + 1 = (1,3,2) + (1,2,3).$$

Lemma II.13.22. *The mapping*

$$\begin{aligned}&\nu\colon KG \to K,\\ &\sum_{g\in G}\alpha_g g \mapsto \sum_{g\in G}\alpha_g\end{aligned}$$

is an epimorphism of K-algebras with

$$I(KG) := \operatorname{Ker}(\nu) = \sum_{g\in G\setminus\{1\}} K(g-1).$$

Proof. Certainly $\nu(1) = 1$ and $\nu(\alpha + \beta) = \nu(\alpha) + \nu(\beta)$ for $\alpha, \beta \in KG$. Furthermore,

$$\nu(\alpha\beta) = \sum_{g\in G}\sum_{h\in G} \alpha_h\beta_{h^{-1}g} = \sum_{g,h\in G} \alpha_g\beta_h = \sum_{g\in G} \alpha_g \cdot \sum_{h\in G} \beta_h = \nu(\alpha)\nu(\beta).$$

Finally, $\nu(\lambda\alpha) = \lambda\nu(\alpha)$ for $\lambda \in K$ also holds. Thus ν is an epimorphism of algebras.

According to the homomorphism theorem (for vector spaces), $\dim_K I(KG) = \dim_K KG - \dim_K K = |G| - 1$. Obviously, the elements $g - 1$ for $g \in G \setminus \{1\}$ lie in $I(KG)$. Since G is a K-basis of KG, the elements $g - 1$ are linearly independent. They thus form a basis of $I(KG)$. □

Definition II.13.23. One calls $\nu\colon KG \to K$ the *augmentation map* and $I(KG)$ the *augmentation ideal* of KG. Furthermore, one calls $KG/I(KG) \simeq K$ the *trivial* KG-module.

Remark II.13.24.

(i) Attention: For arbitrary rings, we had called the module 0 trivial.

(ii) The existence of the trivial module distinguishes group algebras from arbitrary algebras. For example, $K^{2\times 2}$ cannot be a group algebra. Furthermore, a group algebra KG is local if and only if K is the only simple A-module up to isomorphism. In this case, $\mathrm{J}(KG) = I(KG)$.

(iii) The trivial module is also found as a submodule of KG: $K\sum_{g\in G} g$.

(iv) According to Theorem II.8.26, the trivial module can be assigned to exactly one block B_0 of KG. One calls B_0 the *principal block* of KG. For an arbitrary block B of KG, it holds that

$$B = B_0 \iff BK \neq 0 \iff B1 \neq 0 \iff \nu(B) \neq 0 \iff \nu(B) = K.$$

Theorem II.13.25 (Maschke)**.** *KG is semisimple if and only if* $\operatorname{char} K$ *is not a divisor of $|G|$. In particular, KG is semisimple if* $\operatorname{char} K = 0$.

Proof.

⇒: Let KG be semisimple, i. e. the regular KG-module is semisimple. In particular, $I := I(KG)$ has a complement J. Here J is a left ideal of KG with $KG = I \oplus J$. According to Lemma II.13.22, J is one-dimensional, say $J = K\alpha$ with $\alpha = \sum_{g\in G} \alpha_g g \in KG$. For each $h \in G$,

$$(h - 1)\alpha \in I\alpha \cap (h - 1)J \subseteq I \cap J = 0,$$

i. e. $\sum_{g\in G} \alpha_g hg = h\alpha = \alpha = \sum_{g\in G} \alpha_g g$. It follows that $\alpha_g = \alpha_{hg}$ for all $h \in H$. This shows $\alpha_g = \alpha_1$ for all $g \in G$. In particular, $|G|\alpha_1 = \nu(\alpha) \neq 0$ and $\operatorname{char} K \nmid |G|$.

⇐: Now let $\operatorname{char} K \nmid |G|$ and M be a left ideal of KG. According to Corollary II.2.3, there exists a K-subspace $M' \subseteq KG$ with $KG = M \oplus M'$ (however, M' is not necessarily a left ideal). Let $\pi\colon KG \to M$ be the projection and

$$f\colon KG \to M,$$
$$\alpha \mapsto \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}\alpha)$$

(this is well-defined because $|G| \neq 0$ in K). Certainly f is K-linear. For $h \in G$, we additionally have

$$f(h\alpha) = \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}h\alpha) = \frac{1}{|G|} \sum_{g \in G} hh^{-1}g\pi(g^{-1}h\alpha) = h\frac{1}{|G|} \sum_{x \in G} x\pi(x^{-1}\alpha) = hf(\alpha),$$

i. e. f is KG-linear. In particular, $N := \operatorname{Ker}(f)$ is a left ideal of KG. For $m \in M$, we have

$$f(m) = \frac{1}{|G|} \sum_{g \in G} g\pi(\underbrace{g^{-1}m}_{\in M}) = \frac{1}{|G|} \sum_{g \in G} gg^{-1}m = m.$$

This shows $f(KG) = M$ and the homomorphism theorem yields $\dim_K M + \dim_K N = \dim_K KG$. For $m \in M \cap N$, we also have $m = f(m) = 0$. Thus $KG = M \oplus N$ and KG is semisimple. □

Remark II.13.26. Let G be a finite group and K algebraically closed with $\operatorname{char} K \nmid |G|$. By Maschke, KG is semisimple. From Remark II.12.3 and Lemma II.12.6 it follows that

$$\boxed{KG \cong K^{d_1 \times d_1} \times \ldots \times K^{d_k \times d_k},}$$

where $d_1, \ldots, d_k$ are the dimensions of the simple KG-modules. In particular,

$$|G| = \dim_K KG = d_1^2 + \ldots + d_k^2.$$

Example II.13.27. By the fundamental theorem of algebra, $K = \mathbb{C}$ is algebraically closed.

(i) If G is abelian, then $\mathbb{C}G$ is commutative and $d_1 = \ldots = d_k = 1$ holds in Remark II.13.26. This shows $\mathbb{C}G \cong \mathbb{C}^{|G|}$.

(ii) As is well known, $G = S_3$ is non-abelian. Therefore $d_i > 1$ for at least one i (otherwise $\mathbb{C}G$ would be commutative). Because of $6 = |G| = d_1^2 + \ldots + d_k^2$, it follows that $k = 3$ and

$$\mathbb{C}S_3 \cong \mathbb{C}^{2\times 2} \times \mathbb{C}^2.$$

Definition II.13.28. For a conjugacy class C of G, let $C^+ := \sum_{g \in C} g \in KG$ be the *class sum* of C.

Theorem II.13.29. *The class sums form a K-basis of the center $\mathrm{Z}(KG)$. In particular,*

$$\dim_K \mathrm{Z}(KG) = k(G)$$

is the class number of G.

Proof. Let C be a conjugacy class of G. For $g \in G$ it holds that

$$gC^+ = \sum_{c \in C} gc = \sum_{c \in C} gcg^{-1}g = \sum_{d \in C} dg = C^+g.$$

This shows $C^+ \in \mathrm{Z}(KG)$.

Conversely, let $\alpha = \sum_{g \in G} \alpha_g g \in \mathrm{Z}(KG)$. For $h \in G$ it then holds that

$$\alpha = h\alpha h^{-1} = \sum_{g \in G} \alpha_g hgh^{-1}$$

and $\alpha_g = \alpha_{hgh^{-1}}$. Therefore, α is constant on the conjugacy classes of G. Consequently, α is a K-linear combination of the class sums. Since distinct conjugacy classes are disjoint, the class sums are linearly independent. □

Remark II.13.30. Over $\mathbb{C}$ it holds that

$$\mathrm{Z}(\mathbb{C}G) \cong \mathrm{Z}(\mathbb{C}^{d_1\times d_1} \times \ldots \times \mathbb{C}^{d_k\times d_k}) = \mathrm{Z}(\mathbb{C}^{d_1\times d_1}) \times \ldots \times \mathrm{Z}(\mathbb{C}^{d_k\times d_k}) \overset{\text{II.12.5}}{=} \mathbb{C}1_{d_1} \times \ldots \times \mathbb{C}1_{d_k} \cong \mathbb{C}^k.$$

Therefore, $k = \dim \mathrm{Z}(\mathbb{C}G) = k(G)$ is also the number of simple $\mathbb{C}G$-modules up to isomorphism. Thus, $(\mathbb{C}G)^b \cong \mathbb{C}^{k(G)}$ is the basic algebra of $\mathbb{C}G$.

Example II.13.31. We determine the conjugacy classes of $G = A_4$. Certainly $\langle(1,2,3)\rangle \in \mathrm{Syl}_3(G)$. By Sylow, every element $g \in G$ of order 3 is conjugate to $(1,2,3)$ or to $(1,2,3)^2 = (1,3,2)$. These two 3-cycles are on the other hand not conjugate, because otherwise the corresponding cosets in the abelian group $G/V_4 \cong C_3$ would also be conjugate (Exercise I.16). Therefore, $(1,2,3)$ and $(1,3,2)$ represent all conjugacy classes of elements of order 3 in G. The elements of order 2 in G all lie in V_4 and are mapped to each other by conjugation with $(1,2,3)$. Therefore, $V_4 \setminus \{1\}$ is another conjugacy class. As is well known, G has no elements of order 6 or 12. Together with $\{1\}$ we have therefore found all conjugacy classes. Thus $k(G) = 4$ and $12 = |G| = d_1^2 + \ldots + d_4^2$ for $d_1, \ldots, d_4 \in \mathbb{N}$. A simple case distinction yields $d_1 = 3$ and $d_2 = d_3 = d_4 = 1$. One obtains

$$\mathbb{C}A_4 \cong \mathbb{C}^{3\times 3} \times \mathbb{C}^3.$$

II.14 Representations and Characters

Remark II.14.1. In this chapter, for the sake of simplicity, we consider only finite groups G and their group algebras over fields of characteristic 0. We will see that all information about the modules of $\mathbb{C}G$ can be read from a complex matrix of format $k(G) \times k(G)$. With this, deep theorems about finite groups can be proven.

Definition II.14.2. A *representation* of *degree* $n \in \mathbb{N}$ of G over a field K (briefly a *K-representation*) is a group homomorphism $\Delta\colon G \to \mathrm{GL}(n, K)$. If K is not mentioned, we assume $K = \mathbb{C}$.

Remark II.14.3.

(i) Every representation $\Delta\colon G \to \mathrm{GL}(n, K)$ extends to a homomorphism of algebras:

$$\begin{aligned} &\Delta\colon KG \to K^{n\times n}, \\ &\sum_{g\in G} \alpha_g g \mapsto \sum_{g\in G} \alpha_g \Delta(g). \end{aligned}$$

For $v \in V_\Delta := K^{n\times 1}$ and $\alpha \in KG$ we define

$$\alpha v := \Delta(\alpha)v \in V_\Delta.$$

One easily shows that V_Δ becomes a KG-module in this way.

(ii) Conversely, let a finite-dimensional KG-module M be given. Every $g \in G$ induces a map $f_g \in \mathrm{End}_K(M)$ by $f_g(m) := gm$ for $m \in M$. Because of

$$(f_g \circ f_{g^{-1}})(m) = g(g^{-1}m) = (gg^{-1})(m) = 1m = m$$

for all $m \in M$, f_g is invertible, i. e. $f_g \in \mathrm{GL}(M)$. By choosing a K-basis of M, one obtains a representation $G \to \mathrm{GL}(n, K)$, $g \mapsto f_g$. In this way, representations of G and finite-dimensional KG-modules correspond to each other.

Example II.14.4.

(i) The *trivial* representation $G \to \mathrm{GL}(1, K) = K^\times$, $g \mapsto 1$ belongs to the trivial module and extends to the augmentation map $KG \to K$.

(ii) Let Ω be a G-set and V a K-vector space with basis Ω. Through the action of G on Ω, V becomes a KG-module, which is called a *permutation module*. The corresponding *permutation representation* $G \to \mathrm{GL}(V)$ is described by permutation matrices (each $g \in G$ permutes the basis Ω). In the special case $\Omega = G$ with the action by left multiplication, one obtains the regular KG-module. The *regular* representation essentially corresponds to the homomorphism $G \to \mathrm{Sym}(G)$ from Cayley's theorem.

(iii) If Δ is a K-representation, then so is Δ^* with $\Delta^*(g) := \Delta(g^{-1})^{\mathrm{t}}$, because

$$\Delta\big((gh)^{-1}\big)^{\mathrm{t}} = \Delta(h^{-1}g^{-1})^{\mathrm{t}} = \big(\Delta(h^{-1})\Delta(g^{-1})\big)^{\mathrm{t}} = \Delta(g^{-1})^{\mathrm{t}}\Delta(h^{-1})^{\mathrm{t}}$$

for $g, h \in G$. One calls Δ^* the *dual* representation to Δ.

(iv) If $\Delta\colon G \to \mathrm{GL}(n, K)$ is a representation and $H \leq G$, then the *restriction* $\Delta_H\colon H \to \mathrm{GL}(n, K)$, $h \mapsto \Delta(h)$ is a representation of H.

(v) If $\Delta\colon G \to \mathrm{GL}(n, K)$ and $\Gamma\colon G \to \mathrm{GL}(m, K)$ are representations, then so is the *direct sum* $\Delta \oplus \Gamma\colon G \to \mathrm{GL}(n+m, K)$ with

$$(\Delta \oplus \Gamma)(g) = \begin{pmatrix} \Delta(g) & 0 \\ 0 & \Gamma(g) \end{pmatrix}$$

for all $g \in G$.

(vi) The sign $\mathrm{sgn}\colon S_n \to \mathbb{Q}^\times$ is a (non-trivial) $\mathbb{Q}$-representation of degree 1 of the symmetric group.

(vii) For $G = \langle g \rangle \cong C_n$, $\Delta(g) := B_{\Phi_n} \in \mathrm{GL}(\varphi(n), \mathbb{Q})$ defines a $\mathbb{Q}$-representation, where B_{Φ_n} is the companion matrix of the n-th cyclotomic polynomial (note $B_{\Phi_n}^n = 1_{\varphi(n)}$).

(viii) The dihedral group D_{2n} is generated by the rotation σ by $2\pi/n$ and the reflection τ across the x-axis (Exercise I.20). Therefore, there exists a representation $\Delta\colon D_{2n} \to \mathrm{GL}(2, \mathbb{R})$ with

$$\Delta(\sigma) = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}, \qquad \Delta(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Definition II.14.5. Two K-representations Δ and Γ of degree n are called *similar*, if there exists an $S \in \mathrm{GL}(n, K)$ with $\Delta(g) = S\Gamma(g)S^{-1}$ for all $g \in G$.

Lemma II.14.6. *K-representations are similar if and only if the corresponding KG-modules are isomorphic.*

Proof. Let Δ and Γ be similar representations of degree n and let $V_\Delta = K^{n\times 1}$ and $V_\Gamma = K^{n\times 1}$ be the corresponding KG-modules. Let $S \in \mathrm{GL}(n, K)$ with $\Delta(g) = S\Gamma(g)S^{-1}$ for all $g \in G$. Then the map $f\colon V_\Gamma \to V_\Delta$, $v \mapsto Sv$ is first of all a vector space isomorphism. For $g \in G$ and $v \in V_\Gamma$ we have

$$f(gv) = Sgv = S\Gamma(g)v = S\Gamma(g)S^{-1}Sv = \Delta(g)Sv = \Delta(g)f(v) = gf(v).$$

Therefore f is also KG-linear.

Conversely, let $f\colon V_\Gamma \to V_\Delta$ be an isomorphism of KG-modules. Since f is also K-linear, there exists an $S \in \mathrm{GL}(n, K)$ with $f(v) = Sv$ for all $v \in V_\Gamma$. Then

$$S\Gamma(g)v = f(\Gamma(g)v) = f(gv) = gf(v) = \Delta(g)f(v) = \Delta(g)Sv$$

for all $v \in V_\Gamma$. This shows $S\Gamma(g)S^{-1} = \Delta(g)$ for all $g \in G$. Thus Δ and Γ are similar. □

Definition II.14.7. A K-representation Δ is called *irreducible*, if the corresponding KG-module V_Δ is simple. Otherwise Δ is called *reducible*.

Remark II.14.8.

(i) A representation $\Delta\colon G \to \mathrm{GL}(n, K)$ is reducible if and only if there exists a subspace $0 \neq U \subsetneq V_\Delta$ with $\Delta(g)(U) \subseteq U$ for all $g \in G$. If one extends a basis of U to a basis of V_Δ, then the matrices $\Delta(g)$ have the form $\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)$. Now let $\operatorname{char} K = 0$. According to Maschke and Lemma II.8.4, U then possesses a complement W. By a suitable choice of basis we achieve $B = 0$, i. e. Δ has the form $\Gamma \oplus \Lambda$. Every $\mathbb{C}$-representation is therefore (up to similarity) a direct sum of irreducible representations. According to Jordan-Hölder, the direct summands are uniquely determined up to similarity, because they correspond to the composition factors of V_Δ.

(ii) The number of irreducible $\mathbb{C}$-representations up to similarity is the number of simple modules up to isomorphism and therefore coincides with the class number of G (Remark II.13.30).

Definition II.14.9. Let $\operatorname{char} K = 0$. For a K-representation $\Delta\colon G \to \mathrm{GL}(n, K)$, the map $\chi_\Delta\colon G \to K$, $g \mapsto \operatorname{tr} \Delta(g)$ is called the *character* of Δ. One calls $\chi_\Delta(1) = n$ the *degree* of χ_Δ. If Δ is (ir)reducible, then χ_Δ is also called *(ir)reducible*.

Remark II.14.10.

(i) Over fields with positive characteristic, characters are less informative, because $\chi(1) = 0$ can hold.

(ii) For K-representations Δ, Γ and $g \in G$, it holds that $\chi_{\Delta\oplus\Gamma}(g) = \chi_\Delta(g) + \chi_\Gamma(g)$. Therefore, the (component-wise) sum of characters is again a character. According to Remark II.14.8, every character is the sum of irreducible characters.

(iii) The next theorem shows that characters are the "shadows" of representations: Although one replaces an n^2-dimensional object $(\Delta(g))$ with a 1-dimensional object $(\chi(g))$, the essential information is preserved.

(iv) For $A = (a_{ij}) \in K^{n\times m}$ and $B = (b_{ij}) \in K^{m\times n}$, it holds that

$$\operatorname{tr}(AB) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}b_{ji} = \sum_{j=1}^{m}\sum_{i=1}^{n} b_{ji}a_{ij} = \operatorname{tr}(BA).$$

Theorem II.14.11. *K-representations are similar if and only if they have the same character.*

Proof. Let Δ and Γ be K-representations of G with character χ_Δ and χ_Γ respectively. Let $S \in \mathrm{GL}(n, K)$ with $\Delta(g) = S\Gamma(g)S^{-1}$ for all $g \in G$. According to Remark II.14.10, it holds that

$$\chi_\Delta(g) = \operatorname{tr} \Delta(g) = \operatorname{tr}(S\Gamma(g)S^{-1}) = \operatorname{tr}(S^{-1}S\Gamma(g)) = \operatorname{tr} \Gamma(g) = \chi_\Gamma(g)$$

for all $g \in G$.

Conversely, let $\chi_\Delta = \chi_\Gamma$. Let $\Lambda_1, \ldots, \Lambda_k$ be a system of representatives for the similarity classes of irreducible representations and let χ_i be the character of Λ_i (according to the first part of the proof, χ_i does not depend on the choice of the representative). Up to similarity, $\Delta = a_1\Lambda_1 \oplus \ldots \oplus a_k\Lambda_k$ and $\Gamma = b_1\Lambda_1 \oplus \ldots \oplus b_k\Lambda_k$ with $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{N}_0$. Likewise,

$$a_1\chi_1 + \ldots + a_k\chi_k = \chi_\Delta = \chi_\Gamma = b_1\chi_1 + \ldots + b_k\chi_k.$$

Let $e_1, \ldots, e_k$ be the central-primitive idempotents of KG. According to Theorem II.8.24, multiplication by e_i effects the identity on the i-th simple KG-module and the zero map on all other simple modules. If

we thus extend the above representations and characters to KG, then $\Lambda_j(e_i) = \delta_{ij} 1_{d_i}$ and $\chi_j(e_i) = \delta_{ij} d_i$ holds. This shows

$$a_i d_i = (a_1\chi_1 + \ldots + a_k\chi_k)(e_i) = \chi_\Delta(e_i) = \chi_\Gamma(e_i) = b_i d_i.$$

Therefore $(a_1, \ldots, a_k) = (b_1, \ldots, b_k)$ and Δ and Γ are similar. □

Definition II.14.12. Let the set of characters of irreducible K-representations of G be $\mathrm{Irr}_K(G)$ and $\mathrm{Irr}(G) := \mathrm{Irr}_{\mathbb{C}}(G)$. Let the set of conjugacy classes of G be $\mathrm{Cl}(G)$.

Example II.14.13.

(i) According to Remark II.13.26 and Theorem II.14.11, $|\mathrm{Irr}(G)| = k(G) = |\mathrm{Cl}(G)|$ and

$$\boxed{|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2.}$$

In particular, G is abelian if and only if all irreducible characters have degree 1.

(ii) Every K-representation of degree 1 coincides with its character. One then speaks of *linear* characters. In particular, the *trivial* character $\mathbb{1}_G$ is equal to the trivial representation. If λ and μ are linear characters, then so is $\lambda\mu$ with $(\lambda\mu)(g) := \lambda(g)\mu(g)$ for $g \in G$ (this will be generalized in Theorem II.14.38).

(iii) Complex conjugation (applied to each matrix entry) induces a group automorphism on $\mathrm{GL}(n, \mathbb{C})$. For a representation $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$, therefore, $\overline{\Delta}$ with $\overline{\Delta}(g) := \overline{\Delta(g)}$ is also a representation. We will see in Remark II.14.18 that $\overline{\Delta}$ coincides with the dual representation Δ^*. For the character, $\chi_{\overline{\Delta}}(g) = \overline{\chi(g)}$ for $g \in G$ holds. One sets $\overline{\chi_\Delta} := \chi_{\overline{\Delta}}$.

(iv) The *regular* character ρ of G belongs to the regular K-representation Δ. We have already seen that $\Delta(g)(h) = gh$ for $g, h \in G$ holds. For $g \neq 1$, it is always $gh \neq h$, i. e. $\Delta(g)$ has only zeros on the main diagonal. This shows $\rho(1) = |G|$ and $\rho(g) = 0$ for $g \neq 1$. On the other hand, the regular $\mathbb{C}G$-module is the direct sum of all simple modules, where the module with dimension d_i occurs with multiplicity d_i (Remark II.13.26). This shows

$$\rho = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi.$$

(v) If Δ is a K-representation with character χ, then $\det\Delta\colon G \to K$, $g \mapsto \det\Delta(g)$ is a linear character, which we denote by $\det\chi$ (as usual, $\det\chi$ does not depend on Δ).

Definition II.14.14. A map $G \to \mathbb{C}$ is called a *class function* if it is constant on the conjugacy classes of G. The set of all class functions of G forms a $k(G)$-dimensional $\mathbb{C}$-vector space $\mathrm{CF}(G)$ with pointwise addition and scalar multiplication. By

$$\boxed{(\chi, \psi) := \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)}} \qquad (\chi, \psi \in \mathrm{CF}(G))$$

an inner product on $\mathrm{CF}(G)$ is given (this corresponds, up to normalization factors, exactly to the standard inner product on $\mathbb{C}^{k(G)}$).

Example II.14.15. For every representation Δ and $g, h \in G$, it holds that

$$\chi_\Delta(ghg^{-1}) = \operatorname{tr}\Delta(ghg^{-1}) = \operatorname{tr}(\Delta(g)\Delta(h)\Delta(g)^{-1}) = \operatorname{tr}(\Delta(g)^{-1}\Delta(g)\Delta(h)) = \operatorname{tr}\Delta(h) = \chi_\Delta(h).$$

Therefore, characters are class functions.

Definition II.14.16. Let $\operatorname{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$ and $g_1, \ldots, g_k \in G$ be a system of representatives for $\operatorname{Cl}(G)$. Then the matrix $T := (\chi_i(g_j))_{i,j=1}^k \in \mathbb{C}^{k\times k}$ is called the *character table* of G. It naturally depends on the order of the χ_i and the g_j (but not on the choice of the g_j according to Example II.14.15). Usually, one chooses $\chi_1 = \mathbb{1}_G$ and $g_1 = 1$.

Example II.14.17.

(i) According to Example II.13.27, $\operatorname{Irr}(S_3)$ consists of the trivial character $\mathbb{1}$, the character sgn, and another character of degree 2. From Example II.14.4, one obtains a representation of $S_3 \overset{\text{I.5.10}}{\cong} D_6$ of degree 2:

$$\Delta((1,2,3)) = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{2} \\ -\sqrt{2} & -1 \end{pmatrix} \qquad \Delta((1,2)) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

with character $\chi((1,2,3)) = -1$ and $\chi((1,2)) = 0$. Because $\chi \notin \{2\mathbb{1}, \mathbb{1}+\operatorname{sgn}, 2\operatorname{sgn}\}$, χ is irreducible. Therefore, $\operatorname{Irr}(S_3) = \{\mathbb{1}_G, \operatorname{sgn}, \chi\}$ and one obtains the character table of S_3:

	1	$(1,2)$	$(1,2,3)$
$\mathbb{1}$	1	1	1
sgn	1	-1	1
χ	2	0	-1

Alternatively, χ can also be calculated via the regular character ρ: $\chi = \frac{1}{2}(\rho - \mathbb{1} - \operatorname{sgn})$.

(ii) Let $G = \langle g \rangle$ be cyclic of order n. According to Example II.14.13, the irreducible characters $\chi_1, \ldots, \chi_n$ of G have degree 1, so they are also representations. Because $\chi_i(g)^n = \chi_i(g^n) = \chi_i(1) = 1$, $\chi_i(g)$ is an n-th root of unity. For a primitive n-th root of unity $\zeta \in \mathbb{C}$, it thus holds that $\chi_i(g) = \zeta^{i-1}$ with a suitable ordering. Thus, $(\zeta^{ij})_{i,j=0}^{n-1}$ is the character table of G.

Remark II.14.18. Let $\Delta\colon G \to \operatorname{GL}(n,\mathbb{C})$ be a representation and $g \in G$. Because of $\Delta(g)^{|G|} = \Delta(g^{|G|}) = \Delta(1) = 1_n$, the minimal polynomial μ of $\Delta(g)$ is a divisor of $X^{|G|} - 1$. Therefore, μ splits into pairwise distinct linear factors over $\mathbb{C}$. Consequently, $\Delta(g)$ is diagonalizable (Remark II.10.7). By passing to a similar representation, we can assume $\Delta(g) = \operatorname{diag}(\zeta_1, \ldots, \zeta_n)$. Because of $\Delta(g)^{|G|} = 1_n$, the ζ_i are $|G|$-th roots of unity. This shows

$$\Delta^*(g) = \Delta(g^{-1}) = \operatorname{diag}(\zeta_1^{-1}, \ldots, \zeta_n^{-1}) = \operatorname{diag}(\overline{\zeta_1}, \ldots, \overline{\zeta_n}) = \overline{\Delta(g)} = \overline{\Delta}(g)$$

and $\chi_\Delta(g^{-1}) = \overline{\chi_\Delta(g)} = \overline{\chi_\Delta}(g)$. The equation $\chi(g^{-1}) = \overline{\chi(g)}$ holds for every character of a K-representation (even if K is not closed under complex conjugation).

Lemma II.14.19. *The central-primitive idempotents of $\mathbb{C}G$ are*

$$\boxed{e_\chi = \frac{\chi(1)}{|G|}\sum_{g\in G}\overline{\chi(g)}g} \qquad (\chi \in \operatorname{Irr}(G)).$$

Proof. Let $\Delta_1, \dots, \Delta_k$ be a system of representatives for the similarity classes of irreducible representations. Let χ_i be the character of Δ_i. Let $e_1, \dots, e_k$ be the central-primitive idempotents of $\mathbb{C}G$. As in the proof of Theorem II.14.11, $\Delta_i(e_j) = \delta_{ij} 1_{\chi_i(1)}$ and $\chi_i(e_j) = \delta_{ij}\chi_i(1)$ hold, where Δ_i and χ_i are extended to $\mathbb{C}G$. For $g \in G$, we have $\Delta_i(ge_j) = \Delta_i(g)\Delta_i(e_j) = \delta_{ij}\Delta_i(g)$ and $\chi_i(ge_j) = \delta_{ij}\chi_i(g)$. We write $e_i = \sum_{g\in G} e_i(g)g$ with $e_i(g) \in \mathbb{C}$. For the regular character $\rho = \sum_{i=1}^k \chi_i(1)\chi_i$, it then holds that

$$e_i(g)|G| \overset{\text{II.14.13}}{=} \rho(g^{-1}e_i) = \sum_{j=1}^{k} \chi_j(1)\chi_j(g^{-1}e_i) = \chi_i(1)\chi_i(g^{-1}) \overset{\text{II.14.18}}{=} \chi_i(1)\overline{\chi_i(g)}. \qquad \square$$

Theorem II.14.20. *The irreducible characters form an orthonormal basis of* $\mathrm{CF}(G)$.

Proof. With the notation from the previous proof, it holds that

$$\frac{\delta_{ij}\chi_i(1)}{|G|} \sum_{g\in G} \overline{\chi_i(g)}g = \delta_{ij}e_i = e_ie_j = \frac{\chi_i(1)\chi_j(1)}{|G|^2} \sum_{g\in G} \Big(\sum_{h\in G} \overline{\chi_i(h)\chi_j(h^{-1}g)} \Big) g.$$

A comparison of coefficients at the position $g = 1$ shows

$$\delta_{ij} = \frac{1}{|G|} \sum_{h\in G} \overline{\chi_i(h)\chi_j(h^{-1})} = \frac{1}{|G|} \sum_{h\in G} \overline{\chi_i(h)}\chi_j(h) = (\chi_i, \chi_j).$$

Therefore, the irreducible characters are orthonormal and, in particular, linearly independent. $\square$

Remark II.14.21. Every character ψ of G can be uniquely written in the form $\psi = \sum_{\chi\in\mathrm{Irr}(G)} a_\chi \chi$ with $a_\chi \in \mathbb{N}_0$. In this case, $a_\chi = (\psi, \chi)$ and $(\psi, \psi) = \sum_{\chi\in\mathrm{Irr}(G)} a_\chi^2$ holds. Therefore, ψ is irreducible if and only if $(\psi, \psi) = 1$.

Theorem II.14.22 (Orthogonality relations)**.** *Let* $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_k\}$ *and* $g_1, \dots, g_k$ *be a system of representatives for* $\mathrm{Cl}(G)$. *For* $1 \le i, j \le k$, *it then holds that*

$$\boxed{\sum_{l=1}^{k} \frac{\chi_i(g_l)\overline{\chi_j(g_l)}}{|\mathrm{C}_G(g_l)|} = \delta_{ij},} \tag{1}$$

$$\boxed{\sum_{l=1}^{k} \chi_l(g_i)\overline{\chi_l(g_j)} = \delta_{ij}|\mathrm{C}_G(g_i)|.} \tag{2}$$

Proof. The conjugacy class of g_i contains exactly $|G : \mathrm{C}_G(g_i)|$ elements (Theorem I.4.7). Since characters are class functions, it follows that

$$\sum_{l=1}^{k} \frac{\chi_i(g_l)\overline{\chi_j(g_l)}}{|\mathrm{C}_G(g_l)|} = \frac{1}{|G|} \sum_{g\in G} \chi_i(g)\overline{\chi_j(g)} = (\chi_i, \chi_j) \overset{\text{II.14.20}}{=} \delta_{ij}.$$

For $A := \big(\chi_i(g_j)/|\mathrm{C}_G(g_j)|\big)_{i,j} \in \mathbb{C}^{k\times k}$ and $B := \big(\overline{\chi_j(g_i)}\big)_{i,j} \in \mathbb{C}^{k\times k}$, we thus have $AB = 1_k$. This shows $BA = 1_k = \overline{B}\,\overline{A}$, i. e. the second orthogonality relation holds. $\square$

Remark II.14.23. Let $N \trianglelefteq G$ and $\epsilon\colon G \to G/N$ be the canonical epimorphism. Every representation $\Delta\colon G/N \to \mathrm{GL}(n, K)$ induces a representation $\widehat{\Delta} := \Delta \circ \epsilon\colon G \to \mathrm{GL}(n, K)$. One calls $\widehat{\Delta}$ the *inflation* of Δ. If Δ is irreducible, then so is $\widehat{\Delta}$. For the characters, $\chi_{\widehat{\Delta}}(g) = \chi_\Delta(gN)$ holds for $g \in G$.

Example II.14.24. According to the second orthogonality relation, the columns of the character table are pairwise orthogonal. This is useful for the calculation of missing character values: Let $G = A_4$ and $N = V_4$. Then $G/N \cong C_3$. By inflation, one obtains linear characters $\chi_1, \chi_2, \chi_3 \in \mathrm{Irr}(G)$ with $\chi_i((1,2,3)) = \zeta^{i-1}$, where $\zeta := \frac{1}{2}(-1 + \sqrt{3}\mathrm{i})$ (Example II.14.17). According to Example II.13.31, G possesses one more irreducible character ψ of degree 3. This yields the following part of the character table:

A_4	1	$(1,2)(3,4)$	$(1,2,3)$	$(1,3,2)$
χ_1	1	1	1	1
χ_2	1	1	ζ	$\overline{\zeta}$
χ_3	1	1	$\overline{\zeta}$	ζ
ψ	3			

The last row follows easily from the second orthogonality relation:

A_4	1	$(1,2)(3,4)$	$(1,2,3)$	$(1,3,2)$
χ_1	1	1	1	1
χ_2	1	1	ζ	$\overline{\zeta}$
χ_3	1	1	$\overline{\zeta}$	ζ
ψ	3	-1	0	0

Remark II.14.25. According to Remark II.14.18 and Theorem II.11.8, character values are algebraic integers as sums of roots of unity.

Theorem II.14.26. *For $\chi \in \mathrm{Irr}(G)$, the map*

$$\begin{aligned} \omega_\chi \colon \mathrm{Z}(\mathbb{C}G) &\to \mathbb{C}, \\ C^+ &\mapsto |C| \frac{\chi(g)}{\chi(1)} \qquad (g \in C \in \mathrm{Cl}(G)) \end{aligned}$$

is a homomorphism of algebras. Furthermore, $\omega_\chi(C^+)$ is an algebraic integer for all $C \in \mathrm{Cl}(G)$.

Proof. According to Theorem II.13.29, ω_χ is uniquely determined as a $\mathbb{C}$-linear map by $\omega_\chi(C^+)$. Let Δ be a representation with character χ and with simple $\mathbb{C}G$-module V_Δ. Let $n := \chi(1)$. We extend Δ linearly to $\mathbb{C}G$ as before. For $x \in G$, $C \in \mathrm{Cl}(G)$ and $v \in V_\Delta$, it then holds that

$$\Delta(C^+)(xv) = C^+(xv) = (C^+x)v = (xC^+)v = x(C^+v) = x\Delta(C^+)(v).$$

This shows $\Delta(C^+) \in \mathrm{End}_{\mathbb{C}G}(V_\Delta)$. By Schur's Lemma and Lemma II.12.6, $\mathrm{End}_{\mathbb{C}G}(V_\Delta) = \mathbb{C}\,\mathrm{id}$. Therefore $\Delta(C^+) = \lambda 1_n$ with

$$\lambda = \frac{1}{n} \operatorname{tr} \Delta(C^+) = \frac{1}{n} \sum_{c \in C} \operatorname{tr} \Delta(c) = |C| \frac{\chi(g)}{n} = \omega_\chi(C^+),$$

where $g \in C$. Since Δ is a homomorphism, ω_χ is now also a homomorphism of algebras. For $D \in \mathrm{Cl}(G)$, it further holds that

$$C^+D^+ = \sum_{E \in \mathrm{Cl}(G)} a_E E^+$$

with $a_E \in \mathbb{N}_0$ (by multiplying out). It follows that

$$\omega_\chi(C^+)\omega_\chi(D^+) = \omega_\chi(C^+D^+) = \sum_{E \in \mathrm{Cl}(G)} a_E \omega_\chi(E^+) \in \sum_{E \in \mathrm{Cl}(G)} \mathbb{Z}\omega_\chi(E^+) =: M.$$

Therefore M is a finitely generated $\mathbb{Z}$-module with $\omega_\chi(C^+)M \subseteq M$ and $1 = \omega_\chi(1) \in M$. The second assertion now follows from Lemma II.11.6. □

Theorem II.14.27. *For all $\chi \in \mathrm{Irr}(G)$, $\chi(1)$ is a divisor of $|G|$.*

Proof. Let $\mathrm{Cl}(G) = \{C_1, \ldots, C_k\}$ and $g_i \in C_i$ for $i = 1, \ldots, k$. According to the first orthogonality relation,

$$\frac{|G|}{\chi(1)} = \sum_{i=1}^{k} |C_i| \frac{\chi(g_i)}{\chi(1)} \chi(g_i^{-1}) = \sum_{i=1}^{k} \omega_\chi(C_i^+) \chi(g_i^{-1}).$$

According to Remark II.14.25 and Theorem II.14.26, $|G|/\chi(1) \in \mathbb{Q}$ is an algebraic integer. The assertion follows from Example II.11.3. □

Lemma II.14.28. *Let $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ be a representation with character χ. For $g \in G$, it then holds:*

(i) $|\chi(g)| \leq n$.

(ii) $|\chi(g)| = n \iff \Delta(g) \in \mathbb{C}^\times 1_n$.

(iii) $\chi(g) = n \iff g \in \mathrm{Ker}(\Delta)$.

Proof. According to Remark II.14.18, the eigenvalues $\epsilon_1, \ldots, \epsilon_n \in \mathbb{C}$ of $\Delta(g)$ are roots of unity. The Cauchy-Schwarz inequality with the vectors $v := (\epsilon_1, \ldots, \epsilon_n)$ and $w := (1, \ldots, 1)$ yields

$$|\chi(g)| = |\epsilon_1 + \ldots + \epsilon_n| = |\langle v, w \rangle| \leq |v||w| = \sqrt{n}\sqrt{n} = n.$$

This shows (i). If equality holds, then v and w are linearly dependent and it follows that $\epsilon := \epsilon_1 = \epsilon_2 = \ldots = \epsilon_n$. Since $\Delta(g)$ is diagonalizable (Remark II.14.18), it follows that $\Delta(g) = \epsilon 1_n$. Conversely, if $\Delta(g) \in \mathbb{C}^\times 1_n$, then $|\chi(g)| = n$. If even $\chi(g) = n$, then $\epsilon = 1$ and $g \in \mathrm{Ker}(\Delta)$. The converse is also clear here. □

Definition II.14.29. In the situation of Lemma II.14.28, we define

$$\mathrm{Ker}(\chi) := \mathrm{Ker}(\Delta) = \{g \in G : \chi(g) = n\},$$
$$\mathrm{Z}(\chi) := \Delta^{-1}(\mathbb{C}^\times 1_n) = \{g \in G : |\chi(g)| = n\}.$$

One calls $\mathrm{Ker}(\chi)$ the *kernel* and $\mathrm{Z}(\chi)$ the *center* of χ. In the case $\mathrm{Ker}(\chi) = 1$, one calls χ *faithful*.

Remark II.14.30. Because $\mathbb{C}^\times 1_n \trianglelefteq \mathrm{GL}(n, \mathbb{C})$, $\mathrm{Ker}(\chi)$ and $\mathrm{Z}(\chi)$ are normal subgroups of G with $\mathrm{Ker}(\chi) \leq \mathrm{Z}(\chi)$ (Remark I.3.24). According to the isomorphism theorem, $G/\mathrm{Ker}(\chi)$ is isomorphic to a subgroup of $\mathrm{GL}(n, \mathbb{C})$ and $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi)$ is isomorphic to a subgroup of $\mathbb{C}^\times 1_n \cong \mathbb{C}^\times$. According to Theorem I.8.31, $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi)$ is always cyclic.

Lemma II.14.31. *Let $\chi \in \mathrm{Irr}(G)$ and $g \in C \in \mathrm{Cl}(G)$ with $\gcd(\chi(1), |C|) = 1$. Then $g \in \mathrm{Z}(\chi)$ or $\chi(g) = 0$.*

Proof. Let $g \notin \mathrm{Z}(\chi)$ and $\alpha := \frac{\chi(g)}{\chi(1)}$. Because $\gcd(\chi(1), |C|) = 1$, there exist $a, b \in \mathbb{Z}$ with $a\chi(1) + b|C| = 1$. With $\omega_\chi(C^+)$ and $\chi(g)$, also

$$\alpha = \frac{\chi(g)}{\chi(1)}(a\chi(1) + b|C|) = a\chi(g) + b\omega_\chi(C^+)$$

is algebraic integer. Let $n := |\langle g \rangle|$. As a sum of n-th roots of unity, $\chi(g) \in \mathbb{Q}_n$. For $\sigma \in \mathcal{G} := \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$, $\sigma(\alpha)$ is also an algebraic integer (root of the same polynomial). Therefore, also

$$\beta := \prod_{\sigma \in \mathcal{G}} \sigma(\alpha) \in \mathbb{Q}_n^{\mathcal{G}} \overset{\text{I.10.9}}{=} \mathbb{Q}$$

is an algebraic integer, thus $\beta \in \mathbb{Z}$. Because $g \notin \mathrm{Z}(\chi)$, we have $|\alpha| < 1$ according to Lemma II.14.28. With $\chi(g)$, also $\sigma(\chi(g))$ is a sum of roots of unity. By the triangle inequality, it follows that $|\sigma(\chi(g))| \leq \chi(1)$ and $|\sigma(\alpha)| \leq 1$ for all $\sigma \in \mathcal{G}$. Consequently, $|\beta| = \prod_{\sigma \in \mathcal{G}} |\sigma(\alpha)| < 1$, i. e. $\beta = 0$ because $\beta \in \mathbb{Z}$. Thus $\alpha = 0$ and $\chi(g) = 0$. □

Lemma II.14.32. *Let G be non-abelian and simple and $C \in \mathrm{Cl}(G)$. If $|C| = p^k$ is a prime power, then $C = \{1\}$.*

Proof. Assume indirectly that $C \neq \{1\}$. Let $g \in C$ and $\chi \in \mathrm{Irr}(G) \setminus \{\mathbb{1}_G\}$. Since G is simple and non-abelian, $\mathrm{Ker}(\chi) = 1 = \mathrm{Z}(\chi)$ by Remark II.14.30. In the case $p \nmid \chi(1)$, it follows that $\chi(g) = 0$ by Lemma II.14.31. According to the second orthogonality relation,

$$0 = \frac{1}{p} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g) = \frac{1}{p} + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ p \,|\, \chi(1)}} \frac{\chi(1)}{p} \chi(g).$$

But then $1/p$ would be algebraic-integral, contradicting Example II.11.3. □

Theorem II.14.33 (Burnside's $p^a q^b$-Theorem)**.** *Groups of order $p^a q^b$ with $p, q \in \mathbb{P}$ and $a, b \in \mathbb{N}_0$ are solvable.*

Proof. Let G be a minimal counterexample and $1 \neq N \trianglelefteq G$. In the case $N \neq G$, both N and G/N would be solvable and therefore also G (Theorem I.6.5). Thus G is simple and non-abelian. Wlog. let $1 \neq P \in \mathrm{Syl}_p(G)$. By Theorem I.4.11, there exists $g \in \mathrm{Z}(P) \setminus \{1\}$. Then $P \subseteq \mathrm{C}_G(g)$. The length $|C| = |G : \mathrm{C}_G(g)|$ of the conjugacy class C of g is therefore a q-power. From Lemma II.14.32 follows the contradiction $g = 1$. □

Remark II.14.34. Theorem II.14.33 was one of the first applications of representation theory to the study of finite groups. Meanwhile, a (significantly more difficult) proof is known that does not use representation theory.[1] For the next (purely group-theoretic) theorem, however, no proof is known that does not use character theory.

Theorem II.14.35 (Frobenius)**.** *Let $1 < H < G$ with $gHg^{-1} \cap H = 1$ for all $g \in G \setminus H$. Then there exists $N \trianglelefteq G$ with $G = HN$ and $H \cap N = 1$.*

Proof (Knapp-Schmid). Let

$$H^* := \Big(\bigcup_{g \in G} gHg^{-1} \Big) \setminus \{1\}$$

and $N := G \setminus H^*$. By assumption, $\mathrm{N}_G(H) = H$, i. e. H has exactly $|G : H|$ conjugates in G. For any two distinct conjugates xHx^{-1} and yHy^{-1}, it holds that

$$xHx^{-1} \cap yHy^{-1} = x(H \cap x^{-1}yHy^{-1}x)x^{-1} = 1.$$

[1] See Section 10.2 in [H. Kurzweil, B. Stellmacher, *Theorie der endlichen Gruppen*, Springer, Berlin, 1998]

This shows $|H^*| = |G:H|(|H|-1) = |G| - |G:H|$ and $|N| = |G:H|$. If we can show that the class function

$$\rho\colon G \to \mathbb{C}, \qquad g \mapsto \begin{cases} |H| & \text{if } g \in N, \\ 0 & \text{if } g \in H^* \end{cases}$$

is a character of G, then $N = \mathrm{Ker}(\rho) \trianglelefteq G$ follows. Because of $N \cap H = 1$, we then have $|HN| = |H||N| = |G|$ and $G = HN$. For $\chi \in \mathrm{Irr}(G)$, we must show $(\chi, \rho) \in \mathbb{N}_0$. First, $(\rho, \mathbb{1}_G) = \frac{|H||N|}{|G|} = 1$ holds. For $\chi \neq \mathbb{1}_G$, by the first orthogonality relation, it holds that

$$\begin{aligned} c_\chi := (\chi, \rho) &= \frac{1}{|G|} \sum_{g \in N} \chi(g)|H| = \frac{1}{|N|} \sum_{g \in G} \chi(g) - \frac{1}{|N|} \sum_{g \in H^*} \chi(g) \\ &= -\sum_{g \in H \setminus \{1\}} \chi(g) = \chi(1) - |H|(\chi_H, \mathbb{1}_H) \in \mathbb{Z}. \end{aligned}$$

We can assume $c_\chi \neq 0$. The Cauchy-Schwarz inequality applied to the vectors $(\chi(g) : g \in N)$ and $(1, \ldots, 1)$ yields

$$(|N|c_\chi)^2 = \Big(\sum_{g \in N} \chi(g)\Big)^2 \leq |N| \sum_{g \in N} |\chi(g)|^2.$$

It follows

$$1 = (\chi, \chi) = \frac{1}{|G|} \sum_{g \in N} |\chi(g)|^2 + \frac{1}{|G|} \sum_{g \in H^*} |\chi(g)|^2 \geq \frac{1}{|H|}\Big(c_\chi^2 + \sum_{g \in H \setminus \{1\}} |\chi(g)|^2\Big) > 0.$$

Because of $c_\chi^2 - \chi(1)^2 = (c_\chi + \chi(1))(c_\chi - \chi(1))$, on the other hand,

$$\frac{1}{|H|}\Big(c_\chi^2 + \sum_{g \in H \setminus \{1\}} |\chi(g)|^2\Big) = \frac{1}{|H|}\big(c_\chi^2 - \chi(1)^2\big) + (\chi_H, \chi_H) = (\chi_H, \chi_H) - (c_\chi + \chi(1))(\chi_H, \mathbb{1}_H) \in \mathbb{Z}.$$

Therefore, equality holds in the Cauchy-Schwarz inequality. This implies $\chi(g) = \chi(1)$ for all $g \in N$. Thus $c_\chi = \chi(1) > 0$ as desired. □

Remark II.14.36. In the situation of Theorem II.14.35, G is called a *Frobenius group* with *complement* H and *kernel* N.

Example II.14.37. Let $n \geq 3$ be odd. Then $D_{2n} = \langle \sigma, \tau : \sigma^n = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$ is a Frobenius group with complement $\langle \tau \rangle$ and kernel $\langle \sigma \rangle$, since $\sigma^i \tau \sigma^{-i} = \sigma^{2i}\tau \neq \tau$ for $i = 1, \ldots, n-1$.

Theorem II.14.38. *If χ and ψ are characters of G, then so is $\chi\psi$ with $(\chi\psi)(g) := \chi(g)\psi(g)$ for $g \in G$.*

Proof. Let V be a $\mathbb{C}G$-module with character $\overline{\chi}$ and W a $\mathbb{C}G$-module with character ψ. We consider the $\mathbb{C}$-vector space $U := \mathrm{Hom}_{\mathbb{C}}(V, W)$. [2] For $\varphi \in U$ and $g \in G$ let $g\varphi\colon V \to W$, $v \mapsto g\varphi(g^{-1}v)$. Obviously $g\varphi \in U$ and

$$((gh)\varphi)(v) = (gh)\varphi((gh)^{-1}v) = g(h\varphi(h^{-1}(g^{-1}v))) = g((h\varphi)(g^{-1}v)) = (g(h\varphi))(v)$$

for $g, h \in G$. In this way, U becomes a $\mathbb{C}G$-module. Let $b_1, \ldots, b_n$ be a basis of V and $c_1, \ldots, c_m$ be a basis of W. Then the functions $\varphi_{ij}\colon V \to W$, $b_k \mapsto \delta_{ik}c_j$ with $i = 1, \ldots, n$, $j = 1, \ldots, m$ form a basis of U. Let $\Delta\colon G \to \mathrm{GL}(nm, \mathbb{C})$ be the representation of U with respect to this basis. Let $g \in G$,

[2] Most textbooks introduce the tensor product $V \otimes W$ instead. We will do this later in Definition III.3.16.

$g^{-1}b_i = \sum_{j=1}^n \alpha_{ji} b_j$ and $gc_i = \sum_{j=1}^m \beta_{ji} c_j$ with $\alpha_{ji}, \beta_{ji} \in \mathbb{C}$. Then $\chi(g) = \overline{\chi}(g^{-1}) = \alpha_{11} + \ldots + \alpha_{nn}$ and $\psi(g) = \beta_{11} + \ldots + \beta_{mm}$ holds. Furthermore,

$$\begin{aligned}(g\varphi_{ij})(b_k) = g\varphi_{ij}(g^{-1}b_k) &= \sum_{l=1}^n \alpha_{lk} g\varphi_{ij}(b_l) = \alpha_{ik} g c_j = \alpha_{ik} \sum_{l=1}^m \beta_{lj} c_l \\ &= \alpha_{ik} \sum_{l=1}^m \beta_{lj} \varphi_{kl}(b_k) = \sum_{k=1}^n \alpha_{ik} \sum_{l=1}^m \beta_{lj} \varphi_{kl}(b_k)\end{aligned}$$

for $i, k = 1, \ldots, n$ and $j = 1, \ldots, m$. This shows

$$\chi_\Delta(g) = \sum_{i=1}^n \alpha_{ii} \sum_{j=1}^m \beta_{jj} = \chi(g)\psi(g). \qquad \square$$

Theorem II.14.39. *Let G and H be finite groups. For $\chi \in \mathrm{Irr}(G)$ and $\psi \in \mathrm{Irr}(H)$ let*

$$\begin{aligned}\chi \times \psi \colon G \times H &\to \mathbb{C}, \\ (g, h) &\mapsto \chi(g)\psi(h).\end{aligned}$$

Then $\mathrm{Irr}(G \times H) = \{\chi \times \psi : \chi \in \mathrm{Irr}(G), \psi \in \mathrm{Irr}(H)\}$ holds.

Proof. Because of $(G \times H)/H \cong G$, $\chi \in \mathrm{Irr}(G)$ can be viewed as a character of $G \times H$ via inflation. In this case, $\chi(g, h) = \chi(g)$ for $(g, h) \in G \times H$. Analogously, we can assume $\mathrm{Irr}(H) \subseteq \mathrm{Irr}(G \times H)$. According to Theorem II.14.38, $\chi \times \psi$ is a character of $G \times H$. For $\chi, \chi' \in \mathrm{Irr}(G)$ and $\psi, \psi' \in \mathrm{Irr}(H)$ we have

$$\begin{aligned}(\chi \times \psi, \chi' \times \psi') &= \frac{1}{|G \times H|} \sum_{(g,h) \in G \times H} \chi(g)\overline{\chi'(g)}\psi(h)\overline{\psi'(h)} = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi'(g)} \frac{1}{|H|} \sum_{h \in H} \psi(h)\overline{\psi'(h)} \\ &= (\chi, \chi')(\psi, \psi') = \delta_{\chi\chi'}\delta_{\psi\psi'}.\end{aligned}$$

According to Remark II.14.21, $\chi \times \psi$ are pairwise irreducible characters of $G \times H$. Because of

$$\sum_{\chi \in \mathrm{Irr}(G)} \sum_{\psi \in \mathrm{Irr}(H)} (\chi \times \psi)(1)^2 = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 \sum_{\psi \in \mathrm{Irr}(H)} \psi(1)^2 = |G||H| = |G \times H|$$

we have found all irreducible characters. $\square$

Remark II.14.40. If $g_1, \ldots, g_n \in G$ and $h_1, \ldots, h_m \in H$ are systems of representatives for the conjugacy classes of G and H respectively, then $(g_1, h_1), (g_1, h_2), \ldots, (g_n, h_m) \in G \times H$ is obviously a system of representatives for the conjugacy classes of $G \times H$. If $T_G = (a_{ij})$ and T_H are the character tables of G and H respectively, then one obtains the character table of $G \times H$ by the *Kronecker product* of matrices

$$T_{G \times H} = T_G \otimes T_H = \begin{pmatrix} a_{11}T_H & \cdots & a_{1n}T_H \\ \vdots & & \vdots \\ a_{n1}T_H & \cdots & a_{nn}T_H \end{pmatrix} \in \mathbb{C}^{nm \times nm}.$$

Example II.14.41. Since we already know the character tables of cyclic groups (Example II.14.17), the character tables of abelian groups can also be given using the fundamental theorem of finite abelian groups. For example

$$\begin{array}{c|cccc} C_2^2 & 1 & x & y & xy \\ \hline \mathbb{1} & 1 & 1 & 1 & 1 \\ \chi & 1 & -1 & 1 & -1 \\ \psi & 1 & 1 & -1 & -1 \\ \chi\psi & 1 & -1 & -1 & 1 \end{array} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Lemma II.14.42. *The linear characters of G form a group $\hat{G} \cong G/G'$, which acts on $\mathrm{Irr}(G)$ by multiplication, i. e. for $\lambda \in \hat{G}$ and $\chi \in \mathrm{Irr}(G)$ we have $\lambda\chi \in \mathrm{Irr}(G)$.*

Proof. We already know that $\hat{G}$ consists of the inflations of $\mathrm{Irr}(G/G')$. Obviously $\hat{G}$ is a group with respect to multiplication. Let

$$G/G' \cong \langle g_1 \rangle \times \ldots \times \langle g_n \rangle \cong C_{d_1} \times \ldots \times C_{d_n}$$

and $\lambda_i \in \mathrm{Irr}(\langle g_i \rangle)$ with $\lambda_i(g_i) = e^{2\pi \mathrm{i}/d_i}$. According to Theorem II.14.39,

$$G/G' \to \hat{G}, g_1^{k_1} \ldots g_n^{k_n} \mapsto \lambda_1^{k_1} \times \ldots \times \lambda_n^{k_n}$$

is an isomorphism.

For the second statement we use $\lambda(gh) = \lambda(g)\lambda(h)$ for $g, h \in G$. It holds that

$$(\chi\lambda, \chi\lambda) = \frac{1}{|G|} \sum_{g \in G} \chi(g)\lambda(g)\lambda(g^{-1})\chi(g^{-1}) = (\chi, \chi) = 1$$

and the claim follows from Remark II.14.21. □

Remark II.14.43. For the concrete calculation of representations with a computer, it is necessary to approximate the field $\mathbb{C}$ by smaller fields. According to Remark II.14.18, the character values of G lie in $\mathbb{Q}_n$, where $n = |G|$. Brauer's deep induction theorem implies that every $\mathbb{C}$-representation of G is similar to a $\mathbb{Q}_n$-representation. We prove a weaker statement with less effort.

Theorem II.14.44. *For every finite group G there exists a number field K such that every $\mathbb{C}$-representation of G is similar to a K-representation.*

Proof. Most of our previous results also hold for $\overline{\mathbb{Q}}$ instead of $\mathbb{C}$, because we have only used characteristic 0 (Maschke), algebraically closed (Artin-Wedderburn) and complex conjugation (scalar product). Let $\psi_1, \ldots, \psi_k$ be the characters of irreducible $\overline{\mathbb{Q}}$-representations. As in Theorem II.14.20, $\{\psi_1, \ldots, \psi_k\}$ is an orthonormal basis of $\mathrm{CF}(G)$ and $k = k(G)$. Since every $\overline{\mathbb{Q}}$-representation is also a $\mathbb{C}$-representation, it holds that

$$\psi_i = \sum_{\chi \in \mathrm{Irr}(G)} a_{i,\chi}\chi$$

for $1 \leq i \leq k$ and certain $a_{i,\chi} \in \mathbb{N}_0$. From $1 = (\psi_i, \psi_i)_G = \sum_{\chi \in \mathrm{Irr}(G)} a_{i,\chi}^2$ it follows that $\psi_i \in \mathrm{Irr}(G)$ and $\mathrm{Irr}(G) = \{\psi_1, \ldots, \psi_k\}$. Every (irreducible) $\mathbb{C}$-representation is thus similar to a $\overline{\mathbb{Q}}$-representation Δ (Theorem II.14.11). The entries of $\Delta(g)$ for $g \in G$ are algebraic numbers, they thus lie in a number field K. We can choose K large enough so that every (irreducible) $\overline{\mathbb{Q}}$-representation has entries in K. □

Definition II.14.45. A representation over a number field K is called *absolutely irreducible*, if it is irreducible as a $\mathbb{C}$-representation. If all irreducible K-representations are absolutely irreducible, then K is called a *splitting field* of G.

Example II.14.46.

(i) According to Theorem II.14.44, every group has a splitting field with finite degree over $\mathbb{Q}$. According to Remark II.14.18, $\mathbb{Q}_n$ is a splitting field of every abelian group of order n. One can show that $\mathbb{Q}$ is a splitting field of the symmetric groups (without proof, Exercise II.74).

(ii) The companion matrix $B := B_{\Phi_3} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ has order 3. Since the eigenvalues of B are irrational, the embedding $\Delta\colon \langle B\rangle \hookrightarrow \mathrm{GL}(2,\mathbb{Q})$ is an irreducible $\mathbb{Q}$-representation. According to Example II.14.13, on the other hand, every irreducible $\mathbb{C}$-representation of the abelian group $\langle B\rangle \cong C_3$ has degree 1. Therefore, Δ is not absolutely irreducible.

Theorem II.14.47. *For every representation $\Delta\colon G \to \mathrm{GL}(n,K)$ over a number field K, the following statements are equivalent:*

(1) Δ is absolutely irreducible.

(2) $\mathrm{C}_{K^{n\times n}}(\Delta(G)) = K1_n$.

(3) $\Delta(KG) = K^{n\times n}$.

Proof. Let $V := K^n$ be the simple KG-module belonging to Δ, i. e. $gv = \Delta(g)(v)$ for $g \in G$ and $v \in V$. For $f \in \mathrm{End}_K(V) \cong K^{n\times n}$, $f \in \mathrm{End}_{KG}(V)$ holds if and only if

$$(f \circ \Delta(g))(v) = f(gv) = gf(v) = (\Delta(g) \circ f)(v)$$

for all $v \in V$. This shows $D := \mathrm{End}_{KG}(V) \cong \mathrm{C}_{K^{n\times n}}(\Delta(G))$.

(1) $\Rightarrow$ (2): By Schur's Lemma, $\mathrm{C}_{\mathbb{C}^{n\times n}}(\Delta(G)) \cong \mathrm{End}_{\mathbb{C}G}(V) \cong \mathbb{C}$. This shows

$$\mathrm{C}_{K^{n\times n}}(\Delta(G)) = K^{n\times n} \cap \mathrm{C}_{\mathbb{C}^{n\times n}}(\Delta(G)) = K^{n\times n} \cap \mathbb{C}1_n = K1_n.$$

(2) $\Rightarrow$ (3): By Jacobson's Density Theorem (Remark II.8.30), $\Delta\colon KG \to \mathrm{End}_D(V) = \mathrm{End}_K(V) \cong K^{n\times n}$ is surjective.

(3) $\Rightarrow$ (1): Assume Δ is reducible as a $\mathbb{C}$-representation. After a suitable choice of basis, $\Delta(\mathbb{C}G)$ then consists of matrices of the form $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$. This contradicts (3). □

Theorem II.14.48 (Minkowski)**.** *Every finite subgroup G of $\mathrm{GL}(n,\mathbb{Q})$ is conjugate to a subgroup of $\mathrm{GL}(n,\mathbb{Z})$. Furthermore, for every prime $p > 2$, G is isomorphic to a subgroup of $\mathrm{GL}(n,p)$. In particular, $|G|$ is bounded by a function in n.*

Proof. Clearly $M := \sum_{g\in G} g\mathbb{Z}^n \subseteq \mathbb{Q}^n$ is a $\mathbb{Z}$-module containing the free $\mathbb{Z}$-module $\mathbb{Z}^n$. If k is the lcm of all denominators of matrix entries from all $g \in G$, then $k\mathbb{Z}^n \subseteq kM \subseteq \mathbb{Z}^n$. By Theorem II.9.26, M is free of rank n. Let $\gamma\colon \mathbb{Z}^n \to M$ be a corresponding isomorphism of $\mathbb{Z}$-modules. Since $\mathbb{Z}^n$ contains the standard basis of $\mathbb{Q}^n$, γ can be (uniquely) extended to an isomorphism $\gamma\colon \mathbb{Q}^n \to \mathbb{Q}^n$ of $\mathbb{Q}$-vector spaces. For $g \in G$ we have

$$(\gamma^{-1}g\gamma)(\mathbb{Z}^n) = (\gamma^{-1}g)(M) = \gamma^{-1}(M) = \mathbb{Z}^n.$$

This shows $\gamma^{-1}G\gamma \leq \mathrm{GL}(n,\mathbb{Z})$.

For the second assertion, we can assume $G \leq \mathrm{GL}(n,\mathbb{Z})$. It suffices to show that the reduction modulo p, $\Gamma\colon G \to \mathrm{GL}(n,p)$, is injective. In the case $\mathrm{Ker}(\Gamma) \neq 1$, there exists a $g \in \mathrm{Ker}(\Gamma)$ of prime order q. Let $g = 1_n + dA$ with $d \in \mathbb{Z}$ and $A \in \mathbb{Z}^{n\times n}$ with coprime entries. Because $g \equiv 1_n \pmod p$, we have $p \mid d$. By the binomial formula,

$$\begin{aligned} 1_n = g^q = (1_n + dA)^q &= 1_n + qdA + \frac{q(q-1)}{2}d^2A^2 + \ldots + d^qA^q, \\ -qA = \frac{q(q-1)}{2}dA + \ldots + d^{q-1}A^q &\equiv 0 \pmod p. \end{aligned}$$

This shows $q = p$. Because $p > 2$, one obtains the contradiction

$$-A = \frac{p-1}{2}dA + \ldots + \frac{d^{p-1}}{p}A^p \equiv 0 \pmod p. \qquad \square$$

Remark II.14.49.

(i) The companion matrix $B_{\Phi_6} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$ has order 6. Because of $\mathrm{GL}(2,2) \cong S_3$, Theorem II.14.48 cannot hold for $p = 2$. However, the proof shows that the kernel of the map $G \to \mathrm{GL}(n,2)$ is an elementary abelian 2-group.

(ii) The next theorem generalizes the complex conjugation of characters.

Theorem II.14.50. *Let G be a group of order n. Let $\zeta := e^{2\pi\mathrm{i}/n} \in \mathbb{Q}_n$ and $\sigma \in \mathcal{G} := \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ with $\sigma(\zeta) = \zeta^k$. Then:*

(i) By ${}^{\sigma}({}^{G}g) := {}^{G}(g^k)$ for $g \in G$, $\mathcal{G}$ acts on $\mathrm{Cl}(G)$.

(ii) By $\boxed{({}^{\sigma}\chi)(g) := \sigma(\chi(g)) = \chi(g^k)}$ for $g \in G$ and $\chi \in \mathrm{Irr}(G)$, $\mathcal{G}$ acts on $\mathrm{Irr}(G)$.

Proof.

(i) Because of $\gcd(k,n) = 1$, there exists $l \in \mathbb{Z}$ with $kl \equiv 1 \pmod n$. Therefore $G \to G$, $g \mapsto g^k$ is a bijection with inverse map $g \mapsto g^l$. For $g,h,x \in G$, it holds that $g = xhx^{-1} \iff g^k = xh^kx^{-1}$. Thus ${}^{\sigma}C \in \mathrm{Cl}(G)$ for all $C \in \mathrm{Cl}(G)$. For $\tau \in \mathcal{G}$ with $\tau(\zeta) = \zeta^l$, it holds that

$${}^{\sigma\tau}({}^{G}g) = {}^{G}(g^{kl}) = {}^{\sigma}({}^{G}(g^l)) = {}^{\sigma}({}^{\tau}({}^{G}g)).$$

Thus $\mathcal{G}$ acts on $\mathrm{Cl}(G)$.

(ii) Let K be a number field as in Theorem II.14.44 and $\Delta\colon G \to \mathrm{GL}(d,K)$ a representation with character χ. According to Theorem I.12.2, we can assume that $\mathbb{Q} \subseteq K$ is a Galois extension. Let $L := K\mathbb{Q}_n \subseteq \mathbb{C}$ be the compositum of K and $\mathbb{Q}_n$. According to Theorem I.10.15, $\mathbb{Q} \subseteq L$ is also a Galois extension and the restriction $\mathrm{Gal}(L|\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ is surjective. Let $\hat\sigma \in \mathrm{Gal}(L|\mathbb{Q})$ with $\hat\sigma_{|\mathbb{Q}_n} = \sigma$. Applying $\hat\sigma$ to matrix entries yields an automorphism of $\mathrm{GL}(d,K)$. Thus $\hat\sigma \circ \Delta\colon G \to \mathrm{GL}(d,K)$ is an irreducible K-representation with character

$$g \mapsto \mathrm{tr}\big(\hat\sigma(\Delta(g))\big) = \sigma(\mathrm{tr}\,\Delta(g)) = \sigma(\chi(g))$$

for $g \in G$. Let $\zeta^{a_1}, \ldots, \zeta^{a_d} \in \mathbb{Q}_n$ be the eigenvalues of $\Delta(g)$ (Remark II.14.18). Then it holds that

$$\chi(g^k) = \mathrm{tr}\,\Delta(g^k) = \zeta^{a_1k} + \ldots + \zeta^{a_dk} = \sigma(\zeta^{a_1} + \ldots + \zeta^{a_d}) = \sigma(\chi(g)).$$

It is easy to see that $(\sigma,\chi) \mapsto {}^{\sigma}\chi$ defines an action. $\square$

Remark II.14.51.

(i) Conjugacy classes or characters that lie in the same orbit under $\mathcal{G}$ are called *Galois conjugate*.

(ii) Since $\mathcal{G}$ is abelian, one also obtains an action via ${}^{\sigma}({}^{G}g) := {}^{G}(g^{k'})$ with $kk' \equiv 1 \pmod{n}$. It then holds that $({}^{\sigma}\chi)({}^{\sigma}C) = \chi(C) := \chi(g)$ for $C := {}^{G}g$.

(iii) The natural action of $\mathrm{Aut}(G)$ on G (i. e. the embedding $\mathrm{Aut}(G) \hookrightarrow \mathrm{Sym}(G)$) induces actions of $\mathrm{Aut}(G)$ on $\mathrm{Cl}(G)$ and $\mathrm{Irr}(G)$. For $\alpha \in \mathrm{Aut}(G)$, $\chi \in \mathrm{Irr}(G)$ and $g \in C \in \mathrm{Cl}(G)$, it holds that ${}^{\alpha}C := {}^{G}\alpha(g)$ and $({}^{\alpha}\chi)(g) = \chi(\alpha^{-1}(g))$. Again, one obtains $({}^{\alpha}\chi)({}^{\alpha}C) = \chi(C)$. Since $\mathrm{Inn}(G)$ lies in the kernel of the action, it suffices to consider the action of $\mathrm{Out}(G)$.

(iv) The actions of $\mathcal{G}$ and $\mathrm{Out}(G)$ cause permutations of the rows and columns of the character table of G. The next result implies that rows and columns cannot be permuted independently.

Theorem II.14.52 (Brauer's Permutation Lemma)**.** *Let G, H be finite groups such that G acts on $\mathrm{Cl}(H)$ and $\mathrm{Irr}(H)$. For all $g \in G$, $C \in \mathrm{Cl}(H)$ and $\chi \in \mathrm{Irr}(H)$, let $({}^{g}\chi)({}^{g}C) = \chi(C)$ hold. Then the cycle type of $g \in G$ in $\mathrm{Sym}(\mathrm{Cl}(H))$ coincides with the cycle type of g in $\mathrm{Sym}(\mathrm{Irr}(H))$. In particular,*

$$|\{C \in \mathrm{Cl}(H) : {}^{g}C = C\}| = |\{\chi \in \mathrm{Irr}(H) : {}^{g}\chi = \chi\}|$$

for all $g \in G$.

Proof. Let $\mathrm{Cl}(H) = \{C_1, \ldots, C_k\}$ and $\mathrm{Irr}(H) = \{\chi_1, \ldots, \chi_k\}$. Let $X := (\chi_i(C_j))_{i,j}$ be the character table of H. Let $g \in G$ be fixed. The action of g on $\mathrm{Cl}(H)$ (resp. $\mathrm{Irr}(H)$) is then described by a permutation matrix P (resp. Q). It holds that

$$QX = ({}^{g}\chi_i(C_j)) = (\chi_i({}^{g^{-1}}C_j)) = XP.$$

By the second orthogonality relation, X is invertible. It follows that $Q = XPX^{-1}$, i. e. Q and P are similar. Let $(l_1, \ldots, l_n)$ be the cycle type of P. Then P is similar to a block diagonal matrix $\mathrm{diag}(P_1, \ldots, P_l)$, where the block P_i corresponds to the cycle of length l_i. Furthermore, P_i is similar to the companion matrix of $X^{l_i} - 1$. From Lemma II.10.4 one obtains the eigenvalues of P:

$$\{e^{2\pi \mathrm{i} j/l_1} : j = 0, \ldots, l_1 - 1\} \cup \ldots \cup \{e^{2\pi \mathrm{i} j/l_n} : j = 0, \ldots, l_n - 1\}$$

(with multiplicities). Since P and Q have the same eigenvalues, $(l_1, \ldots, l_n)$ is also the cycle type of Q. The last assertion is obtained by counting cycles of length one. □

Theorem II.14.53 (Schur)**.** *Let χ be a faithful character of G with values in a number field K. Then $|G|$ is bounded by a function in $\chi(1)$ and $|K : \mathbb{Q}|$.*

Proof. According to Remark II.14.18, we can assume $K \subseteq \mathbb{Q}_n$ with $n = |G|$. Since $\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ is abelian, $\mathrm{Gal}(\mathbb{Q}_n|K) \trianglelefteq \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ holds. According to the Fundamental Theorem of Galois Theory, $\mathbb{Q} \subseteq K$ is a Galois extension. Let $\mathrm{Gal}(K|\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_k\}$ with $k := |K : \mathbb{Q}|$ and $d := \chi(1)$. Then

$$\psi := \sum_{i=1}^{k} {}^{\sigma_i}\chi$$

is a character of degree dk with values in $\mathbb{Q}$. As algebraic integers, the values of ψ even lie in $\mathbb{Z}$. Obviously, ψ is also faithful, because the corresponding representation maps to block diagonal matrices. According to Lemma II.14.28, $\psi(g) \in \{-dk, \ldots, dk\}$ holds for all $g \in G$. In particular, ψ takes only

finitely many values $dk = x_0, \ldots, x_s$, where $s \leq 2dk$. Let $m_i := |\{g \in G : \psi(g) = x_i\}|$ for $0 \leq i \leq s$. Then $m_0 = 1$ holds, since ψ is faithful. Since ψ^l is a character, it holds that

$$\sum_{i=0}^{s} m_i x_i^l = \sum_{g \in G} \psi(g)^l = |G|(\psi^l, \mathbb{1}_G) \equiv 0 \pmod{|G|}$$

for $l = 0, 1, \ldots$. Thus $v = (m_0, \ldots, m_s)$ is a solution of the system of equations $Av \equiv 0 \pmod{|G|}$ with integer Vandermonde matrix $A := (x_j^i)_{i,j=0}^s$. Multiplication with the matrix complementary to A shows $\det(A)v \equiv 0 \pmod{|G|}$. Evaluation at the first coordinate yields

$$0 \neq \prod_{0 \leq i < j \leq s} (x_j - x_i) = m_0 \det(A) \equiv 0 \pmod{|G|}.$$

In particular,

$$|G| \leq \prod_{i<j} |x_j - x_i| \leq \prod_{t=1}^{2dk} t^{2dk-t+1} = \prod_{t=1}^{2dk} t!. \qquad \square$$

Example II.14.54. Let G be non-abelian and simple. Let $\mathbb{1}_G \neq \chi \in \mathrm{Irr}(G)$. Because of $\mathrm{Ker}(\chi) \lhd G$, χ is faithful. Because of $G' = G$, $\chi(1) > 1$ holds. Let us assume $\chi(1) = 2$. According to Theorem II.14.27, $|G|$ is even and according to Cauchy, there exists an involution $g \in G$. According to Example II.14.13, $\chi(g) = \epsilon_1 + \epsilon_2$ with $\epsilon_i \in \{\pm 1\}$. Because of $\mathrm{Ker}(\chi) = \mathrm{Z}(\chi) = 1$, $\epsilon_1 = -\epsilon_2$ holds according to Lemma II.14.28. But now $(\det \chi)(g) = \epsilon_1\epsilon_2 = -1$ and $\det \chi \neq \mathbb{1}_G$. This contradicts $G' = G$.

Lemma II.14.55. *Let $K \subseteq L$ be a separable field extension with $n := |L : K| < \infty$. Then there exist exactly n K-homomorphisms $\sigma_1, \ldots, \sigma_n \colon L \to \overline{K}$. Let $\Delta \colon L \to \mathrm{End}_K(L)$ be the regular representation (i. e. $\Delta(a)(x) = ax$ for $a, x \in L$). Then $\mathrm{tr}\,\Delta(a) = \sigma_1(a) + \ldots + \sigma_n(a)$ holds for all $a \in L$.*

Proof. According to the primitive element theorem, $L = K(x)$ holds for some $x \in L$. The minimal polynomial μ_x of x has degree n and pairwise distinct roots $x_1, \ldots, x_n \in \overline{K}$. Through $\sigma_i(x) := x_i$ one obtains all K-homomorphisms $L \to \overline{K}$. The matrix of $\Delta(x)$ with respect to the basis $1, x, \ldots, x^{n-1}$ is precisely the companion matrix B of μ_x. Since B has the characteristic polynomial μ_x, $x_1, \ldots, x_n$ are the eigenvalues of $\Delta(x)$. Therefore $\mathrm{tr}\,\Delta(x^i) = x_1^i + \ldots + x_n^i$ holds for $i = 0, \ldots, n-1$. Now let $a = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ with $a_0, \ldots, a_{n-1} \in K$. Then

$$\mathrm{tr}\,\Delta(a) = \sum_{i=0}^{n-1} a_i \,\mathrm{tr}\,\Delta(x^i) = \sum_{i=0}^{n-1} a_i \sum_{j=1}^{n-1} x_j^i = \sum_{j=1}^{n} \sum_{i=0}^{n-1} a_i x_j^i = \sum_{j=1}^{n} \sigma_j(a). \qquad \square$$

Example II.14.56. The regular representation of $\mathbb{C}$ as an $\mathbb{R}$-algebra with respect to the basis $1, \mathrm{i}$ is given by

$$\Delta \colon \mathbb{C} \to \mathbb{R}^{2\times 2}, \qquad a + b\mathrm{i} \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

with $\mathrm{tr}\,\Delta(x) = x + \overline{x} = 2\mathrm{Re}(x)$ for $x \in \mathbb{C}$.

Definition II.14.57. For a field $K \subseteq \mathbb{C}$ and a character χ of G we define

$$K(\chi) := K(\chi(g) : g \in G) \subseteq \mathbb{C}.$$

Remark II.14.58. In the situation of Definition II.14.57, $K(\chi) \subseteq K\mathbb{Q}_n$ holds with $n := |G|$. According to Theorem I.10.15, $K \subseteq K\mathbb{Q}_n$ is a Galois extension with abelian Galois group

$$\mathcal{G} := \mathrm{Gal}(K\mathbb{Q}_n|K) \cong \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}_n \cap K) \leq \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}).$$

Because of $\mathrm{Gal}(K\mathbb{Q}_n|K(\chi)) \trianglelefteq \mathcal{G}$, $K \subseteq K(\chi)$ is also a Galois extension. Let $\sigma \in \mathrm{Gal}(K(\chi)|K)$ with ${}^{\sigma}\chi = \chi$. Then $K(\chi) = K(\chi)^{\sigma}$ and the fundamental theorem of Galois theory implies $\sigma = 1$. Therefore the Galois-conjugate characters ${}^{\sigma}\chi$ with $\sigma \in \mathrm{Gal}(K(\chi)|K)$ are pairwise distinct.

Lemma II.14.59. *For distinct $\chi, \psi \in \mathrm{Irr}_K(G)$, $(\chi, \psi) = 0$ holds.*

Proof. Let M and N be simple KG-modules with respect to χ and ψ. According to Lemma II.14.6 and Theorem II.14.11, $M \not\cong N$. For a central-primitive idempotent $e \in KG$, $em = m$ and $en = 0$ holds for all $m \in M$ and $n \in N$. Let us assume indirectly $(\chi, \psi) \neq 0$. Then there exists a simple $\mathbb{C}G$-module V that occurs as a composition factor of M and N (viewed as $\mathbb{C}G$-modules). Since e cannot simultaneously operate trivially and as the identity on V, one has a contradiction. □

Theorem II.14.60. *Let $K \subseteq L$ be a finite field extension with $L \subseteq \mathbb{C}$ and Δ an absolutely irreducible L-representation with character χ. Then there exists exactly one $m \in \mathbb{N}$ with*

$$m \sum_{\sigma \in \mathrm{Gal}(K(\chi)|K)} {}^{\sigma}\chi \in \mathrm{Irr}_K(G).$$

In this case $m \mid |L : K(\chi)|$ holds.

Proof. Let $\Delta\colon G \to \mathrm{GL}(d, L)$ and $n := |L : K|$. Since Δ is absolutely irreducible, $\chi \in \mathrm{Irr}(G)$. The regular representation $\gamma\colon L \to \mathrm{End}_K(L) \cong K^{n\times n}$ extends to a homomorphism $\Gamma\colon L^{d\times d} \to K^{nd\times nd}$, $(x_{ij}) \mapsto (\gamma(x_{ij}))$. Therefore $\hat{\Delta} := \Gamma \circ \Delta\colon G \to \mathrm{GL}(nd \times nd)$ is a K-representation. For $g \in G$ let $\Delta(g) = (\delta_{ij}(g))$. According to Lemma II.14.55 there exist exactly n K-homomorphisms $\sigma_1, \ldots, \sigma_n\colon L \to \mathbb{C}$. For the character ψ of $\hat{\Delta}$ it holds that

$$\psi(g) = \mathrm{tr}\,\Gamma(\Delta(g)) = \sum_{i=1}^{d} \mathrm{tr}\,\gamma(\delta_{ii}(g)) = \mathrm{tr}\,\gamma(\chi(g)) = \sum_{i=1}^{n} \sigma_i(\chi(g)).$$

According to Remark II.14.58, $K \subseteq K(\chi)$ is a Galois extension. In particular, $\sigma_i(K(\chi)) = K(\chi)$ holds, i. e. the restriction of σ_i lies in $\mathcal{G} := \mathrm{Gal}(K(\chi)|K)$ for $i = 1, \ldots, n$. Each of the $|K(\chi) : K|$ elements of $\mathcal{G}$ possesses, according to the extension theorem, exactly $|L : K(\chi)|$ extensions to L. This shows

$$\psi = |L : K(\chi)| \sum_{\sigma \in \mathcal{G}} {}^{\sigma}\chi$$

We can now decompose ψ into characters of irreducible K-representations $\psi = \psi_1 + \ldots + \psi_k$. Let $\theta \in \mathrm{Irr}(G)$ be an irreducible constituent of ψ_i as a character over $\mathbb{C}$. Then there exists a $\sigma \in \mathcal{G}$ with $\theta = {}^{\sigma}\chi$. Because of $K(\psi_i) = K$, it holds that $(\psi_i, \theta) = (\psi_i, \chi)$. Thus there exist $m_1, \ldots, m_k$ with

$$\psi_i = m_i \sum_{\sigma \in \mathcal{G}} {}^{\sigma}\chi$$

for $i = 1, \ldots, k$. In the case $m_i \neq m_j$, it would be $m_i m_j |\mathcal{G}| = (\psi_i, \psi_j) = 0$ according to Lemma II.14.59. This shows $m := m_1 = \ldots = m_k$ and $m \mid km = m_1 + \ldots + m_k = |L : K(\chi)|$. □

Definition II.14.61. In the situation of Theorem II.14.60, $m_K(\chi) := m$ is called the *Schur index* of χ with respect to K (note that $m_K(\chi)$ does not depend on L).

Lemma II.14.62. *Let $\chi \in \mathrm{Irr}(G)$ and ψ be a character of a K-representation of G. Then $m_K(\chi) \mid (\chi, \psi)$ holds. In particular, $m_K(\chi) \mid \chi(1) \,\big|\, |G|$.*

Proof. Wlog. let $\psi \in \mathrm{Irr}_K(G)$ and $(\chi, \psi) \neq 0$. Because of $\hat{\chi} := m_K(\chi) \sum_{\sigma \in \mathrm{Gal}(K(\chi)|K)} {}^{\sigma}\chi \in \mathrm{Irr}_K(G)$, it holds that $\psi = \hat{\chi}$ according to Lemma II.14.59. Since the characters ${}^{\sigma}\chi$ are pairwise distinct according to Remark II.14.58, $(\chi, \psi) = m_K(\chi)$ holds. The second statement follows by choosing the regular character for ψ. □

Example II.14.63.

(i) For $\chi \in \mathrm{Irr}(G)$, $m_{\mathbb{R}}(\chi) \,\big|\, |\mathbb{C} : \mathbb{R}| = 2$ holds. For $\chi \in \mathrm{Irr}(Q_8)$ of degree 2, $m_{\mathbb{R}}(\chi) = 2$ holds (see Remark A.14.12).

(ii) For all $\chi \in \mathrm{Irr}(S_n)$, $m_{\mathbb{Q}}(\chi) = 1$ holds (Corollary III.4.20).

(iii) Fein has proven that $m_{\mathbb{Q}}(\chi)$ is a divisor of $n(\chi^n, \mathbb{1}_G)$ for all $n \in \mathbb{N}$. In the case $\chi = \overline{\chi}$, the theorem of Brauer-Speiser $m_{\mathbb{Q}}(\chi) \leq 2$ follows from this. In general, however, $m_{\mathbb{Q}}(\chi)$ can become arbitrarily large, where $m_{\mathbb{Q}}(\chi)^2$ is a divisor of $|G|$ according to Fein-Yamada.

(iv) Schur indices can in principle also be defined for fields of positive characteristic, however they are always equal to 1 there (without proof).

Exercises

Set Theory

Exercise II.1 $(1+1+2+2+2+2$ points$)$**.** Let A be an ordered set. Show:

(a) Every least element of A is minimal.

(b) A possesses at most one least element.

(c) If A is well-ordered, then A is also totally ordered.

(d) If A is finite and totally ordered, then A is also well-ordered.

(e) Construct a totally ordered set that is not well-ordered.

(f) Construct a well-ordering on $\mathbb{Z}$.

Exercise II.2 $(2+2+3$ points$)$**.** Let G be a finite group and $H \leq G$. Let $x_1, \ldots, x_n \in G$ be a system of representatives for the left cosets modulo H.

(a) Show that $x_1^{-1}, \ldots, x_n^{-1}$ is a system of representatives for the right cosets modulo H.

(b) Construct an example in which $x_1, \ldots, x_n$ is *not* a system of representatives for the right cosets modulo H.

(c) Show that there always exists a system of representatives for the left cosets modulo H that is simultaneously a system of representatives for the right cosets.
Hint: Hall's Marriage Theorem.

Ideals

Exercise II.3 (2 points)**.** Let K be a field and $n \in \mathbb{N}$. Determine all ideals of $K^{n\times n}$.

Exercise II.4 $(2+2+3$ points$)$**.** Let $R \neq \{0\}$ be a ring. A proper ideal $P \lhd R$ is called a *prime ideal*, if for all $I, J \trianglelefteq R$ it holds:

$$IJ \subseteq P \Rightarrow (I \subseteq P \vee J \subseteq P).$$

The set of prime ideals of R is called the *spectrum* of R and is written as $\operatorname{Spec}(R)$. Show:

(a) Every maximal ideal is a prime ideal. In particular, $\operatorname{Spec}(R) \neq \varnothing$.

(b) Not every prime ideal is maximal (example?).

(c) If R is commutative, then the following statements are equivalent:

(1) P is a prime ideal.

(2) For all $a, b \in R$ it holds: $ab \in P \Rightarrow a \in P \vee b \in P$.

(3) R/P is an integral domain.

Exercise II.5 $(2 + 2 + 2$ points$)$**.** Let R be a commutative ring. For $I \trianglelefteq R$ let

$$\mathcal{P}(I) := \{P \in \operatorname{Spec}(R) : I \subseteq P\}.$$

Show:

(i) $\mathcal{P}(\{0\}) = \operatorname{Spec}(R)$ and $\mathcal{P}(R) = \varnothing$.

(ii) For every family of ideals $(I_j)_{j \in J}$ it holds $\mathcal{P}(\sum I_j) = \bigcap_{j \in J} \mathcal{P}(I_j)$.

(iii) For $I, J \trianglelefteq R$ it holds $\mathcal{P}(IJ) = \mathcal{P}(I \cap J) = \mathcal{P}(I) \cup \mathcal{P}(J)$.

Remark: In this way one obtains the *Zariski topology* on $\operatorname{Spec}(R)$, where the $\mathcal{P}(I)$ for $I \trianglelefteq R$ are the closed sets. For $R = K[X_1, \ldots, X_n]$ there is a connection to the Zariski topology on K^n.

Exercise II.6 $(2 + 2 + 2$ points$)$**.** Let R and S be commutative rings.

(a) Show that $\operatorname{Spec}(R)$ is compact with respect to the Zariski topology (i. e. for every covering $\operatorname{Spec}(R) = \bigcup_{i \in I} A_i$ with open sets A_i there exists a finite subcovering).

(b) Let $f \colon R \to S$ be a ring homomorphism. Show $f^{-1}(P) \in \operatorname{Spec}(R)$ for all $P \in \operatorname{Spec}(S)$.

(c) Show that the map $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$, $P \mapsto f^{-1}(P)$ is continuous with respect to the Zariski topology (preimages of open sets are open).

Exercise II.7 $(1 + 2 + 2 + 3$ points$)$**.** Let R be a ring and $e \in R$ an idempotent ($e^2 = e$). Show:

(a) $1 - e$ is an idempotent.

(b) eRe is a ring with identity element e.
Remark: In the case $e \neq 1$, eRe is *not* a subring of R according to our definition.

(c) Every ideal of eRe has the form eIe with $I \trianglelefteq R$.

(d) If R consists only of idempotents, then R is commutative.
Hint: First show $1 + 1 = 0$ in R.
Remark: A generalization can be found in Theorem A.11.2.

Exercise II.8 (2 points)**.** Let I and J be nilpotent ideals of a ring R. Show that $I + J$ is nilpotent.

Exercise II.9 (3 points)**.** Let $K := \mathbb{Q}(\sqrt{-3})$. Determine the prime ideal factorization of $\mathbb{Z}_K 30$.

Exercise II.10 (2 points)**.** Let I be an ideal of a commutative ring R. One calls

$$\sqrt{I} := \{x \in R : \exists n \in \mathbb{N} : x^n \in I\}$$

the *radical* of I in R. For example, $\sqrt{\{0\}}$ is the set of nilpotent elements of R. Show $I \subseteq \sqrt{I} \trianglelefteq R$ and $\sqrt{I} = \sqrt{\sqrt{I}}$.

Exercise II.11 $(2+2+2+2$ points$)$**.** Let R be a commutative ring and $A, B, C \trianglelefteq R$. Show:

(a) $C \subseteq (A{:}B) \iff BC \subseteq A$.

(b) $((A{:}B){:}C) = (A{:}BC)$.

(c) $(A \cap B{:}C) = (A{:}C) \cap (B{:}C)$.

(d) $(A{:}B + C) = (A{:}B) \cap (A{:}C)$.

Exercise II.12 (2 points)**.** Determine the primary ideals and the radical ideals of $\mathbb{Z}$.

Exercise II.13 (2 points)**.** Let R be a commutative ring and $I \trianglelefteq R$. Prove or disprove the following statement: If $\sqrt{I}$ is a prime ideal, then I is primary.

Exercise II.14 (2 points)**.** Show that $(X^2, XY) = (X) \cap (X^2, XY, Y^2) = (X) \cap (X^2, Y)$ are two different primary decompositions in $K[X, Y, Z]$.

Field Extensions

Exercise II.15 $(2+2$ points$)$**.** Let $K := \mathbb{F}_4(X)$ and L a splitting field of $\alpha := Y^2 + X \in K[Y]$ over K.

(a) Show $|L : \mathbb{F}_2(X)| = 4$.

(b) Determine the separable closure of $\mathbb{F}_2(X)$ in L.

Exercise II.16 $(2+2$ points$)$**.** Show:

(a) A finite field extension $K \subseteq L$ is separable if and only if there exists a Galois extension $K \subseteq M$ with $L \subseteq M$.

(b) If $K \subseteq L$ and $L \subseteq M$ are purely inseparable field extensions, then the extension $K \subseteq M$ is also purely inseparable.

Exercise II.17 $(1+1+1+1$ points$)$**.** Show that for every field K the following statements are equivalent:

(a) K is perfect.

(b) Every finite field extension of K is separable.

(c) Every algebraic field extension of K is separable.

(d) The algebraic closure $\overline{K}$ of K coincides with the separable closure of K in $\overline{K}$.

Exercise II.18 (2 points)**.** Let $K \subseteq L$ be a finite, separable field extension and $\overline{K}$ the algebraic closure of K. Show that there exist exactly $|L : K|$ K-homomorphisms of the form $L \to \overline{K}$.

Exercise II.19 (1 + 1 + 2 + 2 points)**.** Show with the following steps that a finite field extension $K \subseteq L$ has a primitive element if and only if there are only finitely many fields between K and L:

(a) For one implication, one can argue as in the Primitive Element Theorem.

(b) Conversely, let $L = K(x)$ and $\mu \in K[X]$ be the minimal polynomial of x. For every field M with $K \subseteq M \subseteq L$, let μ_M be the minimal polynomial of x over M. Show that $\mu_M \mid \mu$.

(c) Show that $M = K(a_1, \ldots, a_n)$, where $a_1, \ldots, a_n$ are the coefficients of μ_M.

(d) Show that the map $M \mapsto \mu_M$ is injective and conclude that only finitely many M exist.

Exercise II.20 (2 points)**.** Let K be a field and G a finite group. Construct field extensions $K \subseteq L \subseteq M$ such that $L \subseteq M$ is a Galois extension with Galois group G.
Hint: $M := K(X_1, \ldots, X_{|G|})$.

Exercise II.21 (2 + 2 points)**.** Check whether the subset $\{\pi, X\}$ of $\mathbb{R}(X)$ is algebraically independent over $\mathbb{Q}(\sqrt{2})$. Is it a transcendence basis?

Exercise II.22 (3 points)**.** Let K be a field and $P \subseteq K[X]$ the set of irreducible polynomials. Show that

$$\left\{X^i : i \in \mathbb{N}_0\right\} \cup \left\{\frac{X^i}{\alpha^j} : \alpha \in P,\ 0 \leq i < \deg \alpha,\ j \in \mathbb{N}\right\}$$

is a K-basis of $K(X)$.
Hint: Partial fraction decomposition.

Exercise II.23 (2 + 2 + 2 + 2 + 2 + 2 points)**.** An algebraic field extension $K \subseteq L$ is called *normal*, if for every $a \in L$ the minimal polynomial $\mu_a \in K[X]$ splits completely into linear factors in $L[X]$. Show:

(a) Every purely inseparable field extension is normal.

(b) Every field extension of degree 2 is normal.

(c) Every algebraic extension of a finite field is normal.

(d) Every Galois extension is normal.
Hint: $\mathrm{Gal}(L|K)$ acts on the roots of μ_a.

(e) Every finite, separable, normal field extension is a Galois extension.

(f) There exist non-normal field extensions.

Divisibility

Exercise II.24 (4 + 3 points)**.**

(a) Which of the following polynomials are prime elements in $\mathbb{Z}[X]$:

$$-1,\ 2,\ -X^2,\ X + 1?$$

Hint: Lemma I.8.48.

(b) Show that

$$R := \Big\{ \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Z}[X] : a_1 = 0 \Big\}$$

is a subring of $\mathbb{Z}[X]$. Which of the powers X^n with $n \geq 2$ are irreducible or prime elements in R?

Exercise II.25 (2 points)**.** Show that the unit group of the ring

$$R := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$$

is infinite.
Hint: It suffices to find a unit with infinite order.

Exercise II.26 (2 points)**.** Investigate whether $X^2 - Y^2 + 2Y - 1$ is irreducible in $\mathbb{Z}[X, Y]$.

Exercise II.27 (2 points)**.** (EISENSTEIN) Let R be a factorial ring and $p \in R$ a prime element. Let

$$\alpha = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \in R[X]$$

be primitive with $p \mid a_0, \ldots, a_{n-1}$ and $p^2 \nmid a_0$. Show that α is irreducible.

Exercise II.28 (2 points)**.** Calculate a greatest common divisor of $5 + 3\mathrm{i}$ and $6 + 7\mathrm{i}$ in $\mathbb{Z}[\mathrm{i}]$.

Exercise II.29 ($1 + 1 + 1 + 1$ points)**.** Show that the rings

$$\mathbb{Z} + \mathbb{Z}\sqrt{-2}, \qquad \mathbb{Z} + \mathbb{Z}\sqrt{2}, \qquad \mathbb{Z} + \mathbb{Z}\sqrt{3}, \qquad \mathbb{Z} + \mathbb{Z}\frac{1 + \sqrt{-3}}{2}$$

are Euclidean.

Exercise II.30 ($1 + 2 + 2 + 3$ points)**.** A (formal) *power series* over a field K is a (possibly infinite) sum $\sum_{n=0}^{\infty} a_n X^n$ with $a_0, a_1, \ldots \in K$.

(a) Verify that the set $K[[X]]$ of all power series forms an integral domain, where addition and multiplication are defined as for polynomials.

(b) Show that $K[[X]]^\times = \big\{ \sum a_n X^n \in K[[X]] : a_0 \neq 0 \big\}$.

(c) Show that $K[[X]]$ becomes a Euclidean ring via

$$H(\alpha) := \begin{cases} \min\{n \in \mathbb{N} : a_{n-1} \neq 0\} & \text{if } \alpha \neq 0, \\ 0 & \text{if } \alpha = 0 \end{cases}$$

for $\alpha = \sum a_n X^n \in K[[X]]$.

(d) A (formal) *Laurent series* over K has the form $\sum_{n=k}^{\infty} a_n X^n$ with $k \in \mathbb{Z}$ (thus negative exponents are also allowed). Show that the set $K((X))$ of all Laurent series forms a field that is isomorphic to the quotient field $Q(K[[X]])$.
Hint: Use the universal property of $Q(K[[X]])$.

Exercise II.31 (2 points)**.** Let R be a Noetherian integral domain in which every irreducible element is a prime element. Show that R is factorial.
Hint: Proof of Theorem II.5.19.

Exercise II.32 (2 points)**.** Let $a, b, c, d \in \mathbb{N}$ with $a^2 + b^2 = c^2 + d^2 \in \mathbb{P}$. Show that $\{a, b\} = \{c, d\}$.
Remark: The representation of a prime number as a sum of two squares (Theorem II.5.34) is thus essentially unique.

Exercise II.33 ($2 + 2 + 2$ points)**.** Let

$$n = 2^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{2\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} p^{\delta_p}$$

be the prime factorization of $n \in \mathbb{N}$. Let

$$\chi \colon \mathbb{Z} \to \mathbb{Z}, \qquad n \mapsto \begin{cases} (-1)^{\frac{n-1}{2}} & \text{if } n \text{ is odd,} \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

Show that:

(a) $q(n) := |\{(a, b) \in \mathbb{Z}^2 : a^2 + b^2 = n\}| = 4 \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} (\delta_p + 1)$.

(b) $q(n) = 4 \sum_{d \mid n} \chi(d)$.

(c)
$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} \mp \ldots.$$

Hint: Count integer lattice points inside the circle with center $(0, 0)$ and radius r. Consider $r \to \infty$.

Modules

Exercise II.34 ($2 + 2$ points)**.** Let $R := \mathbb{Z}/6\mathbb{Z}$. Determine the simple R-modules up to isomorphism. What do the corresponding endomorphism rings look like?

Exercise II.35 ($2 + 2 + 2 + 2$ points)**.** We consider $\mathbb{Q}$ as a $\mathbb{Z}$-module. Show that:

(a) The rational numbers with odd denominator form a submodule of $\mathbb{Q}$.

(b) Every finitely generated submodule of $\mathbb{Q}$ is cyclic, i.e., of the form $\mathbb{Z}q$ for some $q \in \mathbb{Q}$.

(c) $\mathbb{Q}$ is not finitely generated and therefore not Noetherian.

(d) Investigate whether $\mathbb{Q}$ is Artinian.

Exercise II.36 (2 points)**.** Let R be an Artinian ring and $x \in R \setminus \{0\}$. Show that x is either a zero divisor or invertible.
Hint: Consider $Rx \supseteq Rx^2 \supseteq \ldots$.

Exercise II.37 $(2+2+2$ points$)$**.** Let K be a field and R the ring of upper triangular matrices in $K^{3\times 3}$.

(a) Determine a composition series of the regular R-module.

(b) How many simple R-modules are there up to isomorphism?

(c) Investigate whether the regular R-module is semisimple.

Hint: Exercise I.39.

Exercise II.38 $(2+2+2$ points$)$**.** Let R be a ring and M an R-module. The sum $\mathrm{Soc}(M)$ of all simple submodules of M is called the *socle* of M (this is the "largest" semisimple submodule of M). Show that:

(a) $\mathrm{Soc}(M \times N) = \mathrm{Soc}(M) \times \mathrm{Soc}(N)$ for R-modules M and N.

(b) For modules $N \leq M$, it holds that $\mathrm{Soc}(N) = N \cap \mathrm{Soc}(M)$ and $(\mathrm{Soc}(M) + N)/N \subseteq \mathrm{Soc}(M/N)$.

(c) The socle of the regular R-module is an ideal of R.

Exercise II.39 $(2+2+2$ points$)$**.** Let

$$R := \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a \in \mathbb{Z},\ b, c \in \mathbb{Q} \right\}.$$

Show:

(a) R is a subring of $\mathbb{Q}^{2\times 2}$.

(b) The regular R-left module is Noetherian, while the regular R-right module is not Noetherian.

(c) Conclude $R \ncong R^o$.
Remark: Compare Exercise III.37.

Exercise II.40 $(3+3$ points$)$**.** Show:

(a) An integral domain is a principal ideal domain if every prime ideal is a principal ideal.

(b) (Cohen) A commutative ring is Noetherian if every prime ideal is finitely generated.

Hint: Zorn's Lemma.

Exercise II.41 $(2$ points$)$**.** Let R be a ring. Show that the regular R-left module is semisimple if and only if the regular R-right module is semisimple.
Hint: Artin-Wedderburn.

Exercise II.42 $(2+2+2$ points$)$**.** Determine $\mathrm{J}(\mathbb{Z}/n\mathbb{Z})$, $\mathrm{J}(K[X])$ and $\mathrm{J}(K[[X]])$ for $n \in \mathbb{N}$ and every field K.

Exercise II.43 $(2+2+1+1$ points$)$**.** Let $N \subseteq R$ be the set of all nilpotent elements of a ring R. Show:

(a) If R is Artinian, then $\mathrm{J}(R) \subseteq N$.

(b) If R is commutative, then $N \trianglelefteq R$ and $N \subseteq \mathrm{J}(R)$.

(c) There are Artinian rings R with $\mathrm{J}(R) \subsetneq N$.

(d) There are commutative rings R with $N \subsetneq \mathrm{J}(R)$.
Hint: Exercise II.42.

Exercise II.44 (2 points)**.** Show that every Artinian integral domain is a field.

Exercise II.45 (2 + 2 points)**.** According to Exercise II.37, the ring R of upper triangular matrices in $K^{3\times 3}$ is Artinian for every field K. Determine $\mathrm{J}(R)$ and the smallest natural number k with $\mathrm{J}(R)^k = 0$.

Exercise II.46 (4 points)**.** Let R be a ring and $x \in R$. Show that the following statements are equivalent:

(1) $x \in \mathrm{J}(R)$.

(2) For all $r, s \in R$, $1 + rxs \in R^\times$.

Hint: Nakayama's Lemma with the regular R-module.

Exercise II.47 (2 + 2 points)**.** Let B be a block of an Artinian ring R with block idempotent e. Show $\mathrm{Z}(B) = \mathrm{Z}(R) \cap B = e\mathrm{Z}(R)e$ and $\mathrm{J}(B) = \mathrm{J}(R) \cap B = e\mathrm{J}(R)e$. Conclude that $\mathrm{Z}(B)$ is local.

Exercise II.48 (2 + 2 + 2 points)**.** Let K be a field and V a countably infinite-dimensional K-vector space (e. g. $V = K[X]$). Let $R := \mathrm{End}_K(V)$. Show:

(a) $I := \{f \in R : \dim f(V) < \infty\} \trianglelefteq R$.

(b) For every $f \in R \setminus I$, there exist $g, h \in R$ with $gfh = \mathrm{id}_V$.

(c) The ring R/I is simple, but not semisimple.

Exercise II.49 (2 points)**.** Show that the center of a simple ring is a field.

Modules over Principal Ideal Rings

Exercise II.50 (1 + 1 points)**.** Let R be a ring and M a free R-module. Prove or disprove the following statements:

(a) Every linearly independent subset of M can be extended to a basis of M.

(b) Every generating set of M contains a basis of M.

Exercise II.51 $(3+3$ points$)$**.**

(a) Determine the Smith normal form of

$$\begin{pmatrix} 8 & -25 & -16 \\ 43 & -131 & -86 \\ -20 & 61 & 40 \end{pmatrix} \in \mathbb{Z}^{3\times 3}.$$

(b) Let $N := \mathbb{Z}(4,5,6) + \mathbb{Z}(7,8,9) \leq \mathbb{Z}^3$. Determine the structure of $\mathbb{Z}^3/N$ according to Theorem II.9.30(ii) and (iii).

Exercise II.52 $(2+2$ points$)$**.** Show that the $\mathbb{Z}$-module $\mathbb{Q}$ is torsion-free but not free.
Remark: Therefore, Theorem II.9.30 is false for infinitely generated modules.

Exercise II.53 $(2+2+4+2+2$ points$)$**.** Let A and B be modules over a commutative ring R. Let F be the free R-module with basis $A \times B$. Let E be the submodule of F generated by the elements

$$\begin{aligned} &(a+a',b)-(a,b)-(a',b), && (a,a' \in A, b,b' \in B, r \in R)\\ &(a,b+b')-(a,b)-(a,b'),\\ &(ra,b)-r(a,b),\\ &(a,rb)-r(a,b). \end{aligned}$$

The quotient module F/E is called the *tensor product* of A and B and is written as $A \otimes_R B := F/E$. For $a \in A$ and $b \in B$ let $a \otimes b := (a,b) + E \in A \otimes_R B$. Show:

(a) For $a, a' \in A$, $b, b' \in B$ and $r \in R$ it holds that

$$\begin{aligned} (a+a') \otimes b &= a \otimes b + a' \otimes b,\\ a \otimes (b+b') &= a \otimes b + a \otimes b',\\ (ra) \otimes b &= r(a \otimes b) = a \otimes (rb). \end{aligned}$$

(b) (universal property) For every R-module M and every bilinear map $f\colon A \times B \to M$ there exists exactly one homomorphism $\hat{f}\colon A \otimes_R B \to M$ with $\hat{f}(a \otimes b) = f(a,b)$.

(c) For R-modules A, B and C it holds that

$$\begin{aligned} A \otimes_R B &\simeq B \otimes_R A,\\ A \otimes_R (B \otimes_R C) &\simeq (A \otimes_R B) \otimes_R C,\\ (A \times B) \otimes C &\simeq (A \otimes C) \times (B \otimes C),\\ R \otimes_R A &\simeq A. \end{aligned}$$

(d) For R-modules A, B and C it holds that

$$\mathrm{Hom}_R(A \otimes B, C) \simeq \mathrm{Hom}(A, \mathrm{Hom}_R(B,C))$$

(this means that Hom and $\otimes$ are adjoint functors to each other).

(e) If $f\colon A \to A'$ and $g\colon B \to B'$ are homomorphisms of R-modules, then there exists a homomorphism $f \otimes g\colon A \otimes B \to A' \otimes B'$ with $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$.

Exercise II.54 (3 points)**.** Determine the Frobenius normal form of

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \in \mathbb{F}_2^{4\times 4}.$$

Exercise II.55 (2 + 2 points)**.**

(a) Let $A \in \mathrm{GL}(3, \mathbb{Q})$ with finite order. Show that $|\langle A\rangle| \in \{1, 2, 3, 4, 6\}$.
Hint: Which minimal polynomials are possible?

(b) Let K be a finite field. Determine a system of representatives for the conjugacy classes of $\mathrm{GL}(2, K)$. Which of these matrices lie in $\mathrm{SL}(2, K)$?
Hint: Frobenius normal form.

Exercise II.56 (2 + 2 points)**.** Let $B \in K^{n\times n}$ be the companion matrix of $X^n + a_{n-1}X^{n-1} + \ldots + a_0$ and

$$S = \begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & 1 \\ a_2 & \cdots & a_{n-1} & 1 & \\ \vdots & \iddots & \iddots & & \\ a_{n-1} & 1 & & & \\ 1 & & & & 0 \end{pmatrix} \in \mathrm{GL}(n, K).$$

(a) Show that $S^{-1}BS = B^{\mathrm{t}}$.

(b) (Taussky) Deduce that every square matrix is the product of two symmetric matrices.

Exercise II.57 (2 + 2 points)**.**

(a) Construct a normal basis for $\mathbb{Q} \subseteq L$, where L is the splitting field of $X^3 - 2$ (cf. Exercise I.55).

(b) Let $p \in \mathbb{P}$ and $\zeta \in \mathbb{C}$ be a primitive p-th root of unity. Show that $\zeta, \ldots, \zeta^{p-1}$ is a normal basis of $\mathbb{Q}_p$ over $\mathbb{Q}$.

Exercise II.58 (2 + 2 + 2 + 2 points)**.** Decide which of the following ring extensions are integral:

$$\mathbb{Z} \subseteq \mathbb{Z}[X], \qquad \mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Z}[\sqrt[4]{2}], \qquad \mathbb{Q}[X] \subseteq \mathbb{Q}[X, \sqrt{2}], \qquad \mathbb{F}_3(1, 1) \subseteq \mathbb{F}_3 \times \mathbb{F}_3.$$

Exercise II.59 (2 points)**.** Let $R \subseteq S$ be an integral ring extension and $I \trianglelefteq S$. Show that $(R+I)/I \subseteq S/I$ is also an integral ring extension.

Algebras and Representations

Exercise II.60 (2 points)**.** Let A be a finite-dimensional K-algebra and M an A-module. Show that the following statements are equivalent:

(1) For every homomorphism $f\colon M \to P$ and every monomorphism $g\colon M \to N$ there exists a homomorphism $h\colon N \to P$ with $h \circ g = f$.

(2) For every monomorphism $f\colon P \to M$ there exists an $N \leq M$ with $M = f(P) \oplus N$.

If applicable, M is called *injective*.

Exercise II.61 (2 points)**.** Show that $\mathbb{H}$ is a strongly symmetric $\mathbb{R}$-algebra.

Exercise II.62 $(2+2+2$ points$)$**.** Let K be a field and G a finite group with $N \trianglelefteq G$. Show:

(a) The canonical epimorphism $G \to G/N$ induces an epimorphism of algebras $\nu_N\colon KG \to K[G/N]$.

(b) Determine a K-basis of $\mathrm{Ker}(\nu_N)$.

(c) $\mathrm{Ker}(\nu_N) = KG \cdot I(KN) = I(KN) \cdot KG$, where $I(KN)$ is the augmentation ideal of KN.

Exercise II.63 (3 points)**.** (Skolem-Noether) Let K be a field and $\gamma\colon K^{n\times n} \to K^{n\times n}$ an isomorphism of algebras. Show that there exists an $x \in K^{n\times n}$ with $\gamma(a) = xax^{-1}$ for all $a \in K^{n\times n}$.
Hint: K^n becomes a simple $K^{n\times n}$-module via $av = v$ as well as via $av = \gamma(a)v$.

Exercise II.64 $(2+2+2$ points$)$**.** Let $A := \mathbb{F}_2 S_3$.

(a) Verify that

$$1 = \underbrace{1 + (12) + (23) + (123)}_{=:e_1} + \underbrace{1 + (12) + (23) + (132)}_{=:e_2} + \underbrace{1 + (123) + (132)}_{=:e_3}$$

is a decomposition into pairwise orthogonal primitive idempotents of A.

(b) Conclude that $(12) + (23) + (132)$ is a basic idempotent of A.

(c) Show that $e_1\mathrm{Z}(A)e_1 \neq \mathrm{Z}(e_1Ae_1)$.

Exercise II.65 (3 points)**.** (Higman) Let K be a field and $H \leq G$ finite groups with $p \nmid |G : H|$. Let V be a KG-module such that the restriction V_H is semisimple. Show that V is semisimple.
Remark: The case $V = KG$ and $H = 1$ implies one direction of Maschke's theorem.

Exercise II.66 $(2+2+1$ points$)$**.** Let G be a cyclic group of order $n < \infty$ and K be a field. Show that the K-algebras KG and $K[X]/(X^n - 1)$ are isomorphic. Conclude that

$$\mathbb{Q}G \cong \bigtimes_{d|n} \mathbb{Q}_d.$$

Calculate the degrees of the irreducible $\mathbb{Q}$-representations of G.
Hint: Chinese Remainder Theorem for rings.

Exercise II.67 (2 points)**.** Let K be a field and G a finite group. Show that a finitely generated KG-module M is projective if and only if M is injective.

Exercise II.68 (2 points)**.** Let K be a field and $n \in \mathbb{N}$. Show that $\mathrm{C}_{\mathrm{GL}(n,K)}(\mathrm{SL}(n,K)) = K1_n$.

Exercise II.69 (3 points)**.** Show that the dihedral group D_8 and the quaternion group Q_8 have the same character table (with a suitable ordering).

Exercise II.70 (2 + 2 points)**.** Let $\Delta\colon G \to \mathrm{GL}(n,\mathbb{C})$, $\Gamma\colon G \to \mathrm{GL}(m,\mathbb{C})$ be irreducible matrix representations and $A \in \mathbb{C}^{n\times m}$ with $A\Gamma(g) = \Delta(g)A$ for all $g \in G$. Show:

(a) If Δ and Γ are not similar, then $A = 0$.

(b) If $\Delta = \Gamma$, then $A \in \mathbb{C}1_n$.

Exercise II.71 (2 + 2 + 2 + 2 points)**.**

(a) Show that for $n \in \mathbb{N}$ the map $P\colon S_n \to \mathrm{GL}(n,\mathbb{C})$, $\sigma \mapsto (\delta_{i,\sigma(j)})_{i,j=1}^n$ is a representation of S_n. $P(\sigma)$ is called the *permutation matrix* associated with σ.

(b) According to Remark I.4.2, every action of a group G induces a homomorphism $G \to S_n$. Composition with P yields a representation $\Delta\colon G \to \mathrm{GL}(n,\mathbb{C})$. Describe the character χ of Δ.

(c) Show that $(\chi, \mathbb{1}_G)$ is the number of orbits of the action. In particular, $\chi - \mathbb{1}_G$ is always a character of G.

(d) Calculate $\chi - \mathbb{1}_G$ for the natural action of $G = S_4$ on $\{1,\dots,4\}$ and show that this character is irreducible.

Exercise II.72 (2 points)**.** Let K be a field, $A \in K^{n\times n}$ and $B \in K^{m\times m}$. Show for the Kronecker product that $\det(A \otimes B) = \det(A)^m \det(B)^n$.
Hint: Gaussian elimination.

Exercise II.73 (2 points)**.** If χ and ψ are characters of G, then $\det(\chi\psi) = \det(\chi)^{\psi(1)} \det(\psi)^{\chi(1)}$.

Exercise II.74 (2 + 2 + 2 points)**.** Show for $G = S_n$:

(a) $g, h \in G$ are conjugate if and only if they have the same cycle type.

(b) Every $g \in G$ is conjugate to all generators of $\langle g\rangle$.

(c) The character table of G is integer-valued.
Hint: Brauer's permutation lemma.

Exercise II.75 (2 points)**.** Let $\chi \in \mathrm{Irr}(G)$, $g \in G$ and $z \in \mathrm{Z}(\chi)$. Show that $\chi(gz) = \frac{\chi(z)}{\chi(1)}\chi(g)$.

Exercise II.76 (3 points)**.** A *character Sudoku*: Complete the following character table, in which the first column belongs to the trivial element:

χ_1					
χ_2					
χ_3					
χ_4	1	-1	1	1	i
χ_5	2	2	2	-1	0
χ_6					
χ_7	3	3	-1	0	1
χ_8					
χ_9					
χ_{10}					

Algebra III

III.1 Commutative Algebra

Remark III.1.1. As a continuation of chapter II.11, we study commutative rings R that are not necessarily domains. If R is Noetherian, a substitute for prime factorization and prime ideal decomposition can be constructed using primary decomposition. Subsequently, we develop a notion of dimension, which will be interpreted geometrically in the next chapter.

Theorem III.1.2 (Hilbert's Basis Theorem)**.** *If R is commutative and Noetherian, then so is $R[X]$.*

Proof. Suppose that $I \trianglelefteq R[X]$ is not finitely generated. Let $f_0 := 0 \in R[X]$. For $k \geq 1$, we inductively choose $f_k \in I \setminus (f_0, \ldots, f_{k-1})$ with minimal degree d_k. Then certainly $0 \leq d_1 \leq d_2 \leq \ldots$. Let $a_k \in R$ be the leading coefficient of f_k, i. e. $f_k = a_k X^{d_k} + \ldots$. By assumption, $(a_1) \subseteq (a_1, a_2) \subseteq \ldots$ becomes stationary. In particular, there exists a $k \in \mathbb{N}$ with $a_k = \sum_{i=1}^{k-1} r_i a_i$ for certain $r_i \in R$. Define

$$g_k := f_k - \sum_{i=1}^{k-1} r_i X^{d_k - d_i} f_i.$$

Then $g_k \in I \setminus (f_0, \ldots, f_{k-1})$, but $\deg g_k < d_k$ in contradiction to the choice of f_k. □

Definition III.1.3. A subset S of a ring R is called *multiplicatively closed*, if $1 \in S$, $0 \notin S$ and $xy \in S$ for all $x, y \in S$.

Lemma III.1.4. *Let R be a commutative ring and $S \subseteq R$ multiplicatively closed. Then:*

(i) By

$$(r, s) \sim (r', s') \iff \exists t \in S : t(rs' - r's) = 0$$

an equivalence relation on $R \times S$ is defined. Let $[r, s]$ be the equivalence class of (r, s).

(ii) By

$$[r, s] + [r', s'] := [rs' + r's, ss'],$$
$$[r, s] \cdot [r', s'] := [rr', ss']$$

the set of equivalence classes becomes a commutative ring $R[S^{-1}]$ with $0 := [0, 1]$ and $1 := [1, 1]$.

(iii) The map $\Phi \colon R \to R[S^{-1}]$, $r \mapsto [r, 1]$ is a ring homomorphism with $\Phi(S) \subseteq R[S^{-1}]^\times$.

Proof.

(i) Reflexivity and symmetry are obvious. Let $(r, s) \sim (r', s') \sim (r'', s'')$ and $t, t' \in S$ with $t(rs' - r's) = 0 = t'(r's'' - r''s')$. Then $tt's' \in S$ with

$$tt's'(rs'' - r''s) = (trs')t's'' - (t'r''s')ts = (tr's)t's'' - (t'r's'')ts = 0.$$

This shows $(r, s) \sim (r'', s'')$.

(ii) For well-definedness, let $[a,b] = [a',b']$, $[c,d] = [c',d']$ and $s,t \in S$ with $s(ab' - a'b) = 0$ and $t(cd' - c'd) = 0$. Then it holds that

$$st((ad+cb)b'd' - (a'd' + c'b')bd) = tdd's(ab' - a'b) + sbb't(cd' - c'd) = 0$$

and $[a,b] + [c,d] = [ad+cb, bd] = [a'd' + c'b', b'd'] = [a',b'] + [c',d']$. Analogously,

$$\begin{aligned} st(acb'd' - a'c'bd) &= st(acb'd' - a'bcd' + a'bcd' - a'c'bd) \\ &= tcd's(ab' - a'b) + sa'bt(cd' - c'd) = 0 \end{aligned}$$

and $[a,b][c,d] = [ac, bd] = [a'c', b'd'] = [a',b'][c',d']$. Obviously, both operations are commutative and the multiplication is associative. For the addition, it holds that

$$\begin{aligned} ([a,b] + [c,d]) + [e,f] = [ad+cb, bd] + [e,f] = [(ad+cb)f + ebd, bdf] = [adf + (cf+ed)b, bdf] \\ = [a,b] + [cf+ed, df] = [a,b] + ([c,d] + [e,f]). \end{aligned}$$

Certainly $[0,1]$ is neutral with respect to $+$ and $[1,1]$ is neutral with respect to $\cdot$. Furthermore, $[a,b] + [-a,b] = [0,1]$ holds. The distributive law follows from

$$\begin{aligned} [a,b]([c,d] + [e,f]) = [a,b][cf+ed, df] = [a(cf+ed), bdf] = [acbf + aebd, b^2df] \\ = [ac,bd] + [ae,bf] = [a,b][c,d] + [a,b][e,f]. \end{aligned}$$

(iii) It holds that $\Phi(1) = [1,1] = 1$, $\Phi(a+b) = [a+b,1] = [a,1] + [b,1]$ and $\Phi(ab) = [ab,1] = [a,1][b,1]$. For $s \in S$, it holds that $[s,1][1,s] = 1$. Therefore, $\Phi(s)$ is a unit in $R[S^{-1}]$. □

Definition III.1.5. One calls $R[S^{-1}]$ the *localization* of R at S.

Remark III.1.6.

(i) The definition of $\sim$ states that $[r,s]$ is uniquely determined up to "expanding and canceling".

(ii) If R is an integral domain, one can always choose $t = 1$ in the definition of $\sim$. In this case, Φ is injective and we write $\frac{r}{s}$ instead of $[r,s]$. The choice $S = R \setminus \{0\}$ yields the field of fractions $R[S^{-1}] = Q(R)$ of R and Φ is the canonical embedding from Exercise I.40. For a smaller subset S, one can view $R[S^{-1}]$ as a ring adjunction in $R \subseteq Q(R)$ (the use of square brackets is therefore consistent).

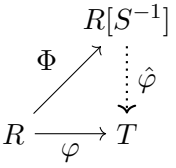
(iii) The elements of S are made invertible by means of Φ in Lemma III.1.4. This explains the notation $R[S^{-1}]$. If S already consists of units, then Φ is an isomorphism and nothing has been gained. Indeed, if $[r,1] = [0,1]$, then there exists $t \in S$ with $tr = 0$. This shows $r = t^{-1}tr = 0$. If $[r,s] \in R[S^{-1}]$ is arbitrary, then $[r,s] = [rs^{-1}, 1] \in \Phi(R)$ holds.

Example III.1.7.

(i) Let $x \in R \setminus \{0\}$ and $S = \{x^n : n \in \mathbb{N}_0\} \setminus \{0\}$. Then $R[x^{-1}] := R[S^{-1}]$ is called the localization of R at x. For $R = K[X]$ and $x = X$ one obtains the ring of *Laurent polynomials* $K[X, X^{-1}]$.

(ii) If $P \trianglelefteq R$ is a prime ideal, then one can choose $S = R \setminus P$. One then writes $R_P := R[S^{-1}]$. Obviously $R_P P := (\Phi(P)) = \{[r,s] : r \in P, s \notin P\} \trianglelefteq R_P$. For $R = \mathbb{Z}$ and $P = (p)$ with $p \in \mathbb{P}$ one obtains $\mathbb{Z}_{(p)} = \{\frac{a}{b} : a,b \in \mathbb{Z}, p \nmid b\}$.

Theorem III.1.8 (Universal property)**.** *Let $\varphi\colon R \to T$ be a homomorphism of commutative rings. Let $S \subseteq R$ be multiplicatively closed with $\varphi(S) \subseteq T^\times$. Then there exists exactly one ring homomorphism $\hat{\varphi}\colon R[S^{-1}] \to T$ with $\hat{\varphi}([r,1]) = \varphi(r)$ for all $r \in R$.*



Proof. For $[a,b] \in R[S^{-1}]$ let $\hat{\varphi}([a,b]) := \varphi(a)\varphi(b)^{-1} \in T$. Let $[a,b] = [c,d]$, $s \in S$ with $s(ad - cb) = 0$. Then it follows $\varphi(s)\varphi(a)\varphi(b)^{-1} = \varphi(s)\varphi(c)\varphi(d)^{-1}$. Because of $\varphi(s) \in T^\times$ it follows $\hat{\varphi}([a,b]) = \varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1} = \hat{\varphi}([c,d])$, i. e. $\hat{\varphi}$ is well-defined. Certainly $\hat{\varphi}([1,1]) = 1$ and $\hat{\varphi}([a,b][c,d]) = \hat{\varphi}([a,b])\hat{\varphi}([c,d])$. Finally, it holds

$$\begin{aligned}\hat{\varphi}([a,b] + [c,d]) &= \hat{\varphi}([ad + cb, bd]) = \varphi(ad + cb)\varphi(bd)^{-1} \\ &= \varphi(a)\varphi(b)^{-1} + \varphi(c)\varphi(d)^{-1} = \hat{\varphi}([a,b]) + \hat{\varphi}([c,d]).\end{aligned}$$

Thus $\hat{\varphi}$ is a ring homomorphism. Let also $\gamma\colon R[S^{-1}] \to T$ be a homomorphism with $\gamma([a,1]) = \varphi(a)$ for all $a \in R$. Then it holds

$$\gamma([a,b]) = \gamma([a,1][1,b]) = \gamma([a,1])\gamma([b,1])^{-1} = \varphi(a)\varphi(b)^{-1} = \hat{\varphi}([a,b])$$

for all $[a,b] \in R[S^{-1}]$. This shows $\gamma = \hat{\varphi}$. □

Theorem III.1.9. *With the notation from Lemma III.1.4, the maps*

$$P \mapsto \Phi^{-1}(P), \qquad Q \mapsto (\Phi(Q))$$

are mutually inverse bijections between the set of prime ideals of $R[S^{-1}]$ and the set of prime ideals of R disjoint from S.

Proof. For a prime ideal $P \trianglelefteq R[S^{-1}]$, $\Phi^{-1}(P) \trianglelefteq R$ is also a prime ideal, since Φ is a homomorphism. Suppose there exists $s \in S \cap \Phi^{-1}(P)$. Then $\Phi(s) \in P \cap R[S^{-1}]^\times$ and one obtains the contradiction $P = R[S^{-1}]$. Thus $\Phi^{-1}(P) \cap S = \varnothing$. It is obvious that $(\Phi(\Phi^{-1}(P))) \subseteq P$. Conversely, let $[r,s] \in P$. Then $[r,1] = [s,1][r,s] \in P$, so $r \in \Phi^{-1}(P)$ and $[r,s] = [1,s][r,1] \in (\Phi(\Phi^{-1}(P)))$. This shows $(\Phi(\Phi^{-1}(P))) = P$.

Conversely, let $Q \trianglelefteq R$ be a prime ideal with $Q \cap S = \varnothing$. By definition, $(\Phi(Q)) \trianglelefteq R[S^{-1}]$. In the case $(\Phi(Q)) = R[S^{-1}]$, $\Phi(Q)$ contains a unit, say $[q,1]$. Let $[rq,s] = [r,s][q,1] = 1$. Then there exists $t \in S$ with $t(rq - s) = 0$. This yields the contradiction $st = trq \in S \cap Q = \varnothing$. Thus $(\Phi(Q))$ is a proper ideal. Let $[a,b],[c,d] \in R[S^{-1}]$ with $[ac,bd] = [a,b][c,d] \in (\Phi(Q))$. Let $[r,s] \in R[S^{-1}]$ and $q \in Q$ with $[ac,bd] = [rq,s]$. Again, there exists $t \in S$ with $t(acs - rqbd) = 0$. From $acst = rbdq \in Q$ it follows that $ac \in Q$, since Q is a prime ideal and $st \in S$. Wlog. let $a \in Q$. Then $[a,b] = [a,1][1,b] \in (\Phi(Q))$. Thus $(\Phi(Q))$ is a prime ideal of $R[S^{-1}]$ with $Q \subseteq \Phi^{-1}((\Phi(Q)))$. Finally, let $x \in \Phi^{-1}((\Phi(Q)))$. Then there exist $q \in Q$ and $[r,s] \in R[S^{-1}]$ with $[x,1] = [r,s][q,1] = [rq,s]$. Let $t \in S$ with $t(xs - rq) = 0$. From $xst = trq \in Q$ it follows that $x \in Q$. This shows $\Phi^{-1}((\Phi(Q))) = Q$. □

Theorem III.1.10. *Let R be a commutative, Noetherian ring and $S \subseteq R$ multiplicatively closed. Then $R[S^{-1}]$ is Noetherian.*

Proof. For $I \trianglelefteq R[S^{-1}]$, $J := \Phi^{-1}(I) \trianglelefteq R$ is finitely generated, say $J = Rx_1 + \ldots + Rx_n$. With $[r,s] \in I$, also $[r,1] = [s,1][r,s] \in I$ and $y \in J$. Then there exist $r_1, \ldots, r_n \in R$ with $r = r_1x_1 + \ldots + r_nx_n$. It follows that $[r,s] = [r_1,s][x_1,1] + \ldots + [r_n,s][x_n,1]$. Therefore I is generated by $[x_1,1], \ldots, [x_n,1]$. This shows that every (left) ideal of $R[S^{-1}]$ is finitely generated. □

Remark III.1.11. A commutative ring R is obviously local if and only if $R/\mathrm{J}(R)$ is a field (cf. Theorem II.12.11).

Theorem III.1.12. *For every prime ideal P of a commutative ring R, R_P is local with $\mathrm{J}(R_P) = R_P P$ and $R_P/\mathrm{J}(R_P) \cong Q(R/P)$.*

Proof. According to Theorem III.1.9, the prime ideals of R_P correspond to the prime ideals of R that are contained in P. Therefore, $R_P P = (\Phi(P))$ must be the unique maximal ideal of R_P.

The canonical ring homomorphism $\varphi\colon R \to R/P \hookrightarrow Q(R/P)$, $r \mapsto r+P$ satisfies $\varphi(R \setminus P) \subseteq Q(R/P)^\times$. According to the universal property, it can be extended to

$$\hat{\varphi}\colon R_P \to Q(R/P), \qquad [r,s] \mapsto \frac{r+P}{s+P}.$$

Because of $Q(R)^\times = \{s+P : s \in R \setminus P\}$, $\hat{\varphi}$ is surjective. According to the isomorphism theorem, $\mathrm{Ker}(\hat{\varphi})$ must be a maximal ideal, i. e. $\mathrm{Ker}(\hat{\varphi}) = \mathrm{J}(R_P)$ and $R_P/\mathrm{J}(R_P) \cong Q(R/P)$. □

Remark III.1.13. Let R be commutative and $I \trianglelefteq R$. In Exercise II.10, the *radical*

$$\sqrt{I} := \{x \in R : \exists n \in \mathbb{N} : x^n \in I\} \trianglelefteq R$$

of I was introduced. It holds that $I \subseteq \sqrt{I} = \sqrt{\sqrt{I}}$ and $I = R \Leftrightarrow \sqrt{I} = R$.

Lemma III.1.14. *Let R be commutative and Noetherian. For every ideal $I \trianglelefteq R$, there exists an $n \in \mathbb{N}$ with $\sqrt{I}^n \subseteq I$.*

Proof. Since R is Noetherian, $\sqrt{I}$ is finitely generated, say $\sqrt{I} = (x_1, \ldots, x_k)$. Let $x_i^{n_i} \in I$ for $i = 1, \ldots, k$ and $n := n_1 + \ldots + n_k$. For $r_1 x_1 + \ldots + r_k x_k \in \sqrt{I}$, it then holds that

$$(r_1 x_1 + \ldots + r_k x_k)^n = \sum_{\substack{(i_1,\ldots,i_k) \in \mathbb{N}_0^k \\ i_1+\ldots+i_k = n}} \binom{n}{i_1, \ldots, i_k} r_1^{i_1} x_1^{i_1} \ldots r_k^{i_k} x_k^{i_k} \in I,$$

because for at least one j, $i_j \geq n_j$. This shows $\sqrt{I}^n \subseteq I$. □

Theorem III.1.15. *For every ideal I of a commutative ring R, $\sqrt{I}$ is the intersection of all prime ideals of R that contain I.*

Proof. Let $x \in \sqrt{I}$ with $x^n \in I$. For every prime ideal $P \supseteq I$, it then holds that $x \in P$. Now let $x \in R \setminus \sqrt{I}$. Using Zorn's Lemma, one easily shows that $\{J \trianglelefteq R : I \subseteq J, x^n \notin J \forall n \in \mathbb{N}\}$ has a maximal element P. Suppose there exist $a, b \in R \setminus P$ with $ab \in P$. Then there exist $n, m \in \mathbb{N}$ with $x^n \in (P, a)$ and $x^m \in (P, b)$. Let $r, s \in R$ and $p, q \in P$ with $x^n = p + ra$ and $x^m = q + sb$. Then one obtains the contradiction $x^{n+m} = (p+ra)(q+sb) = pq + raq + psb + rsab \in P$. Thus P is a prime ideal with $x \notin P$. □

Definition III.1.16. Let R be commutative and $I \trianglelefteq R$. One calls I

- a *radical ideal*, if $I = \sqrt{I}$, i. e. from $x^n \in I$ it follows that $x \in I$ for all $x \in R$ and $n \in \mathbb{N}$.
- *primary*, if $I \neq R$ and for all $x, y \in R$ it holds: From $xy \in I$ it follows that $x \in I$ or $y \in \sqrt{I}$.

Remark III.1.17.

(i) The condition $xy \in I \Rightarrow x \in I \vee y \in \sqrt{I}$ naturally also holds for yx. It can therefore be formulated symmetrically: $xy \in I \Rightarrow x \in I \vee y \in I \vee x, y \in \sqrt{I}$.

(ii) According to Theorem III.1.15, every radical ideal is an intersection of prime ideals. Conversely, it is easy to see that every intersection of prime ideals is a radical ideal.

Example III.1.18.

(i) The prime ideals of R are exactly the primary radical ideals.

(ii) The ideal $(4) \trianglelefteq \mathbb{Z}$ is primary, but neither a prime ideal nor a radical ideal.

(iii) The ideal $(2) \times (0) \trianglelefteq \mathbb{Z} \times \mathbb{Z}$ is a radical ideal, but neither a prime ideal nor primary.

Lemma III.1.19. *If $I \trianglelefteq R$ is primary, then $\sqrt{I}$ is a prime ideal.*

Proof. Let $x, y \in R$ with $xy \in \sqrt{I}$. Then there exists $n \in \mathbb{N}$ with $x^n y^n \in I$. It follows that $x^n \in I$ or $y^{nm} \in I$ for some $m \in \mathbb{N}$. This shows $x \in \sqrt{I}$ or $y \in \sqrt{I}$. Thus $\sqrt{I}$ is a prime ideal. □

Definition III.1.20. Let R be commutative, $I \trianglelefteq R$ and $S \subseteq R$. We define

$$(I{:}S) := \{r \in R : \forall s \in S : rs \in I\}.$$

One easily shows: $I \subseteq (I{:}S) \trianglelefteq R$. For $S = \{s\}$ we write $(I{:}s)$ instead of $(I{:}S)$. The prime ideals of the form $(I{:}s)$ are called the prime ideals *associated* with I.

Theorem III.1.21 (Lasker-Noether)**.** *Let R be commutative and Noetherian. For every ideal $I \trianglelefteq R$ there exist primary ideals $P_1, \ldots, P_n \trianglelefteq R$ with $I = P_1 \cap \ldots \cap P_n$, $\bigcap_{j \neq i} P_j \nsubseteq P_i$ for $i = 1, \ldots, n$ and $\sqrt{P_i} \neq \sqrt{P_j}$ for $i \neq j$. In this case, $\sqrt{P_1}, \ldots, \sqrt{P_n}$ are the prime ideals associated with I. In particular, n is uniquely determined.*

Proof.
Existence: In the case $I = R$, the claim holds with $n = 0$. Let $\mathcal{M}$ be the set of ideals that cannot be written as an intersection of primary ideals. Assume $\mathcal{M} \neq \varnothing$. Since R is Noetherian, there exists a maximal element $M \in \mathcal{M}$. If there exist $I, J \trianglelefteq R$ with $I \neq M \neq J$ and $M = I \cap J$, then $I, J \notin \mathcal{M}$. But then I and J are intersections of primary ideals and thus so is M. Therefore, M is not an intersection of larger ideals. We show that M itself is primary. For this, let $x, y \in R$ with $xy \in M$ and $y \notin \sqrt{M}$. Obviously, $M \subseteq (M{:}y) \subseteq (M{:}y^2) \subseteq \ldots$ holds. Since R is Noetherian,

$$I := (M{:}y^n) = (M{:}y^{n+1}) = \ldots$$

holds for some $n \in \mathbb{N}$. Let $J := M + (y^n) \trianglelefteq R$ and $r \in I \cap J$. Then there exist $s \in R$ and $t \in M$ with $r = t + sy^n$ and $ty^n + sy^{2n} = ry^n \in M$. It follows that $sy^{2n} \in M$ and $s \in (M{:}y^{2n}) = (M{:}y^n) = I$. Now $r = t + sy^n \in M$ and $I \cap J = M$. From the first part of the proof, it follows that $I = M$, because $y^n \in J \setminus M$. Thus $x \in (M{:}y) \subseteq I \subseteq M$ holds and M is primary. This yields the contradiction $M \notin \mathcal{M}$. Every ideal I is therefore an intersection of primary ideals $P_1, \ldots, P_n$.

In the case $\bigcap_{j \neq i} P_j \subseteq P_i$ for some i, one removes P_i without changing the intersection. Let $\sqrt{P_i} = \sqrt{P_j}$ with $i \neq j$. Let $x, y \in R$ with $xy \in P_i \cap P_j$. Then $x \in P_i \cap P_j$ or $y \in \sqrt{P_i} = \sqrt{P_j} = \sqrt{P_i \cap P_j}$ holds. Thus

$P_i \cap P_j$ is primary and we can replace P_i, P_j by $P_i \cap P_j$. After finitely many replacements, $\sqrt{P_i} \neq \sqrt{P_j}$ holds for $i \neq j$.

Uniqueness: Let $1 \leq i \leq n$ and $Q_i := \bigcap_{j \neq i} P_j$ (for $n = 1$ let $Q_i = R$). According to Lemma III.1.14, $\sqrt{P_i}^m \subseteq P_i$ and $\sqrt{P_i}^m Q_i \subseteq P_i \cap Q_i = I$ hold if m is large enough. Let m be minimal with $\sqrt{P_i}^m Q_i \subseteq I$. Then there exists $y \in \sqrt{P_i}^{m-1} Q_i \setminus I$ (if necessary $m = 1$). We show $\sqrt{P_i} = (I{:}y)$. Because $y \notin I$, we have $y \in Q_i \setminus P_i$. For $r \in R$ with $yr \in I \subseteq P_i$, it follows that $r \in \sqrt{P_i}$ since P_i is primary. This shows $(I{:}y) \subseteq \sqrt{P_i}$. Conversely, $\sqrt{P_i} y \subseteq \sqrt{P_i}^m Q_i \subseteq I$ holds, so $\sqrt{P_i} \subseteq (I{:}y)$.

It remains to show that every prime ideal $(I{:}r)$ associated to I appears among the $\sqrt{P_i}$. In the case $r \in I$, $(I{:}r) = R$ would not be a prime ideal. So let $r \notin I$. Then $Q := \prod_{r \notin P_i} P_i \neq R$ is not the empty product. It follows that $Qr \subseteq P_1 \cap \ldots \cap P_n = I$ and $Q \subseteq (I{:}r)$. Since $(I{:}r)$ is a prime ideal, it follows that $P_i \subseteq (I{:}r)$ for some i with $r \notin P_i$. It follows that $\sqrt{P_i} \subseteq \sqrt{(I{:}r)} = (I{:}r)$. Conversely, let $s \in R$ with $rs \in I \subseteq P_i$. Then $s \in \sqrt{P_i}$ follows, since P_i is primary. This shows $(I{:}r) \subseteq P_i$. □

Remark III.1.22. One calls $I = P_1 \cap \ldots \cap P_n$ in Theorem III.1.21 a *primary decomposition* of I. In general, the primary ideals $P_1, \ldots, P_n$ are not uniquely determined (Exercise II.14). However, if I is a radical ideal, then according to Theorem III.1.15 one can choose prime ideals for $P_1, \ldots, P_n$. It then holds that $\sqrt{P_i} = P_i$ for $i = 1, \ldots, n$.

Example III.1.23.

(i) Let R be a factorial ring and $x = p_1^{a_1} \ldots p_n^{a_n} \in R$ a prime factorization. Then $(x) = (p_1^{a_1}) \cap \ldots \cap (p_n^{a_n})$ is a primary decomposition with $\sqrt{(p_i^{a_i})} = (p_i)$ for $i = 1, \ldots, n$.

(ii) Let R be a Dedekind domain and $I = P_1^{a_1} \ldots P_n^{a_n} \trianglelefteq R$ a prime ideal factorization. Then $I = P_1^{a_1} \cap \ldots \cap P_n^{a_n}$ is a primary decomposition with $\sqrt{P_i^{a_i}} = P_i$ for $i = 1, \ldots, n$. The primary decomposition can therefore be viewed as a common generalization of prime factorization and prime ideal factorization. For example, $\mathbb{Z}[\sqrt{-5}][X]$ is Noetherian according to Hilbert's Basis Theorem, but neither factorial nor a Dedekind domain.

(iii) Obviously (X, Z) and (Y, Z) are prime ideals in $R := K[X, Y, Z]$, because $R/(X, Z) \cong K[Y] \cong R/(Y, Z)$ is an integral domain. Therefore $I := (XY, Z) = (X, Z) \cap (Y, Z)$ is a primary decomposition. Suppose that I is a product of prime ideals $I = P_1 \ldots P_n$. Because of $I \subseteq (X, Z)$ and $I \subseteq (Y, Z)$ there exist i, j with $P_i \subseteq (X, Z)$ and $P_j \subseteq (Y, Z)$. In the case $i = j$, $P_i = I$. Because of $X, Y \notin I$, I is however not a prime ideal. Therefore $i \neq j$ and one obtains the contradiction

$$Z \in I \subseteq P_i P_j = (RX + RZ)(RY + RZ) = (XY, XZ, YZ, Z^2)$$

(mentally set $X = Y = 0$). Thus I possesses no prime ideal factorization.

Theorem III.1.24. *Let R be commutative, $I \trianglelefteq R$ and $P \trianglelefteq R$ a prime ideal with $I \subseteq P$. Then there exists a minimal prime ideal Q with $I \subseteq Q \subseteq P$ (i. e. no prime ideal lies between I and Q). If R is additionally Noetherian, then Q is associated to I. In particular, there are then only finitely many Q.*

Proof. The set $\mathcal{M}$ of all prime ideals between I and P is non-empty because of $P \in \mathcal{M}$ and is ordered by $\subseteq$. Let $\mathcal{N} \subseteq \mathcal{M}$ be totally ordered and $S := \bigcap_{N \in \mathcal{N}} N$. If $x_1, x_2 \in R \setminus S$, then there exist $N_i \in \mathcal{N}$ with $x_i \notin N_i$ for $i = 1, 2$. Wlog. let $N_1 \subseteq N_2$. Since N_1 is a prime ideal, it follows that $x_1 x_2 \notin N_1$ and $x_1 x_2 \notin S$. Therefore S is a prime ideal with $I \subseteq S$, i. e. $S \in \mathcal{M}$ is a lower bound of $\mathcal{N}$. By Zorn's Lemma, $\mathcal{M}$ possesses a minimal element Q.

Now let R be Noetherian and $I = P_1 \cap \ldots \cap P_n$ be a primary decomposition, such that $\sqrt{P_1}, \ldots, \sqrt{P_n}$ are the prime ideals associated to I. From $P_1 \ldots P_n \subseteq I \subseteq Q$ it follows that $P_i \subseteq Q$ and $\sqrt{P_i} \subseteq Q$ for some $1 \leq i \leq n$. The minimality of Q yields $Q = \sqrt{P_i}$. The last statement follows from Lasker-Noether. □

Remark III.1.25. In the situation of Theorem III.1.24 one says: *Q lies minimally* over I. If I itself is a prime ideal, then $Q = I$. If I is a radical ideal, then I is the intersection of the prime ideals $P_1, \ldots, P_n$ associated to I (Remark III.1.22). The uniqueness of the primary decomposition shows that $P_1, \ldots, P_n$ lie minimally over I. In general, however, not all prime ideals associated to I are minimal over I.

Lemma III.1.26. *Let R be commutative and M a finitely generated R-module. Let $I \trianglelefteq R$ with $IM = M$. Then there exists $a \in I$ with $(1-a)M = 0$.*

Proof. Let $M = Rx_1 + \ldots + Rx_n$. Because of $IM = M$, it also holds that $M = Ix_1 + \ldots + Ix_n$. Let $a_{ij} \in I$ with $x_i = \sum_{j=1}^n a_{ij} x_j$ for $i = 1, \ldots, n$. With $b_{ij} := \delta_{ij} - a_{ij}$ it holds that $\sum_{j=1}^n b_{ij} x_j = 0$ for $i = 1, \ldots, n$. The Leibniz formula for $B := (b_{ij}) \in R^{n \times n}$ implies $\det B = 1 - a$ for some $a \in I$. Let B_{ij} be the submatrix from the Laplace expansion and $d_{ij} := (-1)^{i+j} \det B_{ij}$. Then $\det B = \sum_{i=1}^n b_{ij} d_{ij}$ holds by expansion along the j-th column. If one replaces the j-th column of B by the k-th column for $k \neq j$, one obtains $\sum_{i=1}^n b_{ik} d_{ij} = 0$, because the new matrix has two identical columns. From this it follows that

$$\det(B) x_j = \sum_{i=1}^n b_{ij} d_{ij} x_j = \sum_{k=1}^n x_k \sum_{i=1}^n b_{ik} d_{ij} = \sum_{i=1}^n d_{ij} \sum_{k=1}^n b_{ik} x_k = 0$$

for $j = 1, \ldots, n$. Together one obtains $(1-a)M = 0$. □

Theorem III.1.27 (Krull's Intersection Theorem)**.** *Let R be commutative and Noetherian. Let $I \lhd R$ and $J := \bigcap_{n \in \mathbb{N}} I^n$. Then $IJ = J$ and there exists an $a \in I$ with $(1-a)J = 0$. If R is local or an integral domain, then $J = 0$.*

Proof. Let $P \trianglelefteq R$ be primary with $IJ \subseteq P \subseteq \sqrt{P}$. From Lemma III.1.19 it follows that $J \subseteq \sqrt{P}$, because $J \subseteq I$. According to Lemma III.1.14, $\sqrt{P}^n \subseteq P$ holds for some $n \in \mathbb{N}$. This shows $J = J^n \subseteq P$. Since IJ is an intersection of primary ideals according to Lasker-Noether, it follows that $J \subseteq IJ \subseteq J$. According to Lemma III.1.26 with $M = J$, there exists $a \in I$ with $(1-a)J = 0$. If R is local, then $1 - a \in R \setminus \mathrm{J}(R)$ is invertible and $J = 0$. If R is an integral domain, then $J = 0$ also holds, because $a \neq 1$. □

Definition III.1.28. Let R be commutative and $P \trianglelefteq R$ a prime ideal. The *height* $h(P) \in \mathbb{N}_0$ of P is the maximal length l of a chain of prime ideals $P = P_0 \supsetneq P_1 \supsetneq \ldots \supsetneq P_l$. If there are arbitrarily long such chains, let $h(P) = \infty$. Finally, let

$$\dim R := \sup\big\{h(P) : P \trianglelefteq R \text{ prime ideal}\big\}$$

be the *Krull dimension* of R.

Example III.1.29.

(i) An integral domain R has Krull dimension 0 if and only if R is a field. On the other hand, the local ring $\mathbb{Z}/4\mathbb{Z}$ also has Krull dimension 0.

(ii) Every Dedekind domain that is not a field has Krull dimension 1, because the non-trivial prime ideals are maximal.

(iii) The sequence of prime ideals $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, \ldots, X_n)$ in $R := K[X_1, \ldots, X_n]$ shows $\dim R \geq n$. We will show that equality holds. Because of $(0) \subsetneq (X) \subsetneq (X, 2)$, on the other hand, $\dim \mathbb{Z}[X] \geq 2$.

Lemma III.1.30. *Let R be commutative and Noetherian. For every maximal ideal $P \trianglelefteq R$ and $n \in \mathbb{N}$, R/P^n is an Artinian R-module.*

Proof. Induction on n: Because of $R/P^{n-1} \simeq (R/P^n)/(P^{n-1}/P^n)$, it suffices by Lemma II.7.6 to show that the R-module $M := P^{n-1}/P^n$ is Artinian (where $P^0 := R$). Because of $PM = 0$, one can consider M as a vector space over the field R/P (cf. proof of Theorem II.9.7). The submodules correspond to the subspaces. Since R is Noetherian, P^{n-1} and M are finitely generated R-modules. Thus M is finite-dimensional and the claim follows. □

Lemma III.1.31. *Let R be commutative, Noetherian and local. Let $a \in \mathrm{J}(R)$ such that R/Ra is an Artinian R-module. Then there exists at most one prime ideal that does not contain a.*

Proof. Let $P \trianglelefteq R$ be a prime ideal with $a \notin P$. For $n \in \mathbb{N}$ let

$$P_n := \{r \in R : \exists s \in R \setminus P : rs \in P^n\} = \Phi^{-1}((R_P P)^n) \trianglelefteq R$$

as in Theorem III.1.9. Since P is a prime ideal, $P = P_1 \supseteq P_2 \supseteq \ldots$ holds. Let $Q := P \cap Ra \trianglelefteq R$. Since $P/Q \simeq (P + Ra)/Ra \subseteq R/Ra$ is artinian, the sequence

$$(P_1 + Q)/Q \supseteq (P_2 + Q)/Q \supseteq \ldots$$

becomes stationary. Let $n \in \mathbb{N}$ with $P_m + Q = P_{m+1} + Q$ for all $m \geq n$. With $P_n \trianglelefteq R$, $M := P_n/P_m$ is also a finitely generated R-module. For $x \in P_n \subseteq P_m + Q \subseteq P_m + Ra$ there exist $y \in P_m$ and $r \in R$ with $x = y + ra$. Because of $ra = x - y \in P_n$ there exists $s \in R \setminus P$ with $ras \in P^n$. From $a \notin P$ it follows that $r \in P_n$. This shows $a(r + P_m) = x + P_m$ and $aM = M$. Since $a \in \mathrm{J}(R)$, $\mathrm{J}(R)M = M$ holds. According to Lemma III.1.26 there exists $b \in \mathrm{J}(R)$ with $(1 - b)M = 0$. Since R is local, $1 - b \in R^\times$ and $M = 0$ holds, i. e. $P_n = P_m$ for $m \geq n$.

Krull's Intersection Theorem applied to the local ring R_P shows $\bigcap_{m \geq 1} (R_P P)^m = 0$. It follows that $P_n = \bigcap_{m \geq n} P_m = \Phi^{-1}(0)$ and $P \subseteq \sqrt{P_n} = \sqrt{\Phi^{-1}(0)}$. Conversely, let $x \in \sqrt{P_n}$ and $x^k \in P_n$. Then there exists $s \in R \setminus P$ with $x^k s \in P^n \subseteq P$. Since P is a prime ideal, $x \in P$ holds. Therefore $P = \sqrt{\Phi^{-1}(0)}$ is uniquely determined. □

Theorem III.1.32 (Krull's Principal Ideal Theorem)**.** *Let R be commutative and noetherian. Let $I \trianglelefteq R$ be a principal ideal and $P \trianglelefteq R$ a minimal prime ideal over I. Then $h(P) \leq 1$ holds.*

Proof. Let $I = Ra$. First let R be local and $P = \mathrm{J}(R)$. Then P is the only prime ideal containing a. According to Theorem III.1.15, $\sqrt{I} = P$. According to Lemma III.1.14, $P^n \subseteq I$ for some $n \in \mathbb{N}$. According to Lemma III.1.30 and Lemma II.7.6, $R/I \simeq (R/P^n)/(I/P^n)$ is an artinian R-module. According to Lemma III.1.31 there is at most one other prime ideal besides P. In particular, $h(P) \leq 1$.

Now let R be arbitrary (commutative and noetherian). According to Theorem III.1.10 and Theorem III.1.12, R_P is noetherian and local. According to Theorem III.1.9, $R_P P$ is a minimal prime ideal over $(\Phi(I)) = R_P a$. The first part of the proof shows that the statement holds in R_P. With Theorem III.1.9 it also holds in R. □

Lemma III.1.33 (Prime Avoidance)**.** *Let R be commutative, $I \trianglelefteq R$ and $P_1, \ldots, P_n \trianglelefteq R$ prime ideals with $I \subseteq P_1 \cup \ldots \cup P_n$. Then $I \subseteq P_i$ for some $i \in \{1, \ldots, n\}$.*

Proof. Let $n > 1$ be minimal. Then there exist $x_i \in I \setminus \bigcup_{j \neq i} P_j \subseteq P_i$. Consider $y := x_1 + x_2 \ldots x_n \in I$. Because $x_1 \notin P_i$ for $i > 1$, it follows that $y \in P_1$ and therefore also $x_2 \ldots x_n \in P_1$. Since P_1 is a prime ideal, it follows that $x_i \in P_1$ for some $i > 1$. Contradiction. □

Remark III.1.34. Let R be noetherian and $I \trianglelefteq R$. According to Lemma II.7.6, the R-module R/I is noetherian. Thus every submodule of R/I is also finitely generated as an R/I-module, i. e. the regular R/I-module is noetherian. Thus R/I is noetherian as a ring. This argument will be used several times in the following.

Lemma III.1.35. *Let R be commutative and noetherian. Let $P_0, \ldots, P_n, Q_1, \ldots, Q_m \trianglelefteq R$ be prime ideals with $P_0 \subsetneq \ldots \subsetneq P_n \nsubseteq Q_1 \cup \ldots \cup Q_m$. Then there exist prime ideals $P_1', \ldots, P_{n-1}' \nsubseteq Q_1 \cup \ldots \cup Q_m$ with $P_0 \subsetneq P_1' \subsetneq \ldots \subsetneq P_{n-1}' \subsetneq P_n$.*

Proof. Induction on n: In the case $n \leq 1$ there is nothing to do. Let $n \geq 2$ and $P_2', \ldots, P_{n-1}' \nsubseteq Q_1 \cup \ldots \cup Q_m$ with $P_1 \subsetneq P_2' \subsetneq \ldots \subsetneq P_{n-1}' \subsetneq P_n$ already constructed. According to Lemma III.1.33, $P_2' \nsubseteq P_1 \cup Q_1 \cup \ldots \cup Q_m$ holds. Let $x \in P_2' \setminus (P_1 \cup Q_1 \cup \ldots \cup Q_m)$. According to Theorem III.1.24, there exists a minimal prime ideal P_1' over $Rx + P_0$ with $P_1' \subseteq P_2'$. Obviously $P_0 \subsetneq P_1'$ and $P_1' \nsubseteq Q_1 \cup \ldots \cup Q_m$ hold.

To prove $P_1' \neq P_2'$, we pass to the noetherian ring $\overline{R} := R/P_0$ (Remark III.1.34). Because $P_0 \subsetneq P_1 \subsetneq P_2'$, P_2'/P_0 has at least height 2 in $\overline{R}$. On the other hand, P_1'/P_0 is minimal over the principal ideal $(Rx + P_0)/P_0$. Krull's Principal Ideal Theorem shows $h(P_1'/P_0) \leq 1$ and it follows that $P_1' \neq P_2'$. □

Theorem III.1.36 (Krull's Height Theorem)**.** *Let R be commutative and noetherian. Let $x_1, \ldots, x_n \in R$ and $P \trianglelefteq R$ be a minimal prime ideal over $(x_1, \ldots, x_m)$. Then $h(P) \leq n$ holds. In particular, every prime ideal in R has finite height.*

Proof. Induction on n: According to the Principal Ideal Theorem, we may assume $n \geq 2$. Let $I := (x_1, \ldots, x_{n-1})$. If P is minimal over I, then $h(P) \leq n - 1$ holds by induction. Let us therefore assume the opposite. According to Theorem III.1.24, there exist only finitely many prime ideals $Q_1, \ldots, Q_m$ minimal over I. According to Lemma III.1.33, $P \nsubseteq Q_1 \cup \ldots \cup Q_m$. Let $P = P_0 \supsetneq P_1 \supsetneq \ldots \supsetneq P_h$ be prime ideals. According to Lemma III.1.35, we can assume $P_{h-1} \nsubseteq Q_1 \cup \ldots \cup Q_m$. In the Noetherian ring $\overline{R} := R/I$ (Remark III.1.34), the prime ideals $Q_1/I, \ldots, Q_m/I$ are minimal, but P/I is not. On the other hand, P/I is minimal over the principal ideal $(x_1, \ldots, x_n)/I \simeq Rx_n/(Rx_n \cap I)$. According to the Principal Ideal Theorem, $h(P/I) = 1$ holds. Let Q be a prime ideal with $P \supseteq Q \supsetneq P_{h-1} + I$. Then $Q \nsubseteq Q_1 \cup \ldots \cup Q_m$ and Q cannot be minimal over I. This shows $h(Q/I) \geq 1$ and $Q = P$. Therefore P/P_{h-1} is minimal over $(P_{h-1} + I)/P_{h-1} \simeq I/(I \cap P_{h-1})$. By induction, $h - 1 \leq h(P/P_{h-1}) \leq n - 1$ holds, thus $h \leq n$.

The second assertion follows because P, as an ideal of a Noetherian ring, is finitely generated. □

Remark III.1.37. Although Noetherian rings are generally not Artinian, Theorem III.1.36 shows that descending chains of prime ideals must become stationary. The length of such chains is, however, not bounded, i. e. there exist Noetherian rings with infinite Krull dimension (example by Nagata).

Lemma III.1.38. *Let R be a Noetherian integral domain and $P \trianglelefteq R[X]$ a prime ideal with $P \cap R = 0$. Then $h(P) \leq 1$ holds.*

Proof. Let $S := R \setminus \{0\}$ be multiplicatively closed, $Q = Q(R) = R[S^{-1}]$ the quotient field of R and $\hat{R} := R[X][S^{-1}]$ the localization of $R[X]$ at S. According to the universal property, the embedding $R[X] \hookrightarrow Q[X]$ can be extended to a homomorphism $\hat{\varphi}\colon \hat{R} \to Q[X]$, $\frac{\alpha}{s} \mapsto \frac{\alpha}{s}$ ($\alpha \in R[X]$, $s \in S$). It holds that $\frac{\alpha}{s} = 0$ in $Q[X]$ if and only if $\alpha = 0$ in $R[S]$. Thus $\hat{\varphi}$ is injective. Since every polynomial in $Q[X]$ can be written in the form $\frac{\alpha}{s}$ with $\alpha \in R[X]$ and $s \in S$ (common denominator of the coefficients), $\hat{\varphi}$ is an isomorphism.[1] In particular, $\hat{R}$ is a principal ideal domain. Let $0 \neq P' \trianglelefteq R[X]$ be a prime ideal with $P' \subseteq P$. It holds that $P' \cap S \subseteq P \cap R \cap S = \{0\} \cap S = \varnothing$. According to Theorem III.1.9, $(\Phi(P')) \subseteq (\Phi(P))$ are non-trivial prime ideals in the principal ideal domain $\hat{R}$. From Lemma II.5.18 it follows that $(\Phi(P')) = (\Phi(P))$ and $P' = P$ according to Theorem III.1.9. This shows $h(P) \leq 1$. □

Theorem III.1.39. *For every Noetherian integral domain R, it holds that* $\boxed{\dim R[X] = 1 + \dim R.}$

Proof. Since R is an integral domain, $(X) \trianglelefteq R[X]$ is a prime ideal. Every chain of prime ideals in $R[X]/(X) \cong R$ corresponds to a chain of prime ideals in $R[X]$, which can be extended by (0). This shows $\dim R[X] \geq 1 + \dim R$. In particular, we can assume $n := \dim R < \infty$ and argue by induction on n. In the case $n = 0$, R is a field and $R[X]$ is a principal ideal domain with Krull dimension 1. Therefore, let $n \geq 1$ and $P_0 \supsetneq \ldots \supsetneq P_m = (0)$ be a chain of prime ideals in $R[X]$. It suffices to show $m \leq n + 1$. Wlog. let $m \geq 2$.

Suppose $P_{m-1} \cap R = 0$. From Lemma III.1.38 it then follows that $P_{m-2} \cap R \neq 0$. Let $0 \neq x \in P_{m-2} \cap R$. Because $h(P_{m-2}) \geq 2$, P_{m-2} cannot be minimal over Rx according to the Principal Ideal Theorem. Let $Q \trianglelefteq R$ be a minimal prime ideal over Rx with $Q \subsetneq P_{m-2}$. We can replace P_{m-1} by Q and from now on assume $I := P_{m-1} \cap R \neq 0$. Since $I \trianglelefteq R$ is a prime ideal, $\overline{R} := R/I$ is a Noetherian integral domain. As usual, it follows that $\dim \overline{R} \leq \dim(R) - 1 = n - 1$. By induction, $\dim \overline{R}[X] \leq n$ holds. The canonical epimorphism $R \to \overline{R}$ extends to an epimorphism $\mu\colon R[X] \to \overline{R}[X]$. For $P := \operatorname{Ker}(\mu) \trianglelefteq R[X]$, it therefore holds that $\dim(R[X]/P) = \dim \overline{R}[X] \leq n$. Since P consists of the polynomials with coefficients in $I \subseteq P_{m-1}$, it follows that $P \subseteq R[X]I \subseteq P_{m-1}$. The chain of prime ideals $P_0/P \supsetneq \ldots \supsetneq P_{m-1}/P$ shows $m - 1 \leq \dim(R[X]/P) \leq n$, hence $m \leq n + 1$. □

Corollary III.1.40. *For every field K, it holds that* $\dim K[X_1, \ldots, X_n] = n$.

[1] Informally expressed: $R[X][S^{-1}] = R[X, S^{-1}] = R[S^{-1}][X] = Q[X]$.

III.2 Algebraic Geometry

Remark III.2.1. In linear algebra, one investigates the solution sets of systems of linear equations. With the principal axis transformation, the solutions of a single quadratic equation can also be described (one obtains conic sections in $\mathbb{R}^2$ or quadrics in $\mathbb{R}^n$). In algebraic geometry, one is more generally interested in the solution sets of systems of polynomial equations. Fermat's Last Theorem, for example, asks for the rational solutions of the equation $X^n + Y^n = Z^n$ for $n \geq 3$. Since the theory is already complicated for one variable (see chapter I.14), we restrict ourselves to algebraically closed fields. We associate the aforementioned solution sets with radical ideals in the polynomial ring in order to introduce a concept of dimension with the help of Krull's theorems.

Theorem III.2.2 (Zariski's Lemma)**.** *Let $K \subseteq L$ be a field extension. If there exists a ring epimorphism $K[X_1, \ldots, X_n] \to L$, then $|L : K| < \infty$.*

Proof. Let $x_i \in L$ be the image of X_i under the given epimorphism. Suppose that a transcendence basis $B \neq \varnothing$ of L over K exists. Let $b \in B$. By replacing K with $K(B \setminus \{b\})$, one can assume $B = \{b\}$. Since $K(b) \subseteq L$ is algebraic, there exists

$$m := \max_{1 \leq i \leq n} |K(x_i, b) : K(b)|.$$

Thus every element of L is a $K(b)$-linear combination of the elements $x_1^{k_1} \ldots x_n^{k_n}$ with $0 \leq k_1, \ldots, k_n \leq m$. In particular, $d := |L : K(b)| < \infty$. Let $e_1, \ldots, e_d \in L$ be a $K(b)$-basis of L. For $1 \leq i, j \leq d$ and $1 \leq s \leq n$ let

$$e_i e_j = \sum_{k=1}^{d} \frac{\alpha_{ijk}(b)}{\beta_{ijk}(b)} e_k \qquad\qquad x_s = \sum_{t=1}^{d} \frac{\gamma_{st}(b)}{\delta_{st}(b)} e_t$$

with $\alpha_{ijk}, \beta_{ijk}, \gamma_{st}, \delta_{st} \in K[X]$. Every $a \in L$ is a K-linear combination of products of the x_i. After multiplying out, a is a $K(b)$-linear combination of the e_i, where the denominators of the coefficients are products of the $\delta_{st}(b)$ and $\beta_{ijk}(b)$. In particular, only finitely many irreducible polynomials from $K[X]$ can occur as factors of these denominators. Since $K[X]$ has infinitely many irreducible polynomials (for $|K| = \infty$ take $X + a$ with $a \in K$ and for $|K| < \infty$ use Remark I.11.16), the e_i cannot be linearly independent. This contradiction shows $B = \varnothing$ and $K \subseteq L$ is algebraic. As above, it then follows that $|L : K| < \infty$. □

Remark III.2.3. The condition in Theorem III.2.2 means that L is finitely generated as a K-algebra. Note: $K[X]$ is finitely generated as a K-algebra, but not finite-dimensional (cf. Theorem III.2.24).

Corollary III.2.4 (Weak Nullstellensatz)**.** *Let K be an algebraically closed field and $I \lhd K[X_1, \ldots, X_n]$. Then there exist $x_1, \ldots, x_n \in K$ with $\alpha(x_1, \ldots, x_n) = 0$ for all $\alpha \in I$.*

Proof. According to Krull's Theorem II.2.7, we can assume that I is maximal. By Theorem I.7.12, $L := K[X_1, \ldots, X_n]/I$ is a field extension of $(K + I)/I \cong K/(K \cap I) \cong K$. By Theorem III.2.2, $|L : K| < \infty$. Since K is algebraically closed, it even holds that $|L : K| = 1$ and $K[X_1, \ldots, X_n] = K + I$. For $i = 1, \ldots, n$ let $x_i \in K$ with $X_i - x_i \in I$. Then $J := (X_1 - x_1, \ldots, X_n - x_n) \subseteq I$. Because $K[X_1, \ldots, X_n]/J \cong K$, J is also maximal and it follows that $I = J$. This proves the claim. □

Definition III.2.5. Let K be an algebraically closed field and $R := K[X_1, \ldots, X_n]$. For $P \subseteq R$ and $A \subseteq K^n$ let

$$\mathcal{V}(P) := \big\{(x_1, \ldots, x_n) \in K^n : \forall \alpha \in P : \alpha(x_1, \ldots, x_n) = 0\big\},$$
$$\mathcal{I}(A) := \big\{\alpha \in R : \forall (x_1, \ldots, x_n) \in A : \alpha(x_1, \ldots, x_n) = 0\big\}.$$

The sets of the form $\mathcal{V}(P)$ for $P \subseteq R$ are called (*affine*) *varieties*. Let $\mathrm{A}(K^n)$ be the set of all varieties of K^n.

Remark III.2.6.

(i) The following results about varieties always refer to algebraically closed fields.

(ii) For $P \subseteq R$ it holds that $\mathcal{V}(P) = \mathcal{V}((P)) = \mathcal{V}(\sqrt{(P)})$. Every variety thus has the form $\mathcal{V}(I)$ for a radical ideal I. According to Hilbert's Basis Theorem, there also exist polynomials $\alpha_1, \ldots, \alpha_k \in R$ with $I = (\alpha_1, \ldots, \alpha_k)$. We set $\mathcal{V}(\alpha_1, \ldots, \alpha_k) := \mathcal{V}(I)$.

Example III.2.7. If P consists of linear polynomials in $X_1, \ldots, X_n$ (i. e. $\deg \alpha \leq 1$ for all $\alpha \in P$), then $\mathcal{V}(P)$ is the solution set of a system of linear equations. In the case $\mathcal{V}(P) \neq \varnothing$, $\mathcal{V}(P)$ is then an affine subspace, thus of the form $x + U$ with $x \in K^n$ and $U \leq K^n$.

Lemma III.2.8. *For $P, Q, P_i \trianglelefteq R := K[X_1, \ldots, X_n]$ it holds that*

(i) $\mathcal{V}(\varnothing) = K^n$, $\mathcal{V}(R) = \varnothing$.

(ii) $\bigcap_{i \in I} \mathcal{V}(P_i) = \mathcal{V}(\bigcup_{i \in I} P_i) = \mathcal{V}(\sum_{i \in I} P_i)$.

(iii) $P \subseteq Q \Rightarrow \mathcal{V}(Q) \subseteq \mathcal{V}(P)$.

(iv) $\mathcal{V}(P) \cup \mathcal{V}(Q) = \mathcal{V}(P \cap Q)$.

Proof. All statements except for $\mathcal{V}(P \cap Q) \subseteq \mathcal{V}(P) \cup \mathcal{V}(Q)$ are trivial. Let $x \in K^n \setminus (\mathcal{V}(P) \cup \mathcal{V}(Q))$. Then there exist $\alpha \in P$ and $\beta \in Q$ with $\alpha(x) \neq 0 \neq \beta(x)$. Then $(\alpha\beta)(x) \neq 0$ and $\alpha\beta \in PQ \subseteq P \cap Q$. This shows $x \notin \mathcal{V}(P \cap Q)$. □

Remark III.2.9. According to Lemma III.2.8, one obtains a topology on K^n by choosing the varieties as the closed sets (the open sets are the complements of closed sets). It is called the *Zariski topology*. For an arbitrary subset $M \subseteq K^n$, $\overline{M} := \mathcal{V}(\mathcal{I}(M)) \in \mathrm{A}(K^n)$ is called the *Zariski closure* of M in K^n.

Example III.2.10. According to Example III.2.7, the singleton subsets of K^n are closed with respect to the Zariski topology and thus also all finite subsets. In the case $R = K[X]$, every non-trivial ideal has the form (α) with $\alpha \neq 0$. Since α has only finitely many roots, all varieties here except for K are finite.

Theorem III.2.11 (Hilbert's Nullstellensatz)**.** *The maps $\mathcal{V}$ and $\mathcal{I}$ are inverse bijections to each other between the set of radical ideals of $K[X_1, \ldots, X_n]$ and $\mathrm{A}(K^n)$.*

Proof (Rabinowitsch). For a radical ideal $I \trianglelefteq R := K[X_1, \ldots, X_n]$ and $A \in \mathrm{A}(K^n)$, it holds that $I \subseteq \mathcal{I}(\mathcal{V}(I))$ and $A \subseteq \mathcal{V}(\mathcal{I}(A))$ by definition. An application of $\mathcal{V}$ to the first inclusion yields $\mathcal{V}(\mathcal{I}(\mathcal{V}(I))) \subseteq \mathcal{V}(I)$. Specifically for $A = \mathcal{V}(I)$, it follows that $\mathcal{V}(\mathcal{I}(A)) \subseteq A$. Thus $\mathcal{V}(\mathcal{I}(A)) = A$.

Now let $\alpha \in \mathcal{I}(\mathcal{V}(I)) \setminus \{0\}$ and $\widehat{I} := (I, \alpha Y - 1) \trianglelefteq R[Y]$. Suppose there exists $(x_1, \ldots, x_n, y) \in \mathcal{V}(\widehat{I})$. Then $(x_1, \ldots, x_n) \in \mathcal{V}(I)$ and one obtains the contradiction

$$(\alpha Y - 1)(x_1, \ldots, x_n, y) = \alpha(x_1, \ldots, x_n)y - 1 = -1 \neq 0.$$

Thus $\mathcal{V}(\widehat{I}) = \varnothing$ and the weak Nullstellensatz implies $\widehat{I} = R[Y]$. Therefore there exist $\beta_1, \ldots, \beta_k, \gamma \in R[Y]$ and $\alpha_1, \ldots, \alpha_k \in I$ with

$$\beta_1\alpha_1 + \ldots + \beta_k\alpha_k + \gamma(\alpha Y - 1) = 1.$$

By substituting Y with α^{-1}, we obtain

$$\sum_{i=1}^{k} \beta_1(X_1, \ldots, X_n, \alpha^{-1})\alpha_i = 1 \in K(X_1, \ldots, X_n)$$

Multiplying by a sufficiently high power α^m, it follows that $\alpha^m \in I$ and $\alpha \in \sqrt{I} = I$. □

Remark III.2.12. In the situation of Theorem III.2.11, the maximal ideals in R correspond to the single-element varieties, i.e., to the elements of K^n (cf. proof of Corollary III.2.4).

Definition III.2.13. A variety $A \in \mathrm{A}(K^n)$ is called *reducible*, if there exist $B, C \in \mathrm{A}(K^n)$ with $A = B \cup C$ and $B, C \subsetneq A$. A non-empty variety is called *irreducible* if it is not reducible.

Lemma III.2.14. *$A \in \mathrm{A}(K^n)$ is irreducible if and only if $\mathcal{I}(A)$ is a prime ideal.*

Proof. Let $A = B \cup C$ be reducible with varieties $B, C \subsetneq A$. Then $\mathcal{I}(B), \mathcal{I}(C) \not\subseteq \mathcal{I}(A)$, but $\mathcal{I}(B)\mathcal{I}(C) \subseteq \mathcal{I}(A)$. Consequently, $\mathcal{I}(A)$ is not a prime ideal. Conversely, if $\mathcal{I}(A)$ is not a prime ideal, then there exist $\alpha, \beta \in R \setminus \mathcal{I}(A)$ with $\alpha\beta \in \mathcal{I}(A)$. For $B := \mathcal{V}((\mathcal{I}(A), \alpha))$ and $C := \mathcal{V}((\mathcal{I}(A), \beta))$, it holds that $A = B \cup C$ and $B, C \subsetneq A$. □

Remark III.2.15. Let $\varnothing \neq \mathcal{A} \subseteq \mathrm{A}(K^n)$. Since R is Noetherian, the set $\{\mathcal{I}(A) : A \in \mathcal{A}\}$ possesses a maximal element, say $\mathcal{I}(A)$ with $A \in \mathcal{A}$. Obviously, A is then a minimal element of $\mathcal{A}$.

Theorem III.2.16. *For every variety $A \in \mathrm{A}(K^n)$ there exist (up to the order) uniquely determined irreducible varieties $A_1, \ldots, A_k$ with $A = A_1 \cup \ldots \cup A_k$ and $A_i \not\subseteq A_j$ for all $i \neq j$.*

Proof. Let $\mathcal{A} \subseteq \mathrm{A}(K^n)$ be the set of varieties that do not possess such a decomposition. Assume $\mathcal{A} \neq \varnothing$. According to Remark III.2.15, $\mathcal{A}$ has a minimal element A. Since A has no decomposition, A is reducible, say $A = B \cup C$. Because of $B, C \subsetneq A$, it follows that $B, C \notin \mathcal{A}$, i. e. B and C can be decomposed in the desired form. But then $B \cup C = A$ can also be decomposed. This contradiction shows $\mathcal{A} = \varnothing$.

To prove uniqueness, we start from two decompositions $A = B_1 \cup \ldots \cup B_k = C_1 \cup \ldots \cup C_l$. For $1 \leq i \leq k$, we have $B_i = B_i \cap A = (B_i \cap C_1) \cup \ldots \cup (B_i \cap C_l)$. Since B_i is irreducible, $B_i \subseteq C_j$ for some $1 \leq j \leq l$. Analogously, there exists $1 \leq s \leq k$ with $C_j \subseteq B_s$. From $B_i \subseteq B_s$ it follows that $i = s$ and $B_i = C_j$. □

Remark III.2.17. In the situation of Theorem III.2.16, $A_1, \ldots, A_k$ are called the (*irreducible*) *components* of A. The uniqueness of the components shows that $\mathcal{I}(A) = \mathcal{I}(A_1) \cap \ldots \cap \mathcal{I}(A_k)$ is a primary decomposition of $\mathcal{I}(A)$, where the prime ideals $\mathcal{I}(A_i) = \sqrt{\mathcal{I}(A_i)}$ are associated to $\mathcal{I}(A)$. According to Theorem III.1.24 and Remark III.1.25, $\mathcal{I}(A_1), \ldots, \mathcal{I}(A_k)$ are exactly the minimal prime ideals over $\mathcal{I}(A)$.

Example III.2.18.

(i) The components of a finite variety are singletons according to Example III.2.10.

(ii) Let $\alpha \in K[X_1, \ldots, X_n] \setminus K$ with prime factorization $\alpha = \alpha_1^{e_1} \ldots \alpha_k^{e_k}$. Then $\mathcal{V}(\alpha_1), \ldots, \mathcal{V}(\alpha_k)$ are the components of $\mathcal{V}(\alpha)$ according to Example III.1.23.

(iii) Let $I := (X^2 - YZ, XZ - X) \trianglelefteq K[X, Y, Z]$ and $A = \mathcal{V}(I) \in \mathrm{A}(K^3)$. Because of $XZ - X = X(Z-1)$, it holds that

$$\begin{aligned} I &= (X^2 - YZ, X) \cap (X^2 - YZ, Z - 1) = (YZ, X) \cap (X^2 - Y, Z - 1) \\ &= (X, Y) \cap (X, Z) \cap (X^2 - Y, Z - 1). \end{aligned}$$

Here (X, Y) and (X, Z) are prime ideals and $K[X, Y, Z]/(X^2 - Y, Z - 1) \cong K[X, Y]/(X^2 - Y)$. Since $X^2 - Y$ is irreducible (approach: $X^2 - Y = (X + aY + b)(X + cY + d)$), $(X^2 - Y, Z - 1)$ is also a prime ideal. As an intersection of prime ideals, I is a radical ideal (Remark III.1.17). Obviously, there are no inclusions among the three prime ideals. The components of A are therefore

$$\begin{aligned} \mathcal{V}(X, Y) &= \{(0, 0, z) : z \in K\}, \\ \mathcal{V}(X, Z) &= \{(0, y, 0) : y \in K\}, \\ \mathcal{V}(X^2 - Y, Z - 1) &= \{(x, x^2, 1) : x \in K\}. \end{aligned}$$

Definition III.2.19. For $A \in \mathrm{A}(K^n)$ one calls

$$K[A] := K[X_1, \ldots, X_n]/\mathcal{I}(A)$$

the *coordinate ring* of A. One calls $\dim A := \dim K[A]$ the *dimension* of A ($\dim K[A]$ is the Krull dimension). Additionally, one sets $\dim \varnothing := -\infty$.

Remark III.2.20.

(i) From Corollary III.1.40 it follows that $d := \dim A \leq n$ for every variety $A \in \mathrm{A}(K^n)$. If $P_0/\mathcal{I}(A) \subsetneq \ldots \subsetneq P_d/\mathcal{I}(A)$ are prime ideals in $K[A]$, then $A \supseteq \mathcal{V}(P_0) \supsetneq \ldots \supsetneq \mathcal{V}(P_d)$ are irreducible varieties and vice versa. One can therefore also define $\dim A$ as the maximal length of a chain of irreducible varieties in A.

(ii) Let $\alpha_1, \ldots, \alpha_k \in K[X_1, \ldots, X_n]$ be linear polynomials without constant term. Then $A = \mathcal{V}(\alpha_1, \ldots, \alpha_k)$ is a subspace of K^n as the solution set of a homogeneous system of equations. Wlog. let $\alpha_1, \ldots, \alpha_k$ be linearly independent (in particular $k \leq n$). According to the Gaussian algorithm, we can assume $\alpha_i = X_i + a_i X_{i+1} + \ldots$ for $i = 1, \ldots, k$ and $a_i \in K$. Now it follows easily that $K[A] \cong K[X_{k+1}, \ldots, X_n]$ and $\dim A = n - k$ according to Corollary III.1.40. Therefore, $\dim A$ coincides with the concept of dimension from linear algebra.

Lemma III.2.21. *If $A_1, \ldots, A_k$ are the components of $A \in \mathrm{A}(K^n)$, then*

$$\dim A = \max_{1 \leq i \leq k} \dim A_i.$$

Proof. If $P_0/\mathcal{I}(A_i) \subsetneq \ldots \subsetneq P_h/\mathcal{I}(A_i)$ are prime ideals in $K[A_i]$, then $P_0/\mathcal{I}(A) \subsetneq \ldots \subsetneq P_h/\mathcal{I}(A)$ are prime ideals in $K[A]$. This shows $\dim A_i \leq \dim A$ for $i = 1, \ldots, k$. Conversely, let $P_0/\mathcal{I}(A) \subsetneq \ldots \subsetneq P_h/\mathcal{I}(A)$ be prime ideals in $K[A]$ with $h = \dim A$. Then P_0 is minimal over $\mathcal{I}(A)$. According to Remark III.2.17, $P_0 = \mathcal{I}(A_i)$ for some $1 \leq i \leq k$. Now $P_0/\mathcal{I}(A_i) \subsetneq \ldots \subsetneq P_h/\mathcal{I}(A_i)$ are prime ideals in $K[A_i]$. It follows that $\dim A = h \leq \dim A_i$. □

Lemma III.2.22.

(i) A variety A is finite if and only if $\dim A \leq 0$.

(ii) For $I = (\alpha_1, \ldots, \alpha_k) \lhd K[X_1, \ldots, X_n]$ with $k < n$ it holds that $\dim \mathcal{V}(I) \geq 1$.

Proof.

(i) Wlog. let $A \neq \varnothing$. Let A be finite, wlog. $A = \{(x_1, \ldots, x_n)\}$ according to Lemma III.2.21 and Example III.2.18. Then $\mathcal{I}(A) = (X_1 - x_1, \ldots, X_n - x_n)$ and $K[A] \cong K$. This shows $\dim A = 0$. Conversely, let $\dim A = 0$ and wlog. A be irreducible. Then $K[A]$ is a field (Example III.1.29) and $\mathcal{I}(A)$ is a maximal ideal. Remark III.2.12 shows $|A| = 1$.

(ii) Let $A := \mathcal{V}(I)$. Because $I \neq K[X_1, \ldots, X_n]$, $\dim A \geq 0$. Assume $\dim A = 0$. Let $P \trianglelefteq K[X_1, \ldots, X_n]$ be a prime ideal minimal over $\mathcal{I}(A) = \sqrt{I}$. The prime ideal $P/\sqrt{I} \trianglelefteq K[A]$ must then be maximal. Thus P is also maximal in $K[X_1, \ldots, X_n]$. As is well known, P has the form $P = (X_1 - x_1, \ldots, X_n - x_n)$. The prime ideals $(0) \subsetneq (X_1 - x_1) \subsetneq (X_1 - x_1, X_2 - x_2) \ldots \subsetneq P$ show $h(P) = n$. Let Q be a prime ideal with $I \subseteq Q \subseteq P$. Because $\sqrt{I} \subseteq \sqrt{Q} = Q$, $Q = P$, i. e. P is also minimal over I. Krull's Height Theorem yields the contradiction $h(P) \leq k < n$. □

Remark III.2.23.

(i) If the polynomials $\alpha_1, \ldots, \alpha_k$ in Lemma III.2.22 are linear, one obtains the well-known statement that an underdetermined linear system of equations has either no or infinitely many solutions (provided $|K| = \infty$). In general, however, Lemma III.2.22 does not hold for arbitrary (infinite) fields. For example, $X^2 + Y^2 = 0$ has only the trivial solution $(0, 0)$ in $\mathbb{R}^2$.

(ii) For $A \neq \varnothing$, one can view $K[A]$ as a vector space over

$$K \cong K/(K \cap \mathcal{I}(A)) \cong (K + \mathcal{I}(A))/\mathcal{I}(A) \subseteq K[A].$$

If A is irreducible, then $K[A]$ is an integral domain (Lemma III.2.14) with quotient field $K(A) := Q(K[A])$. We show in this situation that $\dim A$ coincides with the transcendence degree of $K(A)$ over K (Theorem III.2.26).

(iii) The following theorem holds for arbitrary fields K and provides transcendence bases for rings.

Theorem III.2.24 (Noether normalization)**.** *Let K be a field and $K[X_1, \ldots, X_n] \to R$ a ring epimorphism. Then R is finitely generated as a module over a subring $S \cong K[Y_1, \ldots, Y_d]$ with $d \leq n$.*

Proof. We identify K with its image under the given epimorphism $\Phi\colon K[X_1, \ldots, X_n] \to R$. If Φ is injective, then the assertion holds with $d = n$ and $S = R$. This includes the case $n = 0$. So let $n \geq 1$ and assume the existence of S for $n - 1$ has already been proven. Let $x_i := \Phi(X_i) \in R$ for $i = 1, \ldots, n$. Let $\alpha \in \operatorname{Ker}(\Phi) \setminus \{0\}$ and $q := 1 + \deg \alpha$. We substitute X_i by $X_i + X_n^{q^i}$ for $i = 1, \ldots, n-1$. A monomial $X_1^{a_1} \ldots X_n^{a_n}$ in α then becomes

$$(X_1 + X_n^q)^{a_1} \ldots (X_{n-1} + X_n^{q^{n-1}})^{a_{n-1}} X_n^{a_n} = \ldots + X_n^{a_1 q + \ldots + a_{n-1} q^{n-1} + a_n}.$$

Because $a_1, \ldots, a_n < q$, the expression $a_n + a_1 q + \ldots + a_{n-1} q^{n-1}$ is a q-adic expansion. For different n-tuples $(a_1, \ldots, a_n)$, one therefore obtains different powers of X_n. In particular, there exists exactly one such power X_n^e with maximal exponent e. If $c \in K^\times$ is the corresponding coefficient, then

$$\beta := c^{-1}\alpha(X_1 + X_n^q, \ldots, X_{n-1} + X_n^{q^{n-1}}, X_n)$$

is monic of degree e as a polynomial in X_n. Let $y_i := x_i - x_n^{q^i} \in R$ for $i = 1, \ldots, n-1$ and $T := K[y_1, \ldots, y_{n-1}] \subseteq R$. By induction, T is finitely generated over a subring $S \cong K[Y_1, \ldots, Y_d]$ with $d \leq n-1$. Furthermore, $\gamma := \beta(y_1, \ldots, y_{n-1}, X_n) \in T[X_n]$ is monic of degree e with

$$\gamma(x_n) = c^{-1}\alpha(x_1, \ldots, x_n) = c^{-1}\Phi(\alpha) = 0.$$

Rearranging yields $x_n^e = \sum_{i=1}^{e-1} \gamma_i x_n^i$ with $\gamma_1, \ldots, \gamma_{d-1} \in T$. By assumption, R is generated as a K-vector space by the monomials in $x_1, \ldots, x_n$. In this process, we may replace $x_1, \ldots, x_{n-1}$ by $y_1, \ldots, y_{n-1}$. Therefore, R is generated as a T-module by $1, x_n, \ldots, x_n^{e-1}$. Thus, R is also a finitely generated S-module. □

Definition III.2.25. In the situation of Theorem III.2.24, the subring $K[Y_1, \ldots, Y_d] \cong S \subseteq R$ is called a *Noether normalization* of R.

Theorem III.2.26. *If $A \in \mathrm{A}(K^n)$ is irreducible, then $\dim A$ is the transcendence degree of $K(A)$ over K.*

Proof. Let $K[Y_1, \ldots, Y_d] \cong S \subseteq K[A]$ be a Noether normalization of $K[A]$. According to Example II.11.7, $S \subseteq K[A]$ is an integral ring extension and Theorem II.11.18 shows $\dim A = \dim K[A] = \dim S$. According to Corollary III.1.40, $\dim S = d$ holds. Now let $\alpha_1, \ldots, \alpha_k$ be a generating system of $K[A]$ as an S-module. Then $K(A) = Q(S)(\alpha_1, \ldots, \alpha_k)$ holds. Since $S \subseteq K[A]$ is integral, the field extension $K(Y_1, \ldots, Y_d) \cong Q(S) \subseteq K(A)$ is algebraic. This shows $\mathrm{trg}(K(A)|K) = d = \dim A$. □

Corollary III.2.27. *For $\alpha \in K[X_1, \ldots, X_n] \setminus K$, we have $\dim \mathcal{V}(\alpha) = n - 1$.*

Proof. For the prime factorization $\alpha = \alpha_1^{e_1} \ldots \alpha_k^{e_k}$, it holds that $A := \mathcal{V}(\alpha) = \mathcal{V}(\alpha_1) \cup \ldots \cup \mathcal{V}(\alpha_k)$. We can therefore assume that α is irreducible. Then $\mathcal{I}(A) = \sqrt{(\alpha)} = (\alpha)$ holds. Let $\overline{X_i} := X_i + (\alpha) \in K(A)$ for $i = 1, \ldots, n$. Because of $\alpha(\overline{X_1}, \ldots, \overline{X_n}) = 0$, the elements $\overline{X_1}, \ldots, \overline{X_n}$ are algebraically dependent over K. From the basis extension theorem II.4.12 it follows that $\mathrm{trg}(K(A)|K) \leq n-1$. For the reverse inequality, we can wlog. assume that X_n occurs in α. Suppose there exists a $\beta \in K[X_1, \ldots, X_{n-1}]$ with $\beta(\overline{X_1}, \ldots, \overline{X_{n-1}}) = 0$ in $K(A)$. Then it follows that $\alpha \mid \beta$. Since X_n does not occur in β, it must be that $\beta = 0$. This shows that $\overline{X_1}, \ldots, \overline{X_{n-1}}$ are algebraically independent over K. □

Remark III.2.28. Corollary III.2.27 suggests the term *hypersurface* (as a non-linear version of the hyperplane) for varieties of the form $\mathcal{V}(\alpha)$ with $\alpha \in K[X_1, \ldots, X_n] \setminus K$.

Example III.2.29. Let $A = \mathcal{V}(X^2 - YZ, XZ - X)$ as in Example III.2.18. The components $\mathcal{V}(X, Y)$ and $\mathcal{V}(X, Z)$ obviously have dimension 1. For $A_3 := \mathcal{V}(X^2 - Y, Z - 1)$, it holds that $K[A_3] \cong K[X, Y]/(X^2 - Y)$. According to Corollary III.2.27, A_3 is a hypersurface in K^2 and therefore $\dim A = 1$ according to Lemma III.2.21.

Lemma III.2.30. *Let $I \trianglelefteq K[X_1, \ldots, X_n]$ and $a_1, \ldots, a_d \in K^n \setminus \mathcal{V}(I)$. Then there exists an $\alpha \in I$ with $\alpha(a_i) \neq 0$ for $i = 1, \ldots, d$.*

Proof. Induction on d: In the case $d = 1$, the claim is trivial. Let $d \geq 2$. By induction, there exist $\alpha_i \in I$ with $\alpha_i(a_j) \neq 0$ for $i \neq j$. Wlog. let $\alpha_i(a_i) = 0$ for $i = 1, \ldots, d$ (otherwise choose $\alpha := \alpha_i$). Now $\alpha := \alpha_1 + \alpha_2 \ldots \alpha_d$ has the desired property. □

Remark III.2.31. As is well known, the discriminant of a polynomial $\alpha \in K[X]$ determines whether α has a multiple root in the algebraic closure of K. We define an invariant that indicates whether two arbitrary polynomials have a common root (divisor).

Definition III.2.32. Let R be an integral domain, $\alpha = \sum_{i=0}^{d} a_i X^i \in R[X]$ and $\beta = \sum_{i=0}^{e} b_i X^i \in R[X]$ with $a_d \neq 0 \neq b_e$. One calls

$$S(\alpha, \beta) := \begin{pmatrix} a_0 & & & 0 & b_0 & & 0 \\ a_1 & \ddots & & & b_1 & \ddots & \\ \vdots & \ddots & \ddots & & \vdots & \ddots & b_0 \\ a_d & & \ddots & a_0 & \vdots & & b_1 \\ & \ddots & & a_1 & b_e & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ 0 & & & a_d & 0 & & b_e \end{pmatrix} \in R^{(d+e)\times(d+e)}$$

the *Sylvester matrix* of α, β (if $d + e > 0$). Its determinant $\operatorname{res}(\alpha, \beta) := \det S(\alpha, \beta) \in R$ is called the *resultant* of α, β.[1] For $d = e = 0$ let $\operatorname{res}(\alpha, \beta) := 1$. Furthermore, let $\operatorname{res}(0, \beta) = 0 = \operatorname{res}(\alpha, 0)$.

Example III.2.33.

(i) For $d = 0$ we have $S(\alpha, \beta) = \operatorname{diag}(a_0, \ldots, a_0)$ and $\operatorname{res}(\alpha, \beta) = a_0^e$. Furthermore,

$$\operatorname{res}(X - a, X - b) = \begin{vmatrix} -a & -b \\ 1 & 1 \end{vmatrix} = b - a.$$

(ii) By de swaps of two adjacent columns of $S(\alpha, \beta)$ one obtains $\operatorname{res}(\beta, \alpha) = (-1)^{de} \operatorname{res}(\alpha, \beta)$.

Theorem III.2.34. *Let R be a factorial ring and $\alpha, \beta \in R[X] \setminus \{0\}$. $\gcd(\alpha, \beta) \in R$ holds if and only if $\operatorname{res}(\alpha, \beta) \neq 0$.*

Proof. According to Gauss, $R[X]$ is factorial. Let $d := \deg \alpha$ and $e := \deg \beta$. Let $\delta \in R[X] \setminus R$ be a common divisor of α, β. Then $\alpha \frac{\beta}{\delta} - \beta \frac{\alpha}{\delta} = 0$ holds. We write $\frac{\beta}{\delta} = \sum a'_i X^i$ and $-\frac{\alpha}{\delta} = \sum b'_i X^i$. Because of $\deg \delta > 0$, we have $a'_i = b'_j = 0$ for $i \geq e$ and $j \geq d$. This shows

$$\begin{aligned} a_0 a'_0 + b_0 b'_0 &= 0 \\ a_1 a'_0 + a_0 a'_1 + b_1 b'_0 + b_0 b'_1 &= 0 \\ &\vdots \\ a_d a'_{e-1} + b_e b'_{d-1} &= 0. \end{aligned}$$

Therefore $(a'_0, \ldots, a'_{e-1}, b'_0, \ldots, b'_{d-1})$ is a non-trivial solution of the homogeneous system of equations with coefficient matrix $S(\alpha, \beta)$. After passing to $Q(R)$, it follows that $\operatorname{res}(\alpha, \beta) = 0$.

[1] Do not confuse the resultant with the (cubic) resolvent.

Conversely, if $\operatorname{res}(\alpha,\beta)=0$, then there exists a non-trivial solution $(a'_0,\dots,a'_{e-1},b'_0,\dots,b'_{d-1})\in Q(R)^{d+e}$ of the said system of equations. After multiplication by a common denominator, we can assume $(a'_0,\dots,a'_{e-1},b'_0,\dots,b'_{d-1})\in R^{d+e}$. For $\tilde{\alpha}=\sum a'_iX^i$ and $\tilde{\beta}=\sum b'_iX^i$ we now have $\alpha\tilde{\alpha}+\beta\tilde{\beta}=0$, hence $\alpha\tilde{\alpha}=-\beta\tilde{\beta}$. In the case $\gcd(\alpha,\beta)\in R$, every non-constant prime divisor of α would have to be a divisor of $\tilde{\beta}$. However, this is impossible because of $\deg\tilde{\beta}<d$. Thus $\gcd(\alpha,\beta)\notin R$ is shown. □

Remark III.2.35.

(i) If R is a field, the condition $\gcd(\alpha,\beta)\in R$ means that α and β are coprime.

(ii) The next result is a substitute for Bézout's Lemma.

Lemma III.2.36. *Let R be an integral domain and $\alpha,\beta\in R[X]\setminus R$. Then there exist $\gamma,\delta\in R[X]$ with $\alpha\gamma+\beta\delta=\operatorname{res}(\alpha,\beta)$.*

Proof. As before, let $d:=\deg\alpha$ and $e:=\deg\beta$. By assumption, $d,e\geq 1$. For $i=2,\dots,d+e$, we add X^{i-1} times the i-th row of the Sylvester matrix to the first row (Gaussian elimination):

$$\operatorname{res}(\alpha,\beta)=\begin{vmatrix}
\alpha & X\alpha & \cdots & X^{e-1}\alpha & \beta & \cdots & X^{d-1}\beta\\
a_1 & \ddots & & & b_1 & \ddots & \\
\vdots & \ddots & \ddots & & \vdots & \ddots & b_0\\
a_d & & \ddots & a_0 & \vdots & & b_1\\
 & \ddots & & a_1 & b_e & & \vdots\\
 & & \ddots & \vdots & & \ddots & \vdots\\
 & & & a_d & & & b_e
\end{vmatrix}.$$

Laplace expansion along the first row yields $r_0,\dots,r_{e-1},s_0,\dots,s_{d-1}\in R$ with

$$\operatorname{res}(\alpha,\beta)=\sum_{i=0}^{e-1}\alpha X^ir_i+\sum_{i=0}^{d-1}\beta X^is_i.$$

The claim follows with $\gamma=\sum r_iX^i$ and $\delta=\sum s_iX^i$. □

Lemma III.2.37. *Let R be an integral domain and $\alpha,\beta,\gamma\in R[X]$. Then*

$$\operatorname{res}(\alpha\beta,\gamma)=\operatorname{res}(\alpha,\gamma)\operatorname{res}(\beta,\gamma).$$

Proof. We may replace R by $K:=Q(R)$. Wlog. let $\alpha\neq 0\neq\gamma$ with $d:=\deg\alpha$ and $f:=\deg\gamma$. From the linearity of the determinant in the columns of the Sylvester matrix, it follows that $\operatorname{res}(\alpha,c\gamma)=c^d\operatorname{res}(\alpha,\gamma)$ for all $c\in K$. We can therefore assume that γ is monic. We consider the K-vector space V of all polynomials of degree $<d+f$ with respect to the bases

$$B:=\{1,X,\dots,X^{d+f-1}\},$$
$$C:=\{1,X,\dots,X^{f-1},\gamma,X\gamma,\dots,X^{d-1}\gamma\}.$$

Let $F_\alpha\in\operatorname{End}_K(V)$ with $F_\alpha(X^i):=\alpha X^i$ for $i=0,\dots,f-1$ and $F_\alpha(X^i\gamma):=X^i\gamma$ for $i=0,\dots,d-1$. With respect to C and B, F_α has the representation matrix ${}_B[F_\alpha]_C:=S(\alpha,\gamma)$. The change of basis matrix T from B to C is an upper triangular matrix with ones on the main diagonal, since γ is monic.

In particular, $\det T = 1$. For the representation matrix of F_α with respect to B and B, it therefore holds that ${}_B[F_\alpha]_B = {}_B[F_\alpha]_C T$ and $\det F_\alpha = \det(S(\alpha,\gamma))\det(T) = \operatorname{res}(\alpha,\gamma)$.

Since F_α operates trivially on the subspace $W := \langle \gamma, X\gamma, \ldots, X^{d-1}\gamma\rangle$, F_α induces an endomorphism $\overline{F_\alpha}$ on $\overline{V} := V/W \simeq K[X]/(\gamma)$ with the same determinant. In fact, $\overline{F_\alpha}$ merely describes the multiplication by α modulo (γ). In particular, $\overline{F_{\alpha\beta}} = \overline{F_\alpha} \circ \overline{F_\beta}$. This shows

$$\operatorname{res}(\alpha\beta,\gamma) = \det \overline{F_{\alpha\beta}} = \det(\overline{F_\alpha} \circ \overline{F_\beta}) = \det(F_\alpha)\det(F_\beta) = \operatorname{res}(\alpha,\gamma)\operatorname{res}(\beta,\gamma). \qquad \square$$

Remark III.2.38. For $d = \deg\alpha$, $e = \deg\beta$ and $f = \deg\gamma$ it holds that

$$\operatorname{res}(\gamma,\alpha\beta) = (-1)^{f(d+e)}\operatorname{res}(\alpha\beta,\gamma) = (-1)^{df}\operatorname{res}(\alpha,\gamma)(-1)^{ef}\operatorname{res}(\beta,\gamma) = \operatorname{res}(\gamma,\alpha)\operatorname{res}(\gamma,\beta)$$

according to Example III.2.33.

Theorem III.2.39. *Let R be an integral domain and $\alpha, \beta \in R[X]$ monic. Let $x_1, \ldots, x_d$ and $y_1, \ldots, y_e$ be the roots of α and β in the algebraic closure $\overline{Q(R)}$. Then*

$$\operatorname{res}(\alpha,\beta) = \prod_{i=1}^{d}\prod_{j=1}^{e}(y_j - x_i).$$

Proof. Wlog. let $R = \overline{Q(R)}$. From Lemma III.2.37, Remark III.2.38 and Example III.2.33 it follows that

$$\begin{aligned}\operatorname{res}(\alpha,\beta) &= \operatorname{res}((X-x_1)\ldots(X-x_d),(X-y_1)\ldots(X-y_e)) \\ &= \prod_{i=1}^{d}\prod_{j=1}^{e}\operatorname{res}(X-x_i, X-y_j) = \prod_{i=1}^{d}\prod_{j=1}^{e}(y_j - x_i).\end{aligned} \qquad \square$$

Corollary III.2.40. *Let $\alpha \in K[X] \setminus K$ be monic of degree d. Then $D_\alpha = (-1)^{\frac{d(d-1)}{2}}\operatorname{res}(\alpha',\alpha)$.*

Proof. Wlog. let $K = \overline{K}$. According to Theorem I.11.20, K is perfect. In the case $\alpha' = 0$, $\alpha = \beta^p$ with $\beta \in K[X]$ and $p = \operatorname{char} K > 0$ (cf. proof of Theorem I.11.20). Then α has a multiple root and it follows $D_\alpha = 0 = \operatorname{res}(\alpha',\alpha)$. Let therefore $\alpha = (X-x_1)\ldots(X-x_d)$ and $\alpha' = c(X-y_1)\ldots(X-y_e)$ with $c \in K^\times$. According to the product rule, $\alpha' = \sum_{i=1}^{d}\frac{\alpha}{X-x_i}$ holds. This shows

$$c\prod_{j=1}^{e}(x_i - y_j) = \alpha'(x_i) = \prod_{j\neq i}(x_i - x_j)$$

for $i = 1, \ldots, d$. With Theorem III.2.39 it follows

$$\operatorname{res}(\alpha',\alpha) = c^d\prod_{i=1}^{d}\prod_{j=1}^{e}(x_i - y_j) = \prod_{i=1}^{d}\prod_{j\neq i}(x_i - x_j) = (-1)^{\frac{d(d-1)}{2}}\prod_{i<j}(x_j - x_i)^2 = (-1)^{\frac{d(d-1)}{2}}D_\alpha. \qquad \square$$

Remark III.2.41.

(i) For $\operatorname{char} K \nmid \deg(\alpha)$, $\deg\alpha = \deg(\alpha') + 1$ and $\operatorname{res}(\alpha',\alpha) = \operatorname{res}(\alpha,\alpha')$ according to Example III.2.33.

(ii) By means of the Sylvester matrix, Corollary III.2.40 enables the calculation of the discriminant without leaving R.

Example III.2.42. Let $\operatorname{char} K \neq 3$ and $\alpha = X^3 + aX + b \in K[X]$. Then

$$D_\alpha = -\operatorname{res}(\alpha', \alpha) = -\begin{vmatrix} a & . & . & b & . \\ . & a & . & a & b \\ 3 & . & a & . & a \\ . & 3 & . & 1 & . \\ . & . & 3 & . & 1 \end{vmatrix} = -\begin{vmatrix} 3 & . & a & . & a \\ . & 3 & . & 1 & . \\ . & . & 3 & . & 1 \\ a & . & . & b & . \\ . & a & . & a & b \end{vmatrix} = -\begin{vmatrix} 3 & . & a & . & a \\ . & 3 & . & 1 & . \\ . & . & 3 & . & 1 \\ . & . & -\frac{1}{3}a^2 & b & -\frac{1}{3}a^2 \\ . & . & . & \frac{2}{3}a & b \end{vmatrix}$$

$$= -\begin{vmatrix} 3 & . & a & . & a \\ . & 3 & . & 1 & . \\ . & . & 3 & . & 1 \\ . & . & . & b & -\frac{2}{9}a^2 \\ . & . & . & \frac{2}{3}a & b \end{vmatrix} = -27(b^2 + \frac{4}{27}a^3) = -4a^3 - 27b^2$$

(cf. Example I.14.24).

Theorem III.2.43. *If $I \trianglelefteq K[X_1, \ldots, X_n]$ contains a polynomial that is monic with respect to X_n, then the projection*

$$\begin{aligned} \pi\colon \mathcal{V}(I) &\to \mathcal{V}(I \cap K[X_1, \ldots, X_{n-1}]) \subseteq K^{n-1}, \\ (x_1, \ldots, x_n) &\mapsto (x_1, \ldots, x_{n-1}) \end{aligned}$$

is surjective.

Proof. Obviously, the projection is at least well-defined. Let $(x_1, \ldots, x_{n-1}) \in K^{n-1} \setminus \pi(\mathcal{V}(I))$. Let $\alpha \in I$ be monic in X_n. In the case $\alpha = 1$, both sets are empty. So let $\alpha \notin K$. Let $y_1, \ldots, y_d$ be the roots of $\tilde{\alpha} := \alpha(x_1, \ldots, x_{n-1}, X_n) \in K[X_n] \setminus K$. According to Lemma III.2.30, there exists $\beta \in I$ with $\beta(x_1, \ldots, x_{n-1}, y_i) \neq 0$ for $i = 1, \ldots, d$. In the case $\beta \in R := K[X_1, \ldots, X_{n-1}]$, it already holds that $(x_1, \ldots, x_{n-1}) \notin \mathcal{V}(I \cap R)$. So let $\tilde{\beta} := \beta(x_1, \ldots, x_{n-1}, X_n) \in K[X] \setminus K$. Since $\tilde{\alpha}$ and $\tilde{\beta}$ have no common roots, they are coprime. For $\gamma := \operatorname{res}(\alpha, \beta) \in R$, it therefore holds that $\gamma(x_1, \ldots, x_{n-1}) = \operatorname{res}(\tilde{\alpha}, \tilde{\beta}) \neq 0$ according to Theorem III.2.34. According to Lemma III.2.36, $\gamma \in (\alpha, \beta) \cap R \subseteq I \cap R$. This shows $(x_1, \ldots, x_{n-1}) \notin \mathcal{V}(I \cap R)$. □

Example III.2.44. Obviously, $I := (1 - XY) \trianglelefteq K[X, Y]$ contains *no* monic polynomial in Y. Indeed, the projection $\pi\colon \mathcal{V}(I) \to \mathcal{V}(I \cap K[X]) = \mathcal{V}(0) = K$ is also not surjective, because $0 \notin \pi(\mathcal{V}(I))$.

Remark III.2.45. Theorem III.2.43 enables the elimination of variables (specifically X_n). One therefore calls $I \cap K[X_1, \ldots, X_{n-1}]$ an *elimination ideal*. The calculation of elimination ideals in practice leads to a more general problem:

How can one determine whether a polynomial $\alpha \in R := K[X_1, \ldots, X_n]$ lies in a given ideal $I := (\beta_1, \ldots, \beta_k) \trianglelefteq R$? For $n = 1$, $\gamma := \gcd(\beta_1, \ldots, \beta_k)$ can be calculated with the Euclidean algorithm. It then holds that $\alpha \in I \iff \gamma \mid \alpha$ (Bézout's Lemma). For $n \geq 2$, however, R is not Euclidean and the resultant is not sufficient for calculating the gcd. We therefore seek a replacement for Euclidean division. For this, let K be an arbitrary field (not necessarily $K = \overline{K}$).

Definition III.2.46. Let $\mathcal{M} := \{X_1^{i_1} \ldots X_n^{i_n} : i_1, \ldots, i_n \in \mathbb{N}_0\}$ be the set of all monomials of $R := K[X_1, \ldots, X_n]$. A total ordering relation $\leq$ on $\mathcal{M}$ is called a *monomial order* on R if for all $\alpha, \beta, \gamma \in \mathcal{M}$ it holds that

- $1 \leq \alpha$.

- $\alpha < \beta \implies \alpha\gamma < \beta\gamma$.

Remark III.2.47. Let $\alpha, \beta \in \mathcal{M}$ with $\alpha \mid \beta$. From $1 \leq \frac{\beta}{\alpha}$ it follows that $\alpha \leq \beta$. The divisibility relation, however, cannot be a monomial order for $n \geq 2$, since it is not total.

Example III.2.48.

(i) For $n = 1$, $\alpha \leq \beta \iff \deg \alpha \leq \deg \beta$ is the only monomial order.

(ii) In the proof of Theorem I.14.19, we have already used the lexicographical order with $X_1 > \ldots > X_n$. It is easily shown that it is a monomial order. Another monomial order is constructed in Exercise III.6.

Lemma III.2.49 (Dickson)**.** *For $M \subseteq \mathcal{M}$, there exists a finite subset $N \subseteq M$ with $(M) = (N)$.*

Proof. According to Hilbert's Basis Theorem, there exist $\alpha_1, \ldots, \alpha_k \in K[X_1, \ldots, X_n]$ with $(M) = (\alpha_1, \ldots, \alpha_k)$. For a fixed i, let $\beta_1, \ldots, \beta_s \in M$ and $\gamma_1, \ldots, \gamma_s \in K[X_1, \ldots, X_n]$ with $\alpha_i = \beta_1\gamma_1 + \ldots + \beta_s\gamma_s$. Every monomial of α_i occurs in one of the summands $\beta_j\gamma_j$ and therefore lies in (β_j). Thus, α_i is generated by finitely many elements in M. Overall, $(\alpha_1, \ldots, \alpha_k)$ is also generated by finitely many elements in M. □

Lemma III.2.50. *Let $\leq$ be a monomial order on $K[X_1, \ldots, X_n]$. Then there exists no infinite descending chain $\alpha_1 > \alpha_2 > \ldots$ in $\mathcal{M}$. In particular, every non-empty subset of $\mathcal{M}$ possesses a smallest element.*

Proof. Suppose there exist $\alpha_1, \ldots \in \mathcal{M}$ with $\alpha_1 > \alpha_2 > \ldots$. According to Lemma III.2.49, there exist $\beta_1, \ldots, \beta_k \in \{\alpha_1, \ldots\}$ with $(\alpha_1, \ldots) = (\beta_1, \ldots, \beta_k)$ and wlog. $\beta_1 > \ldots > \beta_k$. Let $\alpha_m < \beta_k$. Then there exist $\gamma_1, \ldots, \gamma_k \in K[X_1, \ldots, X_n]$ with $\alpha_m = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k$. It follows that $\beta_i \mid \alpha_m$ for some $1 \leq i \leq k$. From Remark III.2.47, one obtains the contradiction $\beta_i \leq \alpha_m < \beta_k \leq \beta_i$.

In every non-empty subset $M \subseteq \mathcal{M}$, there now exists a minimal element $\alpha \in M$. Since $\leq$ is total, α must be the smallest element of M (Remark II.1.5). □

Definition III.2.51. In the following, let $\leq$ always be a fixed chosen monomial order. We sort the monomials of a polynomial $\alpha \in K[X_1, \ldots, X_n] \setminus \{0\}$ according to $\leq$ without consideration of the coefficients. Let the largest monomial (*leading monomial*) in α be $\operatorname{lm} \alpha \in \mathcal{M}$ and its coefficient (*leading coefficient*) be $\operatorname{lc} \alpha \in K^\times$. Additionally, let $\operatorname{lm} 0 := 0 =: \operatorname{lc} 0$, where $0 < \rho$ holds for all $\rho \in \mathcal{M}$ (this corresponds to $\deg 0 = -\infty$). In the case $\operatorname{lc} \alpha = 1$, α is called *monic*.

Theorem III.2.52. *Let $R := K[X_1, \ldots, X_n]$. For $\alpha, \beta_1, \ldots, \beta_k \in R \setminus \{0\}$ there exist $\gamma_1, \ldots, \gamma_k, \delta \in R$ with*

(i) $\alpha = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k + \delta$.

(ii) $\operatorname{lm}(\beta_i\gamma_i) \leq \operatorname{lm} \alpha$ *for* $i = 1, \ldots, k$.

(iii) No monomial in δ is divisible by any $\operatorname{lm} \beta_i$.

Proof. If no monomial in α is divisible by any $\operatorname{lm}\beta_i$, then the statement holds with $\gamma_1 = \ldots = \gamma_k = 0$ and $\delta = \alpha$. So let ρ_1 be the largest monomial in $\alpha_1 := \alpha$ that is divisible by some $\operatorname{lm}\beta_i$. Then there exists $c_1 \in K$ such that ρ_1 no longer occurs in

$$\alpha_2 := \alpha_1 - c_1 \frac{\rho_1}{\operatorname{lm}\beta_i}\beta_i$$

(it was replaced by smaller monomials). We repeat the process with α_2 and obtain a sequence $\alpha_1, \alpha_2, \ldots$ with monomials $\rho_1 > \rho_2 > \ldots$. According to Lemma III.2.50, the sequence must terminate, say at the position $\alpha_s =: \delta$. Now no monomial in δ is divisible by any $\operatorname{lm}\beta_i$. Furthermore, $\alpha = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k + \delta$ holds, where each γ_i is a sum of terms of the form $c_j \frac{\rho_j}{\operatorname{lm}\beta_i}$. In particular, $\operatorname{lm}(\beta_i\gamma_i) \leq \rho_1 \leq \operatorname{lm}\alpha$ holds for $i = 1, \ldots, k$. □

Remark III.2.53. For $n = 1$, Theorem III.2.52 yields exactly the Euclidean division. In general, $\gamma_1, \ldots, \gamma_k, \delta$ are not uniquely determined by the given properties (we did not specify in the proof which β_i should be chosen if there are several that divide ρ_1). Nevertheless, we call δ a *remainder* in the division of α by $\beta_1, \ldots, \beta_k$. For $\alpha = 0$, $\gamma_1 = \ldots = \gamma_k = 0 = \delta$ because of $\operatorname{lm}(\beta_i\gamma_i) \leq \operatorname{lm}\alpha = 0$.

Example III.2.54. Let $\alpha = X^2Y - Y$, $\beta_1 = XY - X$ and $\beta_2 = X^2 - Y$. With respect to the lexicographical monomial ordering, $\rho_1 = X^2Y$ is divisible by $\operatorname{lm}\beta_1 = XY$. One obtains

$$\alpha_2 = \alpha - X\beta_1 = X^2 - Y = \beta_2.$$

Thus $\alpha = X\beta_1 + \beta_2$ holds with $\delta = 0$. However, ρ_1 is also divisible by $\operatorname{lm}\beta_2 = X^2$. This time one obtains

$$\alpha_2 = \alpha - Y\beta_2 = Y^2 - Y.$$

Now $\rho_2 = \operatorname{lm}\alpha_2 = Y^2$ is no longer divisible by $\operatorname{lm}\beta_1$ or $\operatorname{lm}\beta_2$. Here, therefore, $\delta = Y(Y-1) \neq 0$ and $\alpha = 0\beta_1 + Y\beta_2 + \delta$ holds.

Definition III.2.55. Let $I \trianglelefteq R := K[X_1, \ldots, X_n]$ and $\operatorname{lm} I := (\operatorname{lm}\alpha : \alpha \in I) \trianglelefteq R$. One calls $\beta_1, \ldots, \beta_k \in R \setminus \{0\}$ a *Gröbner basis* of I if $I = (\beta_1, \ldots, \beta_k)$ and $\operatorname{lm} I = (\operatorname{lm}\beta_1, \ldots, \operatorname{lm}\beta_k)$.

Remark III.2.56. Despite their name, two Gröbner bases of an ideal I can have different numbers of elements. For example, if B is a Gröbner basis of I and $\alpha \in I \setminus B$, then $B \cup \{\alpha\}$ is also a Gröbner basis of I. We introduce a minimality condition in Definition III.2.65.

Theorem III.2.57 (Gröbner)**.** *Let $\beta_1, \ldots, \beta_k$ be a Gröbner basis of $I \trianglelefteq R := K[X_1, \ldots, X_n]$. For $\alpha \in R$, the remainder δ in the division of α by $\beta_1, \ldots, \beta_k$ is uniquely determined and $\alpha \in I$ holds if and only if $\delta = 0$.*

Proof. Let $\alpha = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k + \delta = \beta_1\tilde{\gamma}_1 + \ldots + \beta_k\tilde{\gamma}_k + \tilde{\delta}$ be two decompositions as in Theorem III.2.52. Then $\delta - \tilde{\delta} \in I$ and there exist $\sigma_1, \ldots, \sigma_k \in R$ with $\operatorname{lm}(\delta - \tilde{\delta}) = \sigma_1 \operatorname{lm}\beta_1 + \ldots \sigma_k \operatorname{lm}\beta_k$. In the case $\delta \neq \tilde{\delta}$, a monomial of δ or $\tilde{\delta}$ would be divisible by some $\operatorname{lm}\beta_i$. This contradicts Theorem III.2.52. Thus $\delta = \tilde{\delta}$.

From $\delta = 0$ it follows immediately that $\alpha \in I$. Conversely, let $\alpha \in I$. Then $\delta \in (\alpha, \beta_1, \ldots, \beta_k) = I$. In the case $\delta \neq 0$, we would have $\operatorname{lm}\delta \in \operatorname{lm} I$ and $\operatorname{lm}\beta_i \mid \operatorname{lm}\delta$ for some i in contradiction to Theorem III.2.52. Thus $\delta = 0$. □

Example III.2.58. According to Example III.2.54, $\beta_1 = XY - X$, $\beta_2 = X^2 - Y$ is *not* a Gröbner basis of $I = (\beta_1, \beta_2)$. Because of $Y = X\beta_1 - (Y-1)\beta_2 \in I$ and $X = XY - \beta_1 \in I$, X, Y is a Gröbner basis of I.

Theorem III.2.59. *Every ideal in $K[X_1, \ldots, X_n]$ possesses a Gröbner basis.*

Proof. Let $I \trianglelefteq R := K[X_1, \ldots, X_n]$. In the case $I = 0$, choose the Gröbner basis $\varnothing$. So let $I \neq 0$. According to Lemma III.2.49, there exist $\beta_1, \ldots, \beta_k \in I \setminus \{0\}$ with $\operatorname{lm} I = (\operatorname{lm}\beta_1, \ldots, \operatorname{lm}\beta_k)$. Let $\alpha \in I$ be arbitrary. Let $\gamma_1, \ldots, \gamma_k, \delta \in R$ be as in Theorem III.2.52. Then $\delta \in I$ also holds. In the case $\delta \neq 0$, $\operatorname{lm}\delta \in \operatorname{lm} I$. As in the proof of Theorem III.2.57, $\operatorname{lm}\beta_i \mid \operatorname{lm}\delta$ would then hold for some i. Thus $\delta = 0$ and $\alpha \in (\beta_1, \ldots, \beta_k)$. This shows $I = (\beta_1, \ldots, \beta_k)$, i. e. $\beta_1, \ldots, \beta_k$ is a Gröbner basis of I. □

Remark III.2.60. The proof of Theorem III.2.59 shows that $\beta_1, \ldots, \beta_k \in K[X_1, \ldots, X_n]$ is already a Gröbner basis of I if $\operatorname{lm} I = (\operatorname{lm}\beta_1, \ldots, \operatorname{lm}\beta_k)$ holds, i. e. the condition $I = (\beta_1, \ldots, \beta_k)$ is redundant.

Theorem III.2.61 (Buchberger Criterion)**.** *Let $\beta_1, \ldots, \beta_k \in K[X_1, \ldots, X_n] \setminus \{0\}$ be monic, $\gamma_{ij} := \operatorname{lcm}(\operatorname{lm}\beta_i, \operatorname{lm}\beta_j)$ and*

$$\alpha_{ij} := \frac{\gamma_{ij}}{\operatorname{lm}\beta_i}\beta_i - \frac{\gamma_{ij}}{\operatorname{lm}\beta_j}\beta_j$$

for $i < j$. Let δ_{ij} be a remainder of the division of α_{ij} by $\beta_1, \ldots, \beta_k$. Then $\beta_1, \ldots, \beta_k$ is a Gröbner basis of $(\beta_1, \ldots, \beta_k)$ if and only if $\delta_{ij} = 0$ for all $i < j$.

Proof. If $\beta_1, \ldots, \beta_k$ is a Gröbner basis of I, then $\delta_{ij} = 0$ for $i < j$ according to Theorem III.2.57, because $\alpha_{ij} \in I$. Conversely, let us assume $\delta_{ij} = 0$ for $i < j$. Every $\alpha \in I \setminus \{0\}$ has the form $\alpha = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k$ with $\gamma_1, \ldots, \gamma_k \in K[X_1, \ldots, X_n]$. Let

$$\rho := \max_{1 \le i \le k} \operatorname{lm}(\beta_i\gamma_i).$$

Among all possible representations of α, we choose $\gamma_1, \ldots, \gamma_k$ such that ρ becomes as small as possible (this is possible due to Lemma III.2.50).

Assumption: ρ is not a monomial of α.
After renumbering, we can achieve $\operatorname{lm}(\beta_i\gamma_i) = \rho$ for $i = 1, \ldots, l$. Here, $l \ge 2$ must hold, because otherwise one could not eliminate ρ from $\beta_1\gamma_1 + \ldots + \beta_k\gamma_k = \alpha$. For the same reason, $\operatorname{lm}(\beta_1\gamma_1 + \ldots + \beta_l\gamma_l) < \rho$ holds. Let $\operatorname{lc}\gamma_i = a_i$, $\operatorname{lm}\gamma_i = \rho_i$ and $\tilde{\beta}_i := \beta_i\rho_i$ for $i = 1, \ldots, k$. Then $\operatorname{lm}\tilde{\beta}_i = \rho$ for $i = 1, \ldots, l$ and $\operatorname{lm}(a_1\tilde{\beta}_1 + \ldots + a_l\tilde{\beta}_l) < \rho$. It follows that $a_1 + \ldots + a_l = 0$. We set

$$\tilde{\alpha}_{ij} := \tilde{\beta}_i - \tilde{\beta}_j = \frac{\rho}{\operatorname{lm}\beta_i}\beta_i - \frac{\rho}{\operatorname{lm}\beta_j}\beta_j = \frac{\rho}{\gamma_{ij}}\Big(\frac{\gamma_{ij}}{\operatorname{lm}\beta_i}\beta_i - \frac{\gamma_{ij}}{\operatorname{lm}\beta_j}\beta_j\Big) = \frac{\rho}{\gamma_{ij}}\alpha_{ij}$$

for $i, j = 1, \ldots, l$. Then

$$\begin{aligned} a_1\tilde{\beta}_1 + \ldots + a_l\tilde{\beta}_l &= a_1(\tilde{\beta}_1 - \tilde{\beta}_2) + (a_1 + a_2)(\tilde{\beta}_2 - \tilde{\beta}_3) + \ldots + (a_1 + \ldots + a_{h-1})(\tilde{\beta}_{l-1} - \tilde{\beta}_l) \\ &\quad + (a_1 + \ldots + a_l)\tilde{\beta}_l \\ &= \tilde{a}_1\tilde{\alpha}_{12} + \tilde{a}_2\tilde{\alpha}_{23} + \ldots + \tilde{a}_{l-1}\tilde{\alpha}_{l-1,l} \end{aligned}$$

with $\tilde{a}_i := a_1 + \ldots + a_i \in K$ for $i = 1, \ldots, l$. Because $\operatorname{lm}\tilde{\beta}_i = \rho = \operatorname{lm}\tilde{\beta}_j$, we have $\operatorname{lm}\tilde{\alpha}_{ij} < \rho$. By assumption, α_{ij} for $i < j$ can be "divided" by $\beta_1, \ldots, \beta_k$ without remainder. The same applies to α'_{ij} and $\tilde{a}_1\tilde{\alpha}_{12} + \tilde{a}_2\tilde{\alpha}_{23} + \ldots + \tilde{a}_{h-1}\tilde{\alpha}_{l-1,l}$. Thus there exist $\tilde{\gamma}_1, \ldots, \tilde{\gamma}_k \in K[X_1, \ldots, X_n]$ with

$$a_1\rho_1\beta_1 + \ldots + a_l\rho_l\beta_l = \tilde{a}_1\tilde{\alpha}_{12} + \tilde{a}_2\tilde{\alpha}_{23} + \ldots + \tilde{a}_{l-1}\tilde{\alpha}_{l-1,l} = \tilde{\gamma}_1\beta_1 + \ldots + \tilde{\gamma}_k\beta_k$$

and $\operatorname{lm}(\tilde{\gamma}_i\beta_i) \leq \operatorname{lm}(a_1\tilde{\beta}_1 + \ldots + a_l\tilde{\beta}_l) < \rho$ for $i = 1, \ldots, k$. Because $a_i\rho_i = \operatorname{lc}\gamma_i \operatorname{lm}\gamma_i$, we can modify the $\tilde{\gamma}_i$ such that

$$\beta_1\gamma_1 + \ldots + \beta_l\gamma_l = \beta_1\tilde{\gamma}_1 + \ldots + \beta_k\tilde{\gamma}_k$$

with $\operatorname{lm}(\beta_i\tilde{\gamma}_i) < \rho$ for $i = 1, \ldots, k$ holds. Another modification of the $\tilde{\gamma}_i$ yields

$$\alpha = \beta_1\gamma_1 + \ldots + \beta_k\gamma_k = \beta_1\tilde{\gamma}_1 + \ldots + \beta_k\tilde{\gamma}_k$$

still with $\operatorname{lm}(\beta_i\tilde{\gamma}_i) < \rho$ for $i = 1, \ldots, k$. This contradicts the choice of ρ.

Thus the monomial ρ occurs in α. This means $\operatorname{lm}(\beta_i\gamma_i) \leq \operatorname{lm}\alpha$ for $i = 1, \ldots, k$. In particular, $\operatorname{lm}\alpha$ is a K-linear combination of the $\operatorname{lm}(\beta_i\gamma_i)$, i.e., $\operatorname{lm}\alpha \in (\operatorname{lm}\beta_1, \ldots, \operatorname{lm}\beta_k)$. This shows that $\beta_1, \ldots, \beta_k$ is a Gröbner basis of I. □

Theorem III.2.62 (Buchberger Algorithm)**.**
Input: $\beta_1, \ldots, \beta_k \in K[X_1, \ldots, X_n] \setminus \{0\}$.
Initialization: Normalize $\beta_1, \ldots, \beta_k$ *and set* $B := \{\beta_1, \ldots, \beta_k\}$.
Repeat...
For $i < j$ *calculate and normalize* δ_{ij} *as in Theorem III.2.61 w.r.t. the polynomials in* B.
Add the $\delta_{ij} \neq 0$ *to the set* B.
... until $\delta_{ij} = 0$ *holds for all* $i < j$.
Output: B *is a Gröbner basis of* $(\beta_1, \ldots, \beta_k)$.

Proof. By definition, $\delta_{ij} \in (\beta_1, \ldots, \beta_k) =: I$ for $i < j$. In each step, $I = (B)$ therefore remains true. In the case $\delta_{ij} \neq 0$, no monomial in δ_{ij} is divisible by an $\operatorname{lm}\alpha$ with $\alpha \in B$. Then $(\operatorname{lm}\alpha : \alpha \in B) < (\operatorname{lm}\alpha, \operatorname{lm}\delta_{ij} : \alpha \in B)$ holds. Since $K[X_1, \ldots, X_n]$ is Noetherian, this sequence of ideals must become stationary. After finitely many steps, $\delta_{ij} = 0$ thus holds for all $i < j$. According to the Buchberger criterion, B is a Gröbner basis of I. □

Example III.2.63. Let $\beta_1 = XY - Y \in \mathbb{C}[X, Y]$ and $\beta_2 = X - Y^2 \in \mathbb{C}[X, Y]$ w.r.t. the lexicographical monomial order. As in Theorem III.2.61, let $\gamma_{12} = XY$ and $\alpha_{12} = \beta_1 - Y\beta_2 = Y^3 - Y$. Because of $\operatorname{lm}\alpha_{12} = Y^3 < \operatorname{lm}\beta_i$, $\beta_3 := \delta_{12} = \alpha_{12}$ must hold. With respect to $B = \{\beta_1, \beta_2, \beta_3\}$, we calculate

$$\begin{aligned} &\alpha_{12} = Y^2 - Y, && \alpha_{13} = Y^2\beta_1 - X\beta_3 = XY - Y^3, && \alpha_{23} = Y^3\beta_2 - X\beta_3 = XY - Y^5 \\ &\delta_{12} = \alpha_{12} - \beta_3 = 0, && \delta_{13} = \alpha_{13} - \beta_1 + \beta_3 = 0, && \delta_{23} = \alpha_{23} - \beta_1 + (Y^2 + 1)\beta_3 = 0. \end{aligned}$$

Consequently, B is a Gröbner basis of (β_1, β_2). We check whether $\alpha = X^3 + Y$ lies in I:

$$\alpha - X^2\beta_2 - (XY + Y)\beta_1 = X^2Y^2 + Y - (X^2Y^2 - Y^2) = Y^2 + Y.$$

Since Y^2 is not divisible by any $\operatorname{lm}\beta_i$, the remainder is $\delta = Y^2 + Y \neq 0$, i.e., $\alpha \notin I$.

Remark III.2.64. The Buchberger algorithm in combination with Theorem III.2.57 finds important applications in computer algebra:

(i) It can be decided whether a system of polynomial equations is solvable (check $1 \in I$). According to Exercise III.1, this even works over arbitrary fields.

(ii) One can check $\alpha \in \sqrt{(\beta_1, \ldots, \beta_k)}$. For this, one introduces a new variable Y as in the proof of the Nullstellensatz and checks $\alpha \in (\beta_1, \ldots, \beta_k, \alpha Y - 1)$.

(iii) Elimination ideals can be calculated (Exercise III.8).

(iv) The intersection of ideals $(\beta_1, \ldots, \beta_k) \cap (\gamma_1, \ldots, \gamma_l)$ can be calculated (Exercise III.9).

(v) The dimension of a variety $A \in \mathrm{A}(K^n)$ can be calculated as follows. Let $\beta_1, \ldots, \beta_k$ be a Gröbner basis of $\mathcal{I}(A)$ and $S \subseteq \{X_1, \ldots, X_n\}$ a largest possible subset with

$$(S) \cap \{\operatorname{lm} \beta_1, \ldots, \operatorname{lm} \beta_k\} = \varnothing.$$

Then $\dim A = |S|$ holds (without proof).

In practice, the Buchberger algorithm often yields redundant basis elements (see Example III.2.67). This can be fixed as follows.

Definition III.2.65. A Gröbner basis $\beta_1, \ldots, \beta_k$ is called *reduced*, if the following holds:

- $\beta_1, \ldots, \beta_k$ are monic.
- $\operatorname{lm} \beta_1 > \ldots > \operatorname{lm} \beta_k$.
- No monomial in β_i is divisible by an $\operatorname{lm} \beta_j$ with $i \neq j$.

Theorem III.2.66. *Every ideal $I \trianglelefteq K[X_1, \ldots, X_n]$ possesses exactly one reduced Gröbner basis $\beta_1, \ldots, \beta_k$ (with respect to $\leq$) and every Gröbner basis of I contains at least k polynomials.*

Proof. Wlog. let $I \neq 0$. Let $\beta_1, \ldots, \beta_k$ be an arbitrary Gröbner basis of I. Let us assume wlog. that a monomial in β_k is divisible by some $\operatorname{lm} \beta_i$. Theorem III.2.52 yields

$$\beta_k = \beta_1 \gamma_1 + \ldots + \beta_{k-1} \gamma_{k-1} + \delta,$$

where no monomial in δ is divisible by any $\operatorname{lm} \beta_i$. Obviously, $(\beta_1, \ldots, \beta_k) = (\beta_1, \ldots, \beta_{k-1}, \delta)$ holds. Because $\operatorname{lm}(\beta_i \gamma_i) \leq \operatorname{lm} \beta_k$, $\operatorname{lm} \beta_k$ can be written as a linear combination of $\operatorname{lm}(\beta_1 \gamma_1), \ldots, \operatorname{lm}(\beta_{k-1} \gamma_{k-1}), \operatorname{lm} \delta$. This shows $(\operatorname{lm} \beta_1, \ldots, \operatorname{lm} \beta_k) = (\operatorname{lm} \beta_1, \ldots, \operatorname{lm} \beta_{k-1}, \operatorname{lm} \delta)$. In the case $\delta = 0$, we remove β_k, and otherwise we replace β_k with δ. As in the proof of Theorem III.2.52, this process can only be repeated finitely many times, and in the end, no monomial in β_i is divisible by any $\operatorname{lm} \beta_j$ with $i \neq j$. In particular, $\operatorname{lm} \beta_i \neq \operatorname{lm} \beta_j$ for $i \neq j$ and $\operatorname{lm} \beta_1 > \ldots > \operatorname{lm} \beta_k$ after reordering. The normalization of the β_i does not change the other properties. Thus, we have constructed a reduced Gröbner basis B of I.

Let $\tilde{B}$ be another reduced Gröbner basis of I and $\alpha \in (B \cup \tilde{B}) \setminus (B \cap \tilde{B})$ with $\operatorname{lm} \alpha$ as small as possible. Wlog. let $\alpha \in \tilde{B} \setminus B$. Then there exist $\gamma_1, \ldots, \gamma_k \in K[X_1, \ldots, X_n]$ with

$$\operatorname{lm} \alpha = \gamma_1 \operatorname{lm} \beta_1 + \ldots + \gamma_k \operatorname{lm} \beta_k.$$

Consequently, $\operatorname{lm} \alpha$ is divisible by some $\operatorname{lm} \beta_i$. In the case $\operatorname{lm} \beta_i < \operatorname{lm} \alpha$, we would have $\beta_i \in \tilde{B}$, contradicting the reducedness of $\tilde{B}$. Thus $\operatorname{lm} \beta_i = \operatorname{lm} \alpha$, but $\beta_i \neq \alpha$ because $\alpha \notin B$. According to Theorem III.2.57, there exist $\gamma_1, \ldots, \gamma_k \in K[X_1, \ldots, X_n]$ with $\alpha - \beta_i = \beta_1 \gamma_1 + \ldots + \beta_k \gamma_k$ and $\operatorname{lm}(\beta_j \gamma_j) \leq \operatorname{lm}(\alpha - \beta_i) < \operatorname{lm} \beta_i$ for $j = 1, \ldots, k$. It follows that $\gamma_j = 0$ for $j = 1, \ldots, i$. Let $\operatorname{lm}(\beta_j \gamma_j) = \operatorname{lm}(\alpha - \beta_i)$. Then $\operatorname{lm} \beta_j$ is a divisor of a monomial in α or β_i. Since $\beta_j \in B \cap \tilde{B}$, both are excluded. This contradiction shows $B = \tilde{B}$.

As shown at the beginning, every Gröbner basis can be reduced by removing or replacing elements. Therefore, every Gröbner basis must have at least k elements. □

Example III.2.67.

(i) If the reduced Gröbner basis of an ideal I has exactly k elements, there may well be generating sets with fewer than k polynomials (Exercise III.11).

(ii) The Gröbner basis $\beta_1 = XY - Y$, $\beta_2 = X - Y^2$, $\beta_3 = Y^3 - Y$ of $I = (\beta_1, \beta_2)$ constructed in Example III.2.63 is not reduced, because XY is divisible by $\operatorname{lm} \beta_2 = X$. Euclidean division yields $\beta_1 = Y\beta_2 + \beta_3$. Therefore, β_1 can be removed and one obtains the reduced Gröbner basis β_2, β_3 of I.

(iii) For an ideal I with reduced Gröbner basis B, it holds that $I = K[X_1, \ldots, X_n]$ if and only if $B = \{1\}$ (Exercise III.12).

(iv) The reduced Gröbner basis of a maximal ideal $I \trianglelefteq K[X_1, \ldots, X_n]$ has the form $X_1 - x_1, \ldots, X_n - x_n$ with respect to the lexicographical monomial order.

(v) Let $\beta_1, \ldots, \beta_k \in K[X_1, \ldots, X_n]$ be linear polynomials. Then $\mathcal{V}(\beta_1, \ldots, \beta_k)$ is the solution set of a system of equations whose coefficient matrix A is formed from the coefficients of the β_i. The coefficients of the reduced Gröbner basis of $(\beta_1, \ldots, \beta_k)$ correspond exactly to the reduced row echelon form of A.

(vi) For $\beta_1, \ldots, \beta_k \in K[X]$, $\gcd(\beta_1, \ldots, \beta_k)$ is the reduced Gröbner basis of $(\beta_1, \ldots, \beta_k)$. The procedures described above can therefore be viewed as a common generalization of the Gaussian algorithm and the Euclidean algorithm.

Remark III.2.68. For a polynomial

$$\alpha = (X - x_1)^{a_1} \ldots (X - x_d)^{a_d} \in K[X]$$

one calls a_i, as is well known, the multiplicity of the root x_i. Furthermore, $\deg \alpha = \dim_K K[X]/(\alpha)$ is the number of all roots counted with multiplicities. This can be generalized to several unknowns. Let $I = P_1 \cap \ldots \cap P_d$ be a primary decomposition of $I \trianglelefteq R := K[X_1, \ldots, X_n]$, such that the prime ideals $\sqrt{P_1}, \ldots, \sqrt{P_d}$ are maximal. Each $\sqrt{P_i}$ then corresponds to a root $(x_1, \ldots, x_n) \in \mathcal{V}(I)$ and we call $\dim_K R/P_i$ the *multiplicity* of $(x_1, \ldots, x_n)$. If P_i is contained in a maximal ideal $M \trianglelefteq R$, then it follows that $\sqrt{P_i} \subseteq \sqrt{M} = M$ and $M = \sqrt{P_i}$. In particular, $P_i + P_j = R$ for $i \neq j$. The number of roots of I (counted with multiplicities) is therefore $\dim R/I = \dim(R/P_1) + \ldots + \dim(R/P_d)$ according to the Chinese Remainder Theorem. This number can be calculated using Gröbner bases.

Definition III.2.69. Let $\beta_1, \ldots, \beta_k$ be a Gröbner basis of $I \trianglelefteq K[X_1, \ldots, X_n]$. One calls

$$\mathcal{M} \setminus I = \mathcal{M} \setminus \operatorname{lm} I = \{\rho \in \mathcal{M} : \forall i : \beta_i \nmid \rho\}$$

the set of *standard monomials* with respect to I.

Theorem III.2.70. *Let $I \trianglelefteq R := K[X_1, \ldots, X_n]$. Then the (cosets of the) standard monomials form a K-basis of R/I. In particular, the number of standard monomials is equal to the number of zeros of I.*

Proof. Let $\beta_1, \ldots, \beta_k$ be a Gröbner basis of I. For $\alpha \in R$, let $\delta \in R$ be the (uniquely determined) remainder of the division of α by $\beta_1, \ldots, \beta_k$. Every monomial ρ in δ is not divisible by any of the $\operatorname{lm} \beta_i$. This shows $\rho \notin \operatorname{lm} I$, i. e. ρ is a standard monomial with respect to I. The (cosets of the) standard monomials therefore generate R/I. For linear independence, we assume $\sum_{i=1}^{s} \lambda_i \rho_i \in I$ with $\lambda_1, \ldots, \lambda_s \in K^\times$ and $\rho_1, \ldots, \rho_s \in \mathcal{M} \setminus I$. Wlog. let $\rho_1 > \ldots > \rho_s$. Then $\rho_1 \in \operatorname{lm} I$ would hold. □

III.3 Modular Representation Theory

Remark III.3.1. In chapter II.14 we have seen that modules over the group algebra $\mathbb{C}G$ are essentially determined by their character. Over fields K with positive characteristic, this is in general false according to Maschke, because a character cannot distinguish between semisimple and indecomposable modules with the same composition factors. In fact, the character of a representation can even be the zero map. In this chapter, we introduce some new tools and use them to determine the number of simple and indecomposable KG-modules. Unless otherwise stated, let groups be finite, algebras be finite-dimensional, and modules be finitely generated.

Lemma III.3.2. *Let $p := \operatorname{char} K > 0$ and A be a K-algebra. For $a, b \in A$ the following holds:*

(i) $(a+b)^p \equiv a^p + b^p \pmod{\gamma(A)}$.

(ii) $a \in \gamma(A) \Longrightarrow a^p \in \gamma(A)$.

(iii) $\mathrm{J}(A) + \gamma(A) = \{a \in A : \exists n \in \mathbb{N} : a^{p^n} \in \gamma(A)\}$, *if K is algebraically closed.*

Proof.

(i) If one multiplies out $(a+b)^p$, one obtains the sum of all 2^p terms of the form $c_1 \dots c_p$ with $c_1, \dots, c_p \in \{a, b\}$.[1] Because of

$$c_1 \dots c_p \equiv c_2 \dots c_p c_1 \equiv \dots \equiv c_p c_1 \dots c_{p-1} \pmod{\gamma(A)}$$

it holds that

$$c_1 \dots c_p + c_2 \dots c_p c_1 + \dots + c_p c_1 \dots c_{p-1} \equiv p c_1 \dots c_p \equiv 0 \pmod{\gamma(A)}.$$

Modulo $\gamma(A)$, only the two terms a^p and b^p remain in $(a+b)^p$.

(ii) According to (i), we can assume $a = bc - cb$ with $c \in A$. Then it holds that

$$a^p \equiv (bc)^p - (cb)^p \equiv bc \dots bc - cb \dots cb \equiv 0 \pmod{\gamma(A)}.$$

(iii) According to (i) and (ii), $T := \{a \in A : \exists n \in \mathbb{N} : a^{p^n} \in \gamma(A)\}$ is a vector space. Since $\mathrm{J}(A)$ is nilpotent, $\mathrm{J}(A) \subseteq T$ holds. From (ii) it follows that $\gamma(A) \subseteq T$, thus $\mathrm{J}(A) + \gamma(A) \subseteq T$. According to Artin-Wedderburn and Lemma II.12.6, $A/\mathrm{J}(A) \cong K^{n_1 \times n_1} \times \dots \times K^{n_k \times n_k}$ holds. Together with Lemma II.12.34, this yields

$$(\gamma(A) + \mathrm{J}(A))/\mathrm{J}(A) = \gamma(A/\mathrm{J}(A)) \cong \gamma(K^{n_1 \times n_1}) \times \dots \times \gamma(K^{n_k \times n_k}) \tag{III.3.1}$$

and $\dim A/(\gamma(A) + \mathrm{J}(A)) = k$. On the other hand, the idempotents

$$(E_{11}, 0, \dots, 0), \dots, (0, \dots, 0, E_{11}) \in K^{n_1 \times n_1} \times \dots \times K^{n_k \times n_k}$$

are obviously linearly independent modulo T. This shows $\dim A/T \geq k$ and $T \subseteq \gamma(A) + \mathrm{J}(A)$. □

[1] Since a and b are not necessarily commutable, one may not use the binomial formula.

Corollary III.3.3. *Let K be algebraically closed with characteristic $p > 0$ and A a K-algebra. Then* $\dim R(A) = \dim \mathrm{Z}(A/\mathrm{J}(A))$ *is the number of simple A-modules (up to isomorphism).*

Proof. It holds that $\dim R(A) = \dim(\gamma(A) + \mathrm{J}(A))^{\perp} = \dim A/(\gamma(A) + \mathrm{J}(A))$. Therefore, the claim follows from (III.3.1) in the above proof. □

Definition III.3.4. Let $p \in \mathbb{P}$. One calls $x \in G$ a *p'-element*, if $p \nmid |\langle x \rangle|$. Let G_p (resp. $G_{p'}$) be the set of p-elements (resp. p'-elements) of G. Then $G_p \cap G_{p'} = \{1\}$ holds, but $G \neq G_p \cup G_{p'}$ in general. One calls $C \in \mathrm{Cl}(G)$ a *p-conjugacy class* (resp. *p'-conjugacy class*), if $C \subseteq G_p$ (resp. $C \subseteq G_{p'}$) (note: conjugate elements have the same order).

Lemma III.3.5. *Every element $x \in G$ can be uniquely written in the form $x = x_p x_{p'} = x_{p'} x_p$ with $x_p \in G_p$ and $x_{p'} \in G_{p'}$. One calls x_p the* p-factor *and $x_{p'}$ the* p'-factor *of x.*

Proof. Let $|\langle x \rangle| = p^a m$ with $p \nmid m$. Then there exist $\alpha, \beta \in \mathbb{Z}$ with $\alpha p^a + \beta m = \gcd(p^a, m) = 1$. For $x_p := x^{\beta m} \in G_p$ and $x_{p'} := x^{\alpha p^a} \in G_{p'}$ it holds that $x = x^{\alpha p^a + \beta m} = x_p x_{p'} = x_{p'} x_p$.

Let $y \in G_p$ and $z \in G_{p'}$ with $x = yz = zy$. Then y and z commute with x, x_p and $x_{p'}$. It follows that $y^{-1} x_p = z x_{p'}^{-1} \in G_p \cap G_{p'} = \{1\}$, i. e. $y = x_p$ and $z = x_{p'}$. □

Remark III.3.6. For $x, g \in G$ it holds that $(gxg^{-1})_p = g x_p g^{-1}$ and $(gxg^{-1})_{p'} = g x_{p'} g^{-1}$.

Definition III.3.7. For $x \in G$ let

$$\mathrm{Sec}_{p'}(x) := \{y \in G : \exists g \in G : y_{p'} = g x_{p'} g^{-1}\} \subseteq G$$

be the *p'-section* of x. According to Remark III.3.6, $\mathrm{Sec}_{p'}(x)$ is a union of conjugacy classes of G. Let $\mathrm{Sec}_{p'}(G) := \{\mathrm{Sec}_{p'}(x) : x \in G\}$.

Theorem III.3.8 (Brauer-Tsushima)**.** *For every algebraically closed field K of characteristic $p > 0$ it holds that*

(i) $$\gamma(KG) = \Big\{\sum_{g \in G} \alpha_g g : \forall C \in \mathrm{Cl}(G) : \sum_{c \in C} \alpha_c = 0\Big\},$$

(ii) $$\gamma(KG) + \mathrm{J}(KG) = \Big\{\sum_{g \in G} \alpha_g g : \forall S \in \mathrm{Sec}_{p'}(G) : \sum_{s \in S} \alpha_s = 0\Big\},$$

(iii) $$\mathrm{J}(KG) = \Big\{\sum_{g \in G} \alpha_g g : \forall g \in G, S \in \mathrm{Sec}_{p'}(G) : \sum_{s \in S} \alpha_{gs} = 0\Big\},$$

(iv) $$\Gamma(KG) = \mathrm{Span}_K\{C^+ : C \in \mathrm{Cl}(G) : |C|_p = |G|_p\},$$

(v) $$R(KG) = \mathrm{Span}_K\{S^+ : S \in \mathrm{Sec}_{p'}(G)\}.$$

Proof.

(i) Let Γ be the right side of the equation. For $g, h \in G$, it holds that $gh - hg = gh - g^{-1}(gh)g \in \Gamma$. From this, $\gamma(KG) \subseteq \Gamma$ follows. Conversely, let $\sum_{g \in G} \alpha_g g \in \Gamma$ and $x_C \in C \in \mathrm{Cl}(G)$. For every $c \in C$, there exists $g \in G$ with $c = g x_C g^{-1}$. Then $c - x_C = (g x_C) g^{-1} - g^{-1}(g x_C) \in \gamma(KG)$ and

$$\sum_{g \in G} \alpha_g g = \sum_{C \in \mathrm{Cl}(G)} \sum_{c \in C} \alpha_c (c - x_C) \in \gamma(KG).$$

(ii) Let $|G| = p^a m$ with $p \nmid m$ and $k \geq a$ with $p^k \equiv 1 \pmod{m}$ (e. g. $k = a\varphi(m)$). Then $g^{p^k} = g_p^{p^k} g_{p'}^{p^k} = g_{p'}$ for $g \in G$ by Lagrange. Let $\alpha := \sum_{g \in G} \alpha_g g \in KG$ and $x_1, \ldots, x_l$ be a system of representatives for the p'-conjugacy classes of G. For $g \in \mathrm{Sec}_{p'}(x_i)$, it holds that $g_{p'} \equiv x_i \pmod{\gamma(KG)}$ by (i). From Lemma III.3.2 it follows that

$$\alpha^{p^k} \equiv \sum_{g \in G} \alpha_g^{p^k} g_{p'} \equiv \sum_{i=1}^{l} x_i \sum_{s \in \mathrm{Sec}_{p'}(x_i)} \alpha_s^{p^k} \equiv \sum_{i=1}^{l} x_i \Big(\sum_{s \in \mathrm{Sec}_{p'}(x_i)} \alpha_s \Big)^{p^k} \pmod{\gamma(KG)}. \tag{III.3.2}$$

If $\sum_{s \in \mathrm{Sec}_{p'}(x_i)} \alpha_s = 0$ for all i, then $\alpha^{p^k} \in \gamma(KG)$ and $\alpha \in \gamma(KG) + \mathrm{J}(KG)$ by (III.3.2). Conversely, if $\alpha^{p^n} \in \gamma(KG)$ for some $n \in \mathbb{N}$, then there exists a $k \geq \max\{a, n\}$ with $k \equiv 1 \pmod{m}$. Then $\sum_{s \in \mathrm{Sec}_{p'}(x_i)} \alpha_s = 0$ follows from (III.3.2) for $i = 1, \ldots, l$.

(iii) According to Remark II.13.20, KG is symmetric with respect to $\beta\big(\sum \alpha_g g, \sum \beta_g g\big) = \sum_{g \in G} \alpha_g \beta_{g^{-1}}$. Because $\mathrm{Sec}_{p'}(x)^{-1} = \mathrm{Sec}_{p'}(x^{-1})$ for $x \in G$, the map $S \mapsto S^{-1}$ is a bijection on $\mathrm{Sec}_{p'}(G)$. For $\alpha := \sum \alpha_g g \in KG$, it therefore holds that

$$\begin{aligned} \alpha \in \gamma(KG) + \mathrm{J}(KG) &\overset{(ii)}{\iff} \forall S \in \mathrm{Sec}_{p'}(G) : \beta(S^+, \alpha) = \sum_{s \in S^{-1}} \alpha_s = 0 \\ &\iff \alpha \in \{S^+ : S \in \mathrm{Sec}_{p'}(G)\}^\perp. \end{aligned} \tag{III.3.3}$$

From Theorem II.13.17 it follows that

$$\begin{aligned} \alpha \in \mathrm{J}(KG) &\iff \forall S \in \mathrm{Sec}_{p'}(G) : \sum_{g \in G} \sum_{s \in S} \alpha_g gs = \alpha S^+ = 0 \\ &\iff \forall g \in G, S \in \mathrm{Sec}_{p'}(G) : \sum_{s \in S} \alpha_{gs^{-1}} = 0. \end{aligned}$$

(iv) As is well known, $(g)_{g \in G}$ and $(g^{-1})_{g \in G}$ are dual bases of KG to each other. For $x \in G$, it holds that

$$\Gamma(x) = \sum_{g \in G} gxg^{-1} = |\mathrm{C}_G(x)| \mathrm{Cl}(x)^+.$$

If $|\mathrm{C}_G(x)| = |G|/|C|$ is divisible by p, then $\Gamma(x) = 0$ follows. Thus $\Gamma(KG)$ is spanned by all conjugacy classes C with $|C|_p = |G|_p$.

(v) Follows from (III.3.3). □

Remark III.3.9. The characterizations of $\gamma(KG)$ and $\gamma(KG) + \mathrm{J}(KG)$ in Theorem III.3.8 consist of linearly independent linear equations. In particular, $\dim \gamma(KG) = |G| - k(G) = \dim \mathrm{Z}(KG)^\perp$ in accordance with Theorem II.13.17. The description of $\mathrm{J}(KG)$, however, consists of linearly dependent equations and therefore does not allow for a direct conclusion about $\dim \mathrm{J}(KG)$.

Theorem III.3.10 (Brauer)**.** *Let K be an algebraically closed field of characteristic $p > 0$. Then the number of simple KG-modules coincides with the number of p'-conjugacy classes of G.*

Proof. Apparently, the number l of p'-conjugacy classes coincides with the number of p'-sections. According to Theorem III.3.8, $\dim R(KG) = l$ and the assertion follows from Corollary III.3.3. □

Example III.3.11.

(i) If G is a p'-group, then $\mathrm{Sec}_{p'}(1) = \{1\}$ and $\mathrm{J}(KG) = 0$ in accordance with Maschke. Furthermore, $\mathrm{Sec}_{p'}(G) = \mathrm{Cl}(G)$ and $\Gamma(KG) = R(KG) = \mathrm{Z}(KG)$.

(ii) If G is a p-group, then $\mathrm{Sec}_{p'}(G) = \{G\}$ and

$$\gamma(KG) + \mathrm{J}(KG) = \mathrm{J}(KG) = I(KG)$$

is the augmentation ideal. Furthermore, $\Gamma(KG) = 0$ and $R(KG) = KG^+$.

(iii) Suppose G possesses a normal Sylow p-subgroup $P \trianglelefteq G$. Let $A := KG$. Then $\mathrm{Sec}_{p'}(1) = P^+$. For $\alpha = \sum_{g\in G} \alpha_g g \in \mathrm{J}(A)$, it thus holds that $\sum_{x\in gP} \alpha_x = 0$ for all $gP \in G/P$. This shows

$$\mathrm{J}(A) \subseteq I(KP)A = \mathrm{J}(KP)A$$

according to (ii). According to Exercise II.62, $\mathrm{J}(KP)A = A\,\mathrm{J}(KP)$ is the kernel of the canonical epimorphism $A \to K[G/P]$. Consequently, $(\mathrm{J}(KP)A)^n = \mathrm{J}(KP)^n A$ holds. Like $\mathrm{J}(KP)$, $\mathrm{J}(KP)A$ is also nilpotent. We obtain $\mathrm{J}(A) = \mathrm{J}(KP)A$ and $\dim \mathrm{J}(A) = |G| - |G : P|$. Indeed, $A/\mathrm{J}(A) \cong K[G/P]$ is semisimple according to Maschke. According to the Schur-Zassenhaus Theorem from group theory[2], there exists a subgroup $H \leq G$ with $|H| = |G : P|$. In particular, KH is semisimple and $A = KH \oplus \mathrm{J}(A)$ is the decomposition from Wedderburn-Malcev.

(iv) For $A := KG = \overline{\mathbb{F}}_2 S_3$, we have

$$\mathrm{Sec}_{2'}(1) = \{1, (1,2), (1,3), (2,3)\},$$
$$\mathrm{Sec}_{2'}((1,2,3)) = \{(1,2,3), (1,3,2)\}.$$

Because of $1 + (1,2) \in (\gamma(A) + \mathrm{J}(A)) \setminus \mathrm{J}(A)$, it follows that

$$\dim \mathrm{J}(A) < \dim(\gamma(A) + \mathrm{J}(A)) = 4$$

from Theorem III.3.8. On the other hand, according to Corollary III.3.3, $A/\mathrm{J}(A) \cong K \times K^{n\times n}$ for some $n \in \mathbb{N}$. Thus $n = 2$ and $\dim \mathrm{J}(A) = 1$. Because of $|gS| = |S| \equiv 0 \pmod 2$, we have $\mathrm{J}(A) = KG^+$. Furthermore, $\Gamma(A) = K((1,2,3) + (1,3,2)) \subsetneq R(A) \subsetneq \mathrm{Z}(A)$. Apparently, $e := (1,2,3) + (1,3,2)$ is a central idempotent of A and

$$B := Ae = \langle e,\ 1 + (1,2,3),\ (1,2) + (1,3),\ (1,2) + (2,3)\rangle$$

has dimension 4. Thus one obtains the Wedderburn-Malcev decomposition $A = K \oplus B \oplus \mathrm{J}(A)$.

Remark III.3.12.

(i) Let K be an arbitrary field and

$$(n, S) := \begin{cases} (|G|, G) & \text{if } \operatorname{char} K = 0, \\ (|G|_{p'}, G_{p'}) & \text{if } \operatorname{char} K = p. \end{cases}$$

Let $\zeta \in \overline{K}$ be a primitive n-th root of unity and

$$Z := \{a + n\mathbb{Z} : \exists \gamma \in \mathrm{Gal}(K(\zeta)|K) : \gamma(\zeta) = \zeta^a\} \leq (\mathbb{Z}/n\mathbb{Z})^\times.$$

By

$$x \sim y :\Longleftrightarrow \exists g \in G, a + n\mathbb{Z} \in Z : gxg^{-1} = y^a \qquad (x, y \in S)$$

one obtains an equivalence relation on S. According to a theorem of Berman the number of simple KG-modules is equal to the number of equivalence classes of $\sim$ on S.

[2]See lecture notes group theory.

(ii) The explicit determination of the simple modules is significantly more difficult in positive characteristic than in characteristic 0. For example, one does not even know the dimensions of the simple $\mathbb{F}_2 S_{20}$-modules.

Example III.3.13.

(i) If K is algebraically closed, then $\zeta \in K$ and $A = 1$ in Remark III.3.12. Thus one recovers Brauer's theorem (respectively Remark II.13.26).

(ii) For $K = \mathbb{Q}$ we have $A = (\mathbb{Z}/n\mathbb{Z})^\times$ and $x \sim y \iff \langle x \rangle = \langle y \rangle$. The number of simple $\mathbb{Q}G$-modules is therefore the number of conjugacy classes of cyclic subgroups of G.

(iii) For $K = \mathbb{R}$ we have $A = \langle -1 + n\mathbb{Z} \rangle$. Let r be the number of conjugacy classes $C = C^{-1}$ and $2s$ the number of conjugacy classes $C \neq C^{-1}$. Then $r + s$ is the number of simple $\mathbb{R}G$-modules. If $|G|$ is odd, then $r = 1$ and there are exactly $(k(G) + 1)/2$ simple $\mathbb{R}G$-modules.

Theorem III.3.14. *For every field K of characteristic $p > 0$ the following holds:*

(i) KG is local if and only if G is a p-group.

(ii) If $G \cong C_{p^n}$, then KG has exactly p^n indecomposable KG-modules up to isomorphism. These have the dimensions $1, 2, \ldots, p^n$.

(iii) If G is a non-cyclic p-group, then KG has indecomposable modules in every dimension $d \in \mathbb{N}$.

Proof.

(i) Let us first assume that G is not a p-group. By Cauchy, there exists a subgroup $1 \neq H \leq G$ with $|H| \not\equiv 0 \pmod{p}$, i. e. $|H|^{-1} \in K$. It is easy to see that $\frac{1}{|H|} \sum_{x \in H} x \in KG \setminus \{0, 1\}$ is an idempotent. According to Theorem II.12.11, KG is not local.

Now let G be a p-group. As is well known, K contains the prime field $\mathbb{F}_p$. Let M be a simple KG-module and

$$L := \sum_{g \in G} \mathbb{F}_p gm \subseteq M$$

for a fixed $m \in M \setminus \{0\}$. Obviously, L is a finite $\mathbb{F}_p$-vector space. In particular, $|L|$ is a power of p. For $x \in G$, we have $xL = \sum_{g \in G} \mathbb{F}_p xgm = L$. Therefore, G acts on L by left multiplication. Certainly $0 \in L$ is a fixed point of G. Since both $|G|$ and $|L|$ are powers of p, G must have another fixed point $a \in L \setminus \{0\}$ by the class equation. Now Ka is a submodule of the simple module M and it follows that $M = Ka \simeq K$. According to Remark II.13.24, KG is local.

(ii) Let $G = \langle g \rangle$ and V be an indecomposable KG-module. The minimal polynomial μ of the linear map $f \colon V \to V$, $v \mapsto gv$ divides $X^{p^n} - 1 = (X-1)^{p^n}$. Thus $\mu = (X-1)^k$ for some $1 \leq k \leq p^n$. By linear algebra, there exists an f-invariant decomposition $V = U \oplus W$ such that $f_{|U}$ corresponds to the Jordan block $J_k(1)$ (the proof uses induction on k and also works for $\dim V = \infty$).[3] Since V is indecomposable, $W = 0$ and $\dim V = \dim U = k$. Furthermore, V is uniquely determined up to isomorphism. Conversely, for each $1 \leq k \leq p^n$, one can transform the vector space $V := K^k$ into a KG-module by $gv := J_k(1)v$ for $v \in V$. Due to the uniqueness of the Jordan normal form, V is indecomposable.

[3] See lecture notes linear algebra.

(iii) By Sylow, G has a subgroup H with index p. By Exercise I.25, $H \trianglelefteq G$. Let $x \in G \setminus H$. Since G is not cyclic, x lies in a maximal subgroup $L \neq H$. We show $|G : L| = p$ by induction on $|G|$. This is clear for $|G| = p^2$. By Theorem I.4.11, $Z := \mathrm{Z}(G) \neq 1$. In the case $Z \leq L$, L/Z is maximal in G/Z by the correspondence theorem. Induction shows $|G : L| = |G/Z : L/Z| = p$. So let $Z \nleq L$. Then $G = LZ$ since L is maximal. From $L, Z \subseteq \mathrm{N}_G(L)$ it follows that $L \trianglelefteq G$. Now G/L is a simple p-group, so $|G : L| = p$ by Example I.6.3.

By Exercise I.25, $L \trianglelefteq G$ also holds and $N := H \cap L \trianglelefteq G$. We have

$$G/N = H/N \oplus L/N \cong C_p^2.$$

If U is an indecomposable $K[G/N]$-module, then U becomes an indecomposable KG-module via $gu := (gN)u$ for $g \in G$ and $u \in U$. We can therefore assume $G = \langle g, h \rangle \cong C_p^2$.

We first construct indecomposable modules in dimension $2d$. Let V_{2d} be the K-vector space with basis $b_1, \ldots, b_d, c_1, \ldots, c_d$. Let $\alpha, \beta \in \mathrm{End}(V_{2d})$ with

$$\alpha(b_i) = c_i, \quad \beta(b_j) = c_{j+1}, \quad \alpha(c_i) = \beta(c_i) = \beta(b_d) = 0 \quad (i = 1, \ldots, d,\ j = 1, \ldots, d-1).$$

Obviously $\alpha^2 = \beta^2 = \alpha\beta = \beta\alpha = 0$ holds. It follows that $(\mathrm{id} + \alpha)^p = \mathrm{id} + \alpha^p = \mathrm{id} = (\mathrm{id} + \beta)^p$. Therefore $\Delta\colon G \to \mathrm{GL}(V_{2d})$ with $\Delta(g) = \mathrm{id} + \alpha$ and $\Delta(h) = \mathrm{id} + \beta$ defines a representation. Let $f \in \mathrm{End}_{KG}(V_{2d})$ with matrix $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in K^{2d \times 2d}$ with respect to the given basis. Let $J = J_d(0) \in K^{d \times d}$. Because $f(gv) = gf(v)$ for $v \in V_{2d}$, f commutes with α and β, i. e.

$$\begin{pmatrix} 0 & 0 \\ A & B \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1_n & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \alpha M = M\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1_n & 0 \end{pmatrix} = \begin{pmatrix} B & 0 \\ D & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 \\ JA & JB \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ J & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \beta M = M\beta = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 0 & 0 \\ J & 0 \end{pmatrix} = \begin{pmatrix} BJ & 0 \\ DJ & 0 \end{pmatrix}.$$

It follows that $A = D$, $B = 0$ and $AJ = JA$. In particular, M is a lower triangular matrix. With $A = (a_{ij})$, specifically

$$\begin{pmatrix} a_{12} & \cdots & a_{1,n-1} & 0 \\ \vdots & & \vdots & \vdots \\ a_{n2} & \cdots & a_{n,n-1} & 0 \end{pmatrix} = AJ = JA = \begin{pmatrix} 0 & \cdots & 0 \\ a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n} \end{pmatrix}.$$

It follows that $a_{11} = \ldots = a_{nn}$. In the case $a_{11} \neq 0$, f is invertible and otherwise f is nilpotent. Thus $\mathrm{End}_{KG}(V_{2d})$ is local and V_{2d} is indecomposable by Remark II.12.12.

For odd dimension $2d + 1$, we extend V_{2d} to $V_{2d+1} := V_{2d} \oplus Kc_{d+1}$ and set

$$\alpha(b_i) = c_i, \qquad \beta(b_i) = c_{i+1}, \qquad \alpha(c_j) = \beta(c_j) = 0 \qquad (i = 1, \ldots, d,\ j = 1, \ldots, d+1)$$

(since the trivial module is indecomposable, we can assume $d \geq 1$). A similar calculation shows $M = \left(\begin{smallmatrix} A & 0 \\ C & D \end{smallmatrix}\right)$ with $A \in K^{d \times d}$, $C \in K^{(d+1) \times d}$ and

$$D = \begin{pmatrix} A & * \\ 0 & * \end{pmatrix} = \begin{pmatrix} * & 0 \\ * & A \end{pmatrix} = \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ * & & a_{11} \end{pmatrix} \in K^{(d+1) \times (d+1)}.$$

Thus V_{2d+1} is also indecomposable. □

Remark III.3.15.

(i) If an algebra A has only finitely many indecomposable modules up to isomorphism, one says: A has finite *representation type*. The *Brauer-Thrall conjecture* proven by ROITER states that an algebra of infinite representation type has indecomposable modules with arbitrarily large dimension. If K is algebraically closed, there are, if applicable, infinitely many $d \in \mathbb{N}$ with infinitely many non-isomorphic indecomposable modules in dimension d (second Brauer-Thrall conjecture; cf. Exercise III.16).

(ii) For $\operatorname{char} K = p$ and $G = \langle g \rangle \cong C_{p^n}$, $KG \to K[X]/(X^{p^n})$, $g \mapsto 1 + X + (X^{p^n})$ is an isomorphism of algebras (cf. Exercise II.66). Analogously, $KC_p^2 \cong K[X,Y]/(X^p, Y^p)$ holds.

Definition III.3.16.

(i) For K-vector spaces V and W with bases $b_1, \ldots, b_n$ and $c_1, \ldots, c_m$, let $V \otimes W$ be a K-vector space with basis $\{b_i \otimes c_j : i = 1, \ldots, n,\ j = 1, \ldots, m\}$. One calls $V \otimes W$ the *tensor product* of V and W. For $v = \sum_{i=1}^n \lambda_i b_i$ and $w = \sum_{j=1}^m \mu_j c_j$, one defines $v \otimes w := \sum_{i,j} \lambda_i \mu_j (b_i \otimes c_j)$.

(ii) Now let V and W additionally be KG-modules. For $g \in G$, $\gamma_g(b_i \otimes c_j) := gb_i \otimes gc_j$ defines a linear map on $V \otimes W$. For $v = \sum_{i=1}^n \lambda_i b_i$ and $w = \sum_{j=1}^m \mu_j c_j$, it holds that

$$\gamma_g(v \otimes w) = \gamma_g\Big(\sum_{i,j} \lambda_i \mu_j (b_i \otimes c_j)\Big) = \sum_{i,j} \lambda_i \mu_j (gb_i \otimes gc_j) = gv \otimes gw.$$

Therefore, $\Delta\colon G \to \mathrm{GL}(V \otimes W)$, $g \mapsto \gamma_g$ is a representation and $V \otimes W$ becomes a KG-module via $g(v \otimes w) := gv \otimes gw$.

Remark III.3.17.

(i) Tensor products of modules of arbitrary algebras and rings are significantly more complex to define (see Exercise II.53 and Definition III.6.14).

(ii) For KG-modules U, V, W one easily shows that the following canonical maps are isomorphisms:

- $K \otimes V \simeq V$.
- $V \otimes W \simeq W \otimes V$.
- $U \otimes (V \otimes W) \simeq (U \otimes V) \otimes W$.
- $U \otimes (V \times W) \simeq (U \otimes V) \times (U \otimes W)$.

(iii) Let $\Delta\colon G \to \mathrm{GL}(n, K)$ and $\Gamma\colon G \to \mathrm{GL}(m, K)$ be the representations of V and W with respect to the bases $b_1, \ldots, b_n$ and $c_1, \ldots, c_m$, respectively. Let $g \in G$ and $\Delta(g) = (a_{ij}) \in K^{n \times n}$, i. e. $gb_i = \sum_{j=1}^n a_{ji} b_j$. Then the representation $\Delta \otimes \Gamma$ belonging to $V \otimes W$ with respect to $b_1 \otimes c_1, b_1 \otimes c_2, \ldots, b_n \otimes c_m$ is given by

$$(\Delta \otimes \Gamma)(g) = \Delta(g) \otimes \Gamma(g) := \begin{pmatrix} a_{11}\Gamma(g) & \cdots & a_{1n}\Gamma(g) \\ \vdots & & \vdots \\ a_{na}\Gamma(g) & \cdots & a_{nn}\Gamma(g) \end{pmatrix} \in K^{nm \times nm}$$

(Kronecker product).

(iv) Now let $K = \mathbb{C}$. For the character of $\Delta \otimes \Gamma$ it then holds that

$$\chi_{\Delta\otimes\Gamma}(g) = a_{11} \operatorname{tr} \Gamma(g) + \ldots + a_{nn} \operatorname{tr} \Gamma(g) = \chi_\Delta(g)\chi_\Gamma(g)$$

for $g \in G$ (cf. Theorem II.14.38).

Theorem III.3.18 (Universal property of the tensor product)**.** *Let U, V and W be KG-modules and $f\colon V \times W \to U$ a bilinear map with $gf(v,w) = f(gv,gw)$ for all $g \in G$, $v \in V$ and $w \in W$. Then there exists exactly one homomorphism $\hat{f}\colon V \otimes W \to U$ with $\hat{f}(v \otimes w) = f(v,w)$ for all $v \in V$ and $w \in W$.*

Proof. Let $b_1, \ldots, b_n$ and $c_1, \ldots, c_m$ be bases of V and W, respectively. We define $\hat{f}(b_i \otimes c_j) := f(b_i, c_j)$ and extend linearly. Then $\hat{f}(v \otimes w) = f(v,w)$ holds for all $v \in V$ and $w \in W$. For $g \in G$ it holds that

$$\hat{f}\big(g(v \otimes w)\big) = \hat{f}(gv \otimes gw) = f(gv,gw) = gf(v,w) = g\hat{f}(v \otimes w),$$

i. e. $\hat{f}$ is a homomorphism of KG-modules. Since $V \otimes W$ is generated by $b_i \otimes c_j$, $\hat{f}$ is uniquely determined. □

Lemma III.3.19. *For KG-modules U, V, W with $U \leq V$ it holds that $W \otimes (V/U) \simeq (W \otimes V)/(W \otimes U)$.*

Proof. The bilinear map $f\colon W \times V \to W \otimes (V/U)$, $(w,v) \mapsto w \otimes (v+U)$ satisfies $gf(w,v) = gw \otimes g(v+U) = f(gw,gv)$. Therefore there exists an epimorphism $\hat{f}\colon W \otimes V \to W \otimes (V/U)$, $w \otimes v \mapsto w \otimes (v+U)$ with $W \otimes U \leq \operatorname{Ker}(\hat{f})$. Because of $\dim(W \otimes (V/U)) = \dim W \dim(V/U) = \dim W \dim V - \dim W \dim U$ it holds that $\operatorname{Ker}(\hat{f}) = W \otimes U$. □

Remark III.3.20.

(i) Let V and W be KG-modules. For $g \in G$, $\varphi \in \operatorname{Hom}_K(V,W)$ and $v \in V$ we define

$$\gamma_g(\varphi)(v) := g\varphi(g^{-1}v)$$

as in the proof of Theorem II.14.38. For $g, h \in G$ it holds that

$$\gamma_{gh}(\varphi)(v) = gh\varphi(h^{-1}g^{-1}v) = g\gamma_h(\varphi)(g^{-1}v) = \gamma_g(\gamma_h(\varphi))(v).$$

Therefore $\Delta\colon G \to \mathrm{GL}(\operatorname{Hom}_K(V,W))$, $g \mapsto \gamma_g$ is a representation and $\operatorname{Hom}_K(V,W)$ becomes a KG-module of dimension $\dim(V)\dim(W)$ via $(g\varphi)(v) := g\varphi(g^{-1}v)$.

(ii) If one chooses the trivial module $W = K$, one obtains the *dual space* $V^* := \operatorname{Hom}_K(V,K)$ with $(g\varphi)(v) = \varphi(g^{-1}v)$ for $g \in G$, $\varphi \in V^*$ and $v \in V$. One then speaks of the *dual* module to V. In the case $V \simeq V^*$, V is called *self-dual*.

(iii) For submodules $U \leq V$ and $W \leq V^*$ let

$$U^\perp := \{\varphi \in V^* : \varphi(U) = 0\}, \qquad W_\perp := \{v \in V : \forall \varphi \in W : \varphi(w) = 0\}.^4$$

For $g \in G$, $\varphi \in U^\perp$, $\psi \in W_\perp$ and $v \in W_\perp$ it holds that $(g\varphi)(U) = \varphi(g^{-1}U) = \varphi(U) = 0$ and $\psi(gv) = g^{-1}\psi(v) = 0$. This shows that $U^\perp$ and $W_\perp$ are submodules of V^* and V respectively. According to linear algebra,

$$\dim U + \dim U^\perp = \dim V = \dim V^* = \dim W + \dim W_\perp.$$

By definition $U \subseteq (U^\perp)_\perp$ and $W \subseteq (W_\perp)^\perp$. For dimension reasons $U = (U^\perp)_\perp$ and $W = (W_\perp)^\perp$ hold. By restriction one also obtains $\boxed{V^*/U^\perp \simeq U^*.}$

[4] The bilinear form $V \times V^* \to K$, $(v,\varphi) \mapsto \varphi(v)$ explains the use of the symbol $\perp$. These orthogonal spaces should be distinguished from those defined for symmetric algebras in Remark II.13.16.

(iv) According to linear algebra, the map $\Phi\colon V \to V^{**}$, $v \mapsto \Phi_v$ with $\Phi_v(\varphi) = \varphi(v)$ is a vector space isomorphism. For $g \in G$, $v \in V$ and $\varphi \in V^*$ it holds that

$$\Phi(gv)(\varphi) = \varphi(gv) = (g^{-1}\varphi)(v) = \Phi(v)(g^{-1}\varphi) = (g\Phi(v))(\varphi).$$

This shows that Φ is also an isomorphism of KG-modules. For $v \in V$ and $W \leq V^*$ it holds that

$$v \in W_\perp \iff \forall \varphi \in W : \varphi(v) = 0 \iff \forall \varphi \in W : \Phi_v(\varphi) = 0 \iff \Phi_v \in W^\perp.$$

Therefore $\Phi(W_\perp) = W^\perp$. From (iii) one obtains $\boxed{V/W_\perp \simeq V^{**}/W^\perp \simeq W^*.}$

(v) If $f\colon V \to W$ is a homomorphism of KG-modules, then so is the *dual* map $f^*\colon W^* \to V^*$, $\varphi \mapsto \varphi \circ f$, because

$$f^*(g\varphi)(v) = (g\varphi)(f(v)) = \varphi(g^{-1}f(v)) = \varphi(f(g^{-1}v)) = f^*(\varphi)(g^{-1}v) = (g(f^*(\varphi)))(v)$$

for $g \in G$, $\varphi \in W^*$ and $v \in V$. In particular, it holds that

$$V \simeq W \Longrightarrow V^* \simeq W^* \Longrightarrow V \simeq V^{**} \simeq W^{**} \simeq W.$$

Let $\Phi\colon V \to V^{**}$ and $\Psi\colon W \to W^{**}$ be the isomorphisms from (iv). For $\varphi \in W^*$ and $v \in V$ it holds that $(\Phi(v) \circ f^*)(\varphi) = \Phi(v)(\varphi \circ f) = \varphi(f(v))$ and

$$(\Psi^{-1} \circ f^{**} \circ \Phi)(v) = \Psi^{-1}(\Phi(v) \circ f^*) = f(v).$$

Therefore $\mathrm{Hom}_{KG}(V, W) \to \mathrm{Hom}_{KG}(W^*, V^*)$, $f \mapsto f^*$ is a vector space isomorphism.

(vi) Let $\Delta\colon G \to \mathrm{GL}(n, K)$ be a representation associated to V with respect to a basis $b_1, \ldots, b_n$. Let $g \in G$ and $g^{-1}b_i = \sum_{j=1}^n a_{ji}b_j$. Let $\beta_1, \ldots, \beta_n$ be the corresponding dual basis of V^*, i. e. $\beta_i(b_j) = \delta_{ij}$ for $1 \leq i, j \leq n$. Then it follows that $(g\beta_i)(b_j) = \beta_i(g^{-1}b_j) = a_{ij}$ and $g\beta_i = \sum_{j=1}^n a_{ij}\beta_j$. For the representation $\Delta^*\colon G \to \mathrm{GL}(n, K)$ belonging to V^* with respect to $\beta_1, \ldots, \beta_n$, it thus holds that $\Delta^*(g) = \Delta(g^{-1})^{\mathrm{t}}$ for $g \in G$ (cf. Example II.14.4). In the case $K = \mathbb{C}$, it is well known that for the character $\chi_{\Delta^*} = \overline{\chi_\Delta}$ holds. In particular, V is self-dual if and only if χ_Δ is real.

Lemma III.3.21. *For KG-modules U, V, W, the following holds:*

(i) $(V \times W)^* \simeq V^* \times W^*$ *and* $(V \otimes W)^* \simeq V^* \otimes W^*$.

(ii) $\mathrm{Hom}_K(V, W) \simeq V^* \otimes W$.

(iii) $\mathrm{Hom}_K(U \otimes V, W) \simeq \mathrm{Hom}_K(U, \mathrm{Hom}_K(V, W))$.

Proof.

(i) The map $(V \times W)^* \to V^* \times W^*$, $\varphi \mapsto (\varphi_{|V}, \varphi_{|W})$ is clearly a monomorphism of KG-modules. For dimension reasons, it is an isomorphism. Let $\varphi \in V^*$ and $\psi \in W^*$. By the universal property for tensor products of vector spaces, there exists $f_{\varphi,\psi} \in (V \otimes W)^*$ with $f_{\varphi,\psi}(v \otimes w) := \varphi(v)\psi(w)$. The bilinear map $f\colon V^* \times W^* \to (V \otimes W)^*$, $(\varphi, \psi) \mapsto f_{\varphi,\psi}$ satisfies

$$\begin{aligned} f(g\varphi, g\psi)(v \otimes w) = f_{g\varphi,g\psi}(v \otimes w) &= (g\varphi)(v)(g\psi)(w) = \varphi(g^{-1}v)\psi(g^{-1}w) \\ &= f_{\varphi,\psi}(g^{-1}(v \otimes w)) = (gf(\varphi, \psi))(v \otimes w). \end{aligned}$$

From the universal property, one obtains a homomorphism

$$\hat{f}\colon V^* \otimes W^* \to (V \otimes W)^*,$$
$$\varphi \otimes \psi \mapsto f_{\varphi,\psi}.$$

Let $b_1, \ldots, b_n$ and $c_1, \ldots, c_m$ be bases of V and W, respectively. Let $\beta_1, \ldots, \beta_n$ and $\gamma_1, \ldots, \gamma_m$ be the corresponding dual bases of V^* and W^*. Let $\alpha \in (V \otimes W)^*$ with $\alpha(b_i \otimes c_j) := \alpha_{ij}$. For $\rho := \sum_{i,j} \alpha_{ij}\beta_i \otimes \gamma_j \in V^* \otimes W^*$, it holds that

$$\hat{f}(\rho)(b_s \otimes c_t) = \sum_{i,j} \alpha_{ij}\beta_i(b_s)\gamma_j(c_t) = \alpha_{st} = \alpha(b_s \otimes c_t) \qquad (s = 1, \ldots, n,\ t = 1, \ldots, m).$$

Thus $\hat{f}$ is surjective and, for dimension reasons, also injective.

(ii) For $\varphi \in V^*$ and $w \in W$, let $f_{\varphi,w}\colon V \to W$, $v \mapsto \varphi(v)w$. Clearly $f_{\varphi,w} \in \mathrm{Hom}_K(V, W)$ and the map $f\colon V^* \times W \to \mathrm{Hom}_K(V, W)$, $(\varphi, w) \mapsto f_{\varphi,w}$ is bilinear. For $g \in G$, it holds that

$$f(g\varphi, gw)(v) = (g\varphi)(v)(gw) = g\varphi(g^{-1}v)w = (gf_{\varphi,w})(v).$$

The universal property yields a homomorphism

$$\hat{f}\colon V^* \otimes W \to \mathrm{Hom}_K(V, W),$$
$$\varphi \otimes w \mapsto f_{\varphi,w}.$$

Let $b_1, \ldots, b_n$ and $c_1, \ldots, c_m$ be bases of V and W, respectively. Let $\varphi \in \mathrm{Hom}_K(V, W)$ with $\varphi(b_i) = \sum_{j=1}^m \lambda_{ij}c_j$ and $\lambda_{ij} \in K$. Let $\beta_1, \ldots, \beta_n$ be the dual basis of V^*. We define $\rho := \sum_{i,j} \lambda_{ij}\beta_i \otimes c_j \in V^* \otimes W$. Then it holds that

$$\hat{f}(\rho)(b_k) = \sum_{i,j} \lambda_{ij}\beta_i(b_k)c_j = \sum_{j=1}^m \lambda_{kj}c_j = \varphi(b_k)$$

for $k = 1, \ldots, m$. Thus $\hat{f}$ is surjective and, for dimension reasons, also injective.

(iii) It holds that

$$\begin{aligned}\mathrm{Hom}_K(U \otimes V, W) &\overset{\text{(ii)}}{\simeq} (U \otimes V)^* \otimes W \overset{\text{(i)}}{\simeq} U^* \otimes V^* \otimes W \\ &\simeq U^* \otimes \mathrm{Hom}_K(V, W) \simeq \mathrm{Hom}_K(U, \mathrm{Hom}_K(V, W)).\end{aligned}$$ □

Theorem III.3.22. *For every KG-module V, the following holds:*

(i) V is simple (resp. indecomposable) if and only if V^* is.

(ii) V is free (resp. projective) if and only if V^* is.

(iii) V is projective-indecomposable if and only if V^* is.

Proof. Due to $V^{**} \simeq V$, it suffices to prove one direction in each case.

(i) Let V be simple and $W < V^*$. Then $W_\perp = V$ and $W^* \simeq V/W_\perp \simeq 0$. This shows $W = 0$. Now let V be indecomposable and $V^* = U \oplus W$. Then $V \simeq V^{**} \cong U^* \oplus W^*$ according to Lemma III.3.21. Again, one obtains $U = 0$ or $W = 0$.

(ii) If V is free, then V possesses a finite basis according to Lemma II.9.5. So let $V \simeq (KG)^n$. Then $V^* \simeq ((KG)^*)^n$. The regular representation $\Delta\colon G \to \mathrm{GL}(|G|, K)$ maps to permutation matrices and these are known to be orthogonal. Therefore $\Delta^* = \Delta$ and $(KG)^* \simeq KG$. Thus V^* is free. Finally, let V be projective. Then there exists an epimorphism $f\colon (KG)^n \to V$ and $V \times \mathrm{Ker}(f) \simeq (KG)^n$. Because of $V^* \times \mathrm{Ker}(f)^* \simeq ((KG)^n)^* \simeq (KG)^n$, V^* is projective.

(iii) Follows from (i) and (ii). □

Remark III.3.23.

(i) For an arbitrary family of KG-modules V_i ($i \in I$), $\left(\coprod_{i\in I} V_i\right)^* \simeq \times_{i\in I} V_i^*$ holds. If V is free with infinite rank (or semisimple), then V^* does not have to be free (resp. semisimple).

(ii) The next result generalizes $\mathrm{J}(A)^\perp = \mathrm{Soc}(A)$ for $A = KG$.

Lemma III.3.24. *For every KG-module V, $\mathrm{Soc}(V)^\perp = \mathrm{J}(V^*)$ and $\mathrm{J}(V)^\perp = \mathrm{Soc}(V^*)$ hold. Consequently,* $\boxed{\mathrm{Soc}(V)^* \simeq V^*/\mathrm{J}(V^*)}$ *and* $\boxed{\mathrm{Soc}(V^*) \simeq (V/\mathrm{J}(V))^*.}$

Proof. According to Remark III.3.20, the maps $U \mapsto U^\perp$ and $W \mapsto W_\perp$ are inverse bijections to each other between the submodules of V and the submodules of V^*. In this context, $V^*/U^\perp \simeq U^*$ and $V/W_\perp \simeq W^*$ hold. According to Theorem III.3.22, the largest semisimple submodule of V is mapped to the smallest submodule of V^* with semisimple factor modules. This shows $\mathrm{Soc}(V)^\perp = \mathrm{J}(V^*)$ and analogously $\mathrm{J}(V)^\perp = \mathrm{Soc}(V^*)$. It follows that $\mathrm{Soc}(V)^* \simeq V^*/\mathrm{Soc}(V)^\perp = V^*/\mathrm{J}(V^*)$ and $\mathrm{Soc}(V^*) \simeq V/\mathrm{Soc}(V^*)_\perp = V/(\mathrm{J}(V)^\perp)_\perp = V/\mathrm{J}(V)$. □

Theorem III.3.25. *For every projective KG-module P, $\mathrm{Soc}(P) \simeq P/\mathrm{J}(P)$ holds.*

Proof. Wlog. let P be projective-indecomposable. Let $e \in KG$ be a primitive idempotent with $P = KGe$. According to Lemma III.3.24, $S := \mathrm{Soc}(P) \subseteq P$ is a simple KG-module. Let $s = \sum_{g\in G} \alpha_g g \in S \setminus \{0\}$. Then there exists a $g \in G$ with $\alpha_g \neq 0$. According to Remark II.13.20, KG is symmetric with respect to the bilinear form $\beta(\sum \sigma_g g, \sum \tau_g g) = \sum_{g\in G} \sigma_g \tau_{g^{-1}}$. It follows that

$$\beta(eg^{-1}s, 1) = \beta(eg^{-1}, s) = \beta(s, eg^{-1}) = \beta(se, g^{-1}) = \beta(s, g^{-1}) = \alpha_g \neq 0.$$

In particular, $0 \neq eg^{-1}s \in S$ and $P \to S$, $x \mapsto xg^{-1}s$ is a non-trivial homomorphism. Since S is simple, it follows that $P/\mathrm{J}(P) \simeq S$. □

Theorem III.3.26. *If K is algebraically closed, then the Cartan matrix of KG is symmetric.*

Proof. The statement follows from Remark II.13.20 and Theorem II.13.4. □

Remark III.3.27.

(i) Let $C(KG) = (c_{ij})$. If $c_{ii} = 1$, then $c_{ij} = 0$ for all $j \neq i$ follows from Theorem III.3.25.

(ii) For $\mathrm{char}\, K = 0$, $C(KG) = 1_k$ according to Maschke. In general, one can show that $C = C(KG)$ is positive definite (if $K = \overline{K}$). In the case $p := \mathrm{char}\, K > 0$, the elementary divisors of C (as an integer matrix) are powers of p. In particular, $\det C$ is a p-power (without proof). For arbitrary algebras, the Cartan matrix is in general not invertible (Exercise III.20).

(iii) The assumption $K = \overline{K}$ in Theorem III.3.26 is necessary:

$$C(\mathbb{F}_2 A_4) = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}, \qquad C(\mathbb{F}_4 A_4) = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

Definition III.3.28. For a KG-module V and $H \leq G$, one obtains the KH-module V_H by restriction. Conversely, we construct a KG-module from a KH-module U. For this, we consider the K-vector space

$$U^G := (KG \otimes U)/\operatorname{Span}_K\{gh \otimes u - g \otimes hu : g \in G, h \in H, u \in U\}.$$

In the following, we will identify the elements of U^G with suitable representatives from $KG \otimes U$. It then holds that $gh \otimes u = g \otimes hu$ for $g \in G$, $h \in KH$ and $u \in U$.

Lemma III.3.29. *By $x(g \otimes u) := xg \otimes u$ for $x, g \in G, u \in U$, U^G becomes a KG-module of dimension $|G : H| \dim U$. One calls U^G the module* induced *from U.*

Proof. Let B be a basis of U and R a system of representatives for G/H. For each $g \in G$ there exist $r \in R$ and $h \in H$ with $g = rh$. For $u \in U$ it then holds that $g \otimes u = r \otimes hu$. Therefore U^G is generated as a K-vector space by the elements of the form $r \otimes b$ with $r \in R$ and $b \in B$. In particular, $\dim U^G \leq |G : H| \dim U$. For $r, s \in R$ we define a K-linear map $\varphi_r \colon KG \otimes U \to U$, $sh \otimes b \mapsto \delta_{rs} hb$ with $h \in H$ and $b \in B$. Then

$$\begin{aligned} \varphi \colon KG \otimes U &\to U^{|G:H|}, \\ x &\mapsto (\varphi_r(x))_{r \in R} \end{aligned}$$

is K-linear and surjective. Because of $\varphi_r(rh \otimes u - r \otimes hu) = hu - hu = 0$, it holds that $gh \otimes u - g \otimes hu \in \operatorname{Ker}(\varphi)$ for all $g \in G$, $h \in H$ and $u \in U$. It follows that

$$|G : H| \dim U = \dim(U^{|G:H|}) = \dim(KG \otimes U) - \dim \operatorname{Ker}(\varphi) \leq \dim U^G \leq |G : H| \dim U.$$

Thus the elements $r \otimes b$ with $r \in R$ and $b \in B$ form a basis of U^G. We define $g(r \otimes b) := gr \otimes b$ and extend linearly. For an arbitrary $x \in G$ there exist $r \in R$ and $h \in H$ with $x = rh$. It then holds that

$$g(x \otimes u) = g(r \otimes hu) = gr \otimes hu = grh \otimes u = gx \otimes u.$$

This shows $(gg')(x \otimes u) = (gg')x \otimes u = g(g'x) \otimes u = g(g'(x \otimes u))$ for $g, g' \in G$. In this way U^G becomes a KG-module. □

Remark III.3.30. Let $\Delta \colon H \to \mathrm{GL}(n, K)$ be a representation with KH-module U with respect to a basis B. Let $r_1, \ldots, r_k$ be representatives for G/H. As in the proof of Lemma III.3.29, $\hat{B} := \{r_i \otimes b : b \in B,\ i = 1, \ldots, k\}$ is a basis of U^G. For $g \in G$ and $r_i \in R$ there exists exactly one $r_j \in R$ with $r_j^{-1} g r_i \in H$. It then holds that $g(r_i \otimes b) = r_j \otimes r_j^{-1} g r_i b$. We define $\hat{\Delta}(g) := \Delta(g)$ if $g \in H$ and $\hat{\Delta}(g) := 0 \in K^{n \times n}$ otherwise. The *induced* representation Δ^G of U^G with respect to $\hat{B}$ then has the form

$$\Delta^G(g) = \begin{pmatrix} \hat{\Delta}(r_1^{-1} g r_1) & \cdots & \hat{\Delta}(r_1^{-1} g r_k) \\ \vdots & & \vdots \\ \hat{\Delta}(r_k^{-1} g r_1) & \cdots & \hat{\Delta}(r_k^{-1} g r_k) \end{pmatrix}.$$

Now let $K = \mathbb{C}$ and ψ be the character of Δ. For the *induced* character ψ^G of Δ^G it holds that

$$\psi^G(g) = \sum_{i=1}^{k} \operatorname{tr} \hat{\Delta}(r_i^{-1} g r_i) = \sum_{\substack{1 \leq i \leq k \\ g \in r_i H r_i^{-1}}} \psi(r_i^{-1} g r_i) = \sum_{\substack{xH \in G/H \\ gxH = xH}} \psi(x^{-1} g x).$$

Example III.3.31. Let Ω be a transitive G-set and $H := G_\omega$ for an $\omega \in \Omega$. For the basis of the permutation module V from Example II.14.4, one can choose the cosets $G/H = \{r_1H, \dots, r_kH\}$ according to Theorem I.4.7. It then holds that $V \simeq U^G$, where $U \simeq K$ is the trivial module of H. The permutation character is therefore $(\mathbb{1}_H)^G$. In particular, $(\mathbb{1}_1)^G$ is the regular character. If $H \trianglelefteq G$, then U^G is the inflation of the regular $K[G/N]$-module.

Lemma III.3.32 (Frobenius-Nakayama reciprocity)**.** *Let V be a KG-module, $H \leq G$ and U a KH-module. Then*

$$\begin{aligned} \mathrm{Hom}_{KH}(U, V_H) &\to \mathrm{Hom}_{KG}(U^G, V), \qquad \varphi \mapsto \widehat{\varphi} \\ \mathrm{Hom}_{KH}(V_H, U) &\to \mathrm{Hom}_{KG}(V, U^G), \qquad \psi \mapsto \widetilde{\psi} \end{aligned}$$

are vector space isomorphisms with $\widehat{\varphi}(g \otimes u) = g\varphi(u)$ and $\widetilde{\psi}(v) = \sum_{gH \in G/H} g \otimes \psi(g^{-1}v)$ for $g \in G$, $u \in U$ and $v \in V$.

Proof. As in the proof of Lemma III.3.29, let R be a system of representatives for G/H and B a basis of U.

(i) For $\varphi \in \mathrm{Hom}_{KH}(U, V_H)$, we define $\widehat{\varphi}(r \otimes b) := r\varphi(b)$ for $r \in R$ and $b \in B$. Let $u \in U$ and $g = rh \in G$ with $r \in R$ and $h \in H$. Let $hu = \sum_{b \in B} \alpha_b b \in U$ with $\alpha_b \in K$. Then it follows

$$\widehat{\varphi}(g \otimes u) = \widehat{\varphi}(r \otimes hu) = \widehat{\varphi}\Big(\sum_{b \in B} \alpha_b (r \otimes b)\Big) = \sum_{b \in B} \alpha_b r\varphi(b) = r\varphi(hu) = rh\varphi(u) = g\varphi(u).$$

For $x \in G$, we have $\widehat{\varphi}(xg \otimes u) = (xg)\varphi(u) = x(g\varphi(u)) = x\widehat{\varphi}(g \otimes u)$. This shows $\widehat{\varphi} \in \mathrm{Hom}_{KG}(U^G, V)$. If $\widehat{\varphi} = 0$, then $\varphi(b) = \widehat{\varphi}(1 \otimes b) = 0$ and $\varphi = 0$. Therefore, the map $\varphi \mapsto \widehat{\varphi}$ is injective and K-linear. Conversely, if $\rho \in \mathrm{Hom}_{KG}(U^G, V)$ is given, then $\varphi \colon U \to V_H$, $u \mapsto \rho(1 \otimes u)$ is clearly a homomorphism with $\widehat{\varphi} = \rho$.

(ii) For $\psi \in \mathrm{Hom}_{KH}(V_H, U)$, we can directly define $\widetilde{\psi}(v) = \sum_{r \in R} r \otimes \psi(r^{-1}v)$ for $v \in V$. If R' is another system of representatives for G/H, then there exists a bijection $R \to R'$, $r \mapsto r'$ with $r^{-1}r' \in H$ for $r \in R$. It follows

$$r' \otimes \psi((r')^{-1}v) = rr^{-1}r' \otimes \psi((r')^{-1}v) = r \otimes r^{-1}r'\psi((r')^{-1}v) = r \otimes \psi(r^{-1}v).$$

Thus $\widetilde{\psi}$ does not depend on the choice of R. For $g \in G$, gR is also a system of representatives for G/H. This implies

$$\widetilde{\psi}(gv) = \sum_{r \in R} r \otimes \psi(r^{-1}gv) = \sum_{r \in R} gr \otimes \psi((gr)^{-1}gv) = g\sum_{r \in R} r \otimes \psi(r^{-1}v) = g\widetilde{\psi}(v)$$

and $\widetilde{\psi} \in \mathrm{Hom}_{KG}(V, U^G)$. Let $\widetilde{\psi} = 0$. Since the elements $r \otimes \psi(r^{-1}v)$ for $r \in R$ are linearly independent, it follows that $\psi(r^{-1}v) = 0$ for all $v \in V$. Therefore $\psi = 0$ and the map $\psi \mapsto \widetilde{\psi}$ is injective and K-linear.

Finally, let $\rho \in \mathrm{Hom}_{KG}(V, U^G)$ be given. For $v \in V$, let $\rho_r(v) \in U$ with $\rho(v) = \sum_{r \in R} r \otimes \rho_r(v)$. Wlog. let $1 \in R$. For $h \in H$, we have

$$\sum_{r \in R} r \otimes \rho_r(hv) = \rho(hv) = h\rho(v) = \sum_{r \in R} hr \otimes \rho_r(v) = 1 \otimes h\rho_1(v) + \sum_{r \in R \setminus \{1\}} hr \otimes \rho_r(v).$$

Therefore $\rho_1 \colon V_H \to U$ is a homomorphism. For $s \in R$, it also holds that

$$\sum_{r\in R} r \otimes \rho_r(s^{-1}v) = \rho(s^{-1}v) = s^{-1}\rho(v) = \sum_{r\in R} s^{-1}r \otimes \rho_r(v) = 1 \otimes \rho_s(v) + \sum_{r\in R\setminus\{s\}} s^{-1}r \otimes \rho_r(v).$$

Consequently, $\rho_1(s^{-1}v) = \rho_s(v)$ and

$$\widetilde{\rho_1}(v) = \sum_{r\in R} r \otimes \rho_1(r^{-1}v) = \rho(v).$$

Thus $\psi \mapsto \widetilde{\psi}$ is also surjective. □

Remark III.3.33. Let $K = \mathbb{C}$ in the situation of Lemma III.3.32. Then all modules are semisimple and we can write $U \simeq T_1^{a_1} \times \ldots \times T_k^{a_k}$ and $V_H \simeq T_1^{b_1} \times \ldots \times T_k^{b_k}$ with pairwise non-isomorphic simple KH-modules $T_1, \ldots, T_k$. Let ψ and χ be the characters of U and V. According to Schur's Lemma and Lemma II.7.20, it holds that

$$(\psi, \chi_H) = a_1b_1 + \ldots + a_kb_k = \dim \mathrm{Hom}_{\mathbb{C}H}(U, V_H) \overset{\text{III.3.32}}{=} \dim \mathrm{Hom}_{\mathbb{C}G}(U^G, V) = (\psi^G, \chi).$$

This equation is referred to as *Frobenius reciprocity*. If U and V are simple, one obtains: The multiplicity of U in V_H is the multiplicity of V in U^G.

Lemma III.3.34. *For subgroups $H \leq L \leq G$, KH-modules U, V and a KG-module W, it holds that*

(i) $(U \times V)^G \simeq U^G \times V^G$.

(ii) $(U^*)^G \simeq (U^G)^*$.

(iii) $(U^L)^G \simeq U^G$.

(iv) $U^G \otimes W \simeq (U \otimes W_H)^G$.

(v) If U is free (resp. projective), then so is U^G.

(vi) If W is free (resp. projective), then so is W_H.

(vii) If W is free (resp. projective), then so is $Q \otimes W$ for every KG-module Q.

Proof.

(i) Since $\varphi \colon U \times V \to (U^G \times V^G)_H$, $(u, v) \mapsto (1 \otimes u, 1 \otimes v)$ is a homomorphism, there exists $\widehat{\varphi} \colon (U \times V)^G \to U^G \times V^G$, $g \otimes (u, v) \mapsto (g \otimes u, g \otimes v)$ by Lemma III.3.32. Because of $\widehat{\varphi}(g \otimes (u, 0)) = (g \otimes u, 0)$, $\widehat{\varphi}$ is surjective and, for dimension reasons, also injective.

(ii) For $\lambda \in U^*$ let $\overline{\lambda} \in (U^G)^*$ with

$$\overline{\lambda}(g \otimes u) = \begin{cases} \lambda(gu) & \text{if } g \in H, \\ 0 & \text{otherwise.} \end{cases}$$

For $h \in H$ it holds that $\overline{h\lambda} = h\overline{\lambda}$. Therefore $\varphi \colon U^* \to ((U^G)^*)_H$, $\lambda \mapsto \overline{\lambda}$ is a homomorphism. By Lemma III.3.32 there exists $\widehat{\varphi} \colon (U^*)^G \to (U^G)^*$, $g \otimes \lambda \mapsto g\overline{\lambda}$. Let R be a system of representatives for G/H and $\sum_{r\in R} r \otimes \lambda_r \in \mathrm{Ker}(\widehat{\varphi})$. For $s \in R$ and $u \in U$ it holds that

$$0 = \sum_{r\in R} r\overline{\lambda_r}(s \otimes u) = \sum_{r\in R} \overline{\lambda_r}(r^{-1}s \otimes u) = \lambda_s(u).$$

This shows $\lambda_s = 0$ for all $s \in R$. Consequently, $\widehat{\varphi}$ is injective and, for dimension reasons, also surjective.

(iii) With $\varphi\colon U^L \to (U^G)_L$, $x \otimes u \mapsto x \otimes u$, also $\widehat{\varphi}\colon (U^L)^G \to (U^G)$, $g \otimes (x \otimes u) \mapsto gx \otimes u$ is a homomorphism. Obviously $\widehat{\varphi}$ is surjective and because of

$$\dim(U^L)^G = |G : L| \dim U^L = |G : L||L : H| \dim U = |G : H| \dim U = \dim U^G$$

also injective.

(iv) The map $f\colon U \times W_H \to (U^G \otimes W)_H$, $(u, w) \mapsto (1 \otimes u) \otimes w$ is bilinear and satisfies

$$f(h(u, w)) = (1 \otimes hu) \otimes hw = (h \otimes u) \otimes hw = h(f(u, w))$$

for $h \in H$. By the universal property, there exists a homomorphism $\varphi\colon U \otimes W_H \to (U^G \otimes W)_H$, $u \otimes w \mapsto (1 \otimes u) \otimes w$. This yields a homomorphism $\widehat{\varphi}\colon (U \otimes W_H)^G \to U^G \otimes W$, $g \otimes (u \otimes w) \mapsto (g \otimes u) \otimes gw$. One easily sees that $\widehat{\varphi}$ is surjective. Because of

$$\dim(U \otimes W_H)^G = |G : H| \dim(U) \dim(W) = \dim(U^G) \dim W = \dim(U^G \otimes W)$$

$\widehat{\varphi}$ is injective.

(v) The inclusion $\varphi\colon KH \to KG$ induces a homomorphism $\widehat{\varphi}\colon (KH)^G \to KG$, $g \otimes a \mapsto ga$ for $a \in KH$. Obviously $\widehat{\varphi}$ is an isomorphism. If U is free, then $U \simeq (KH)^n$ and $U^G \simeq ((KH)^n)^G \simeq ((KH)^G)^n \simeq KG^n$ by (i). Thus U^G is free. The analogous statement for projective modules also follows from (i).

(vi) For $g \in G$, $KH \to KHg$, $h \mapsto hg$ is an isomorphism of KH-modules. Let R be a system of representatives for the right cosets of G modulo H. Then $KG = \bigoplus_{r \in R} KHr \simeq (KH)^{|G:H|}$. From this the assertion follows easily.

(vii) Let $n \in \mathbb{N}$ with $W = KG^n$. For the trivial $K1$-module $U \simeq K$, it holds that $KG \simeq U^G$ and

$$Q \otimes W \simeq (Q \otimes U^G)^n \overset{\text{(v)}}{\simeq} ((Q_1 \otimes U)^G)^n \simeq ((U^{\dim Q})^G)^n \overset{\text{(i)}}{\simeq} KG^{n \dim Q}.$$

Therefore $Q \otimes W$ is free. Now let W be projective with $W \oplus W' = KG^n$. Then $(Q \otimes W) \oplus (Q \otimes W') \simeq Q \otimes KG^n$. Thus $Q \otimes W$ is projective. □

Theorem III.3.35. *Let K be a field of characteristic $p > 0$ and $|G| = p^a n$ with $p \nmid n$. Then the following statements are equivalent:*

(1) $C(KG)$ is a diagonal matrix.

(2) The principal block of KG is local.

(3) There exists an $N \trianglelefteq G$ with $|N| = n$.

Proof.

(1) ⇒ (2): Theorem II.12.29 implies that the trivial module K is the only simple module of the principal block B_0. Because of $\mathrm{End}_{B_0}(K) \cong K$, it follows that $B_0/\mathrm{J}(B_0) \cong K$ by Remark II.12.3.

(2) ⇒ (3): Let $e_0 = \sum_{g \in G} \alpha_g g \in \mathrm{Z}(KG)$ be the principal block idempotent. By assumption, the principal block $B_0 = KGe_0$ is a projective-indecomposable KG-module. By Theorem II.12.29, all composition factors of B_0 are trivial. Let $\Delta\colon G \to \mathrm{GL}(B_0)$ be the representation by left multiplication and $N := \mathrm{Ker}(\Delta) \trianglelefteq G$. Let $g \in G$ be a p'-element. By Maschke, B_0 is a semisimple $K\langle g \rangle$-module whose composition factors are still trivial. This shows $g \in N$. Conversely, let $g \in N$.

Since $g_{p'} \in N$, it follows that $g_p \in N$. From $g_p e_0 = e_0$ it follows that $\alpha_x = \alpha_{xh}$ for $x \in G$ and $h \in H := \langle g_p \rangle$. For the augmentation map $\nu\colon KG \to K$, we have

$$1 = \nu(e_0) = \sum_{x \in G} \alpha_x = \sum_{xH \in G/H} |H| \alpha_x$$

by Remark II.13.24. This shows $H = 1$ and $g = g_{p'}$. Thus N consists of all p'-elements of G. By Lagrange, $|N|$ is a divisor of n. Since $xN = x_p N$, on the other hand G/N is a p-group. Consequently, $|N| = n$.

(3) $\Rightarrow$ (1): Let $P \in \mathrm{Syl}_p(G)$. By Lagrange, $P \cap N = 1$. From $|PN| = |P||N| = |G|$ it follows that $G = PN$ and $G/N \cong P$. By inflation, KP becomes a KG-module. By Maschke, KN is semisimple. Therefore $KN = U \oplus W$, where $U \simeq K$ is the trivial KN-module. This shows

$$KG \simeq KN^G \simeq U^G \oplus W^G \overset{\text{III.3.31}}{\simeq} K[G/N] \oplus W^G \simeq KP \oplus W^G.$$

In particular, KP is a projective KG-module. For every simple KG-module V, the module $V \otimes KP$ is also projective by Lemma III.3.34. Since P is a p-group, all composition factors of KP are trivial. If S/T is such a composition factor, then

$$(V \otimes S)/(V \otimes T) \overset{\text{III.3.19}}{\simeq} V \otimes (S/T) \simeq V$$

is a composition factor of $V \otimes KP$. Therefore all composition factors of $V \otimes KP$ are isomorphic to V. A projective-indecomposable summand Q of $V \otimes KP$ therefore satisfies $Q/\mathrm{J}(Q) \simeq V$. Furthermore, all composition factors of Q are isomorphic to V. Since V was an arbitrary simple KG-module, $C(KG)$ must be a diagonal matrix. □

Remark III.3.36. In the situation of Theorem III.3.35, $e := \frac{1}{n} \sum_{x \in N} x \in \mathrm{Z}(KG)$ is a central idempotent. For $y \in N$, we have $ye = e$. Let $P \in \mathrm{Syl}_p(G)$. Then $G = PN$ and every $g \in G$ can be uniquely written in the form $g = xy$ with $x \in P$ and $y \in N$. It holds that $ge = xe$. For distinct $x, x' \in P$, $xN \cap x'N = \varnothing$. Therefore $KP \to KGe$, $x \mapsto xe$ is an isomorphism of algebras. Since KP is indecomposable, KGe is also indecomposable and e is primitive. Because of $\nu(e) = 1$, $B_0 := KGe$ must be the principal block of KG. Thus $B_0 \cong KP$ holds.

Theorem III.3.37 (Dickson)**.** *Let $p := \mathrm{char}\, K > 0$ and $|G| = p^a n$ with $p \nmid n$. Let M be a projective KG-module. Then $\dim_K M$ is divisible by p^a.*

Proof. Let $P \in \mathrm{Syl}_p(G)$. According to Lemma III.3.34, M_P is projective. According to Theorem III.3.14, $KP \cong \mathrm{End}_{KP}(KP)^o$ is local, i. e. the regular KP-module is indecomposable. Thus M_P is even a free KP-module by Krull-Schmidt; say $M_P \simeq (KP)^k$. Then it follows that $\dim_K M = k|P| = kp^a$. □

Example III.3.38. Let $p := \mathrm{char}\, K > 0$ and $|G| = p^a n$ with $p \nmid n$. Suppose there exists a subgroup $H \leq G$ with $|H| = n$ (a theorem of Hall from group theory states that H always exists for solvable groups G). Let U be a 1-dimensional KH-module. By Maschke, U is projective and therefore so is $V := U^G$. Because of $\dim V = |G : H| \dim U = p^a$, V is projective-indecomposable by Dickson. Now let $U \simeq K$ be the trivial KH-module. According to Lemma III.3.32,

$$\dim \mathrm{Hom}_{KG}(V, K) = \dim \mathrm{Hom}_{KH}(U, U) = 1$$

and it follows that $V/\mathrm{J}(V) \simeq K$. If G is solvable and K is algebraically closed, then for every projective-indecomposable KG-module V there exists a simple KH-module U with $V \simeq U^G$ (without proof).

Lemma III.3.39. *Let V be a KG-module and $H \leq G$ with $|G:H| \in K^\times$. Then V is a direct summand of $(V_H)^G$.*

Proof. The identity $V_H \to V_H$ yields, with Lemma III.3.32, homomorphisms

$$\begin{aligned} \varphi\colon (V_H)^G &\to V, & g \otimes v &\mapsto gv, \\ \psi\colon V &\to (V_H)^G, & v &\mapsto \sum_{gH \in G/H} g \otimes g^{-1}v. \end{aligned}$$

Because of $(\varphi\psi)(v) = |G:H|v \neq 0$, ψ is injective and φ is surjective. In particular, $V \simeq \psi(V) \leq (V_H)^G$. For $U := \operatorname{Ker}(\varphi) \leq (V_H)^G$, we have $\psi(V) \cap U = 0$ and $\dim V = \dim((V_H)^G/U) = \dim(V_H)^G - \dim U$. This shows $(V_H)^G = \psi(V) \oplus U$. □

Remark III.3.40.

(i) Let $S, T \leq G$. Then $S \times T$ acts on G by ${}^{(s,t)}g := sgt^{-1}$ for $(s,t) \in S \times T$. The orbits have the form SgT and are called *double cosets* of G by S, T.

(ii) Let $g \in G$, $H \leq G$ and U be a KH-module. Then $gHg^{-1} \leq G$ and $g \otimes U = \{g \otimes u : u \in U\}$ is a gHg^{-1}-module with

$$ghg^{-1}(g \otimes u) := g \otimes hu$$

for $h \in H$ and $u \in U$ (the axioms transfer from U^G to $g \otimes U$).

Lemma III.3.41 (Mackey formulas)**.** *Let $S, T \leq G$ and R be a transversal for the double cosets of G by S, T. Let U be a KS-module and V be a KT-module. Then:*

$$\boxed{(V^G)_S \simeq \bigtimes_{r \in R} \left((r \otimes V)_{rTr^{-1} \cap S}\right)^S,}$$

$$\boxed{U^G \otimes V^G \simeq \bigtimes_{r \in R} \left(U_{rTr^{-1} \cap S} \otimes (r \otimes V)_{rTr^{-1} \cap S}\right)^G.}$$

Proof.

(i) Obviously, the map

$$\begin{aligned} \varphi\colon \bigtimes_{r \in R} \left((r \otimes V)_{rTr^{-1} \cap S}\right)^S &\to (V^G)_S \\ (s_r \otimes r \otimes v)_{r \in R} &\mapsto \sum_{r \in R} s_r r \otimes v_r. \end{aligned}$$

is a homomorphism of KS-modules. For each $g \in G$ there exists exactly one triple $(s, r, t) \in S \times R \times T$ with $g = srt$. Therefore φ is surjective. Furthermore, SR is a transversal for G/T. Thus, if $(s_r \otimes r \otimes v)_{r \in R} \in \operatorname{Ker}(\varphi)$, then $s_r r \otimes v_r = 0 = v_r$ for all $r \in R$. Therefore φ is also injective.

(ii) By Lemma III.3.34 and (i) it holds that

$$\begin{aligned} U^G \otimes V^G &\simeq (U \otimes (V^G)_S)^G \simeq \Big(U \otimes \bigtimes_{r\in R} \big((r\otimes V)_{rTr^{-1}\cap S}\big)^S\Big)^G \\ &\simeq \Big(\bigtimes_{r\in R} \big(U \otimes ((r\otimes V)_{rTr^{-1}\cap S})^S\big)\Big)^G \simeq \Big(\bigtimes_{r\in R} \big(U_{rTr^{-1}\cap S} \otimes (r\otimes V)_{rTr^{-1}\cap S}\big)^S\Big)^G \\ &\simeq \bigtimes_{r\in R} \big(U_{rTr^{-1}\cap S} \otimes (r\otimes V)_{rTr^{-1}\cap S}\big)^G. \end{aligned}$$

□

Theorem III.3.42 (Higman)**.** *Let K be a field of characteristic $p > 0$ and $P \in \mathrm{Syl}_p(G)$.*

(i) If P is cyclic, then every indecomposable KG-module has dimension $\leq |G|$ and there are at most finitely many such modules up to isomorphism.

(ii) If P is not cyclic, then there exist indecomposable KG-modules with arbitrarily large dimension.

In particular, KG has finite representation type if and only if P is cyclic.

Proof.

(i) Let V be an indecomposable KG-module. According to Lemma III.3.39, $(V_P)^G \simeq V \oplus U$. Let $V_P = V_1 \oplus \ldots \oplus V_k$ with indecomposable modules $V_1, \ldots, V_k$. Then $V \oplus U \simeq V_1^G \oplus \ldots \oplus V_k^G$ holds. By Krull-Schmidt, V is isomorphic to a direct summand of V_i^G. From Theorem III.3.14 it follows that

$$\dim V \leq \dim V_i^G = |G:P| \dim V_i \leq |G:P||P| = |G|.$$

Obviously, V_i^G has at most $\dim V_i^G$ many direct summands. Since KP has only one indecomposable module in each dimension $d \in \{1, \ldots, |P|\}$, there are at most

$$|G:P| \sum_{d=1}^{|P|} d = |G| \frac{|P|+1}{2} < \infty$$

indecomposable KG-modules up to isomorphism.

(ii) According to Theorem III.3.14, for every $d \in \mathbb{N}$ there exists an indecomposable KP-module U of dimension d. Let R be a transversal for the double cosets of G by P, P with $1 \in R$. By the Mackey formula, $U \simeq 1 \otimes U$ is a direct summand of $(U^G)_P$. Therefore, there exists an indecomposable KG-module V such that U is a summand of V_P.[5] In particular, $\dim V \geq \dim U = d$. □

Remark III.3.43.

(i) Let $N \trianglelefteq G$ and U be a KN-module. For $g \in G$, $g \otimes U$ is also a KN-module, because $gNg^{-1} = N$. Due to $g \otimes (h \otimes U) \simeq gh \otimes U$ for $g, h \in G$, G acts on the set of isomorphism classes of KN-modules. Let

$$G_U := \{g \in G : g \otimes U \simeq U\} \leq G$$

be the stabilizer of U in G. Certainly $N \leq G_U$ holds.

(ii) The map $U \to g \otimes U$, $u \mapsto g \otimes u$ induces a bijection between the sets of submodules. In particular, U is simple (resp. indecomposable) if and only if $g \otimes U$ is. Furthermore, $KN \to g \otimes KN$, $x \mapsto g \otimes g^{-1}xg$ for $x \in N$ is an isomorphism of KN-modules. Thus, U is free (resp. projective) if and only if $g \otimes U$ is.

[5] This also shows that the estimate in (i) is not optimal.

(iii) If U is simple, then $(U^G)_N \simeq \bigtimes_{gN\in G/N} g\otimes U$ is semisimple.

(iv) For $N \le H \le G$, let $\Gamma(H,U)$ be the set of isomorphism classes of simple KH-modules W such that U is isomorphic to a submodule of W_N.

Theorem III.3.44 (Clifford)**.** *Let V be a simple KG-module, $N \trianglelefteq G$ and U a simple KN-module. Then the following hold:*

(i) U is isomorphic to a submodule of V_N if and only if V is isomorphic to a submodule of U^G.

(ii) If $U \le V_N$, then there exists $e \le |G_U : N|$ with

$$\boxed{V_N \simeq \bigtimes_{gG_U\in G/G_U} (g\otimes U)^e.}$$

(iii) The map $\Gamma(G_U,U) \to \Gamma(G,U)$, $W \mapsto W^G$ is a bijection, where U occurs as a direct summand as many times in W_N as in $(W^G)_N$. Furthermore, W occurs only once as a composition factor of $(W^G)_{G_U}$.

Proof.

(ii) Apparently $\sum_{g\in G} gU \neq 0$ is a submodule of V. Since V is simple, it follows that $V = \sum_{g\in G} gU$. Let R be a transversal for G/G_U. For $r \in R$ and $h \in G_U$ we have

$$rhU \simeq rh\otimes U \simeq r\otimes(h\otimes U) \simeq r\otimes U.$$

Since $r\otimes U$ is a simple KN-module, it follows that

$$V_r := \sum_{h\in G_U} rhU = \sum_{hN\in G_U/N} rhU \simeq (r\otimes U)^e$$

for some $e \le |G_U : N|$ according to Theorem II.7.4. For $r \neq s \in R$ we have $r\otimes U \not\simeq s\otimes U$. This implies $V = \bigoplus_{r\in R} V_r$. Since the map $V_r \to V_s$, $x \mapsto sr^{-1}x$ is a vector space isomorphism, $V_s \simeq (s\otimes U)^e$ holds for all $s \in R$.

(i) Let $U \le V_N$ (up to isomorphism). According to (ii), V_N is semisimple and therefore $V_N = U\oplus W$ for a KN-module W. From Frobenius-Nakayama it follows that $\mathrm{Hom}_{KG}(V,U^G) \simeq \mathrm{Hom}_{KN}(V_N,U) \neq 0$. Since V is simple, every non-trivial homomorphism $V \to U^G$ is injective. Thus V is isomorphic to a submodule of U^G. Conversely, let $V \le U^G$. Then $\mathrm{Hom}_{KN}(V_H,U) \simeq \mathrm{Hom}_{KG}(V,U^G) \neq 0$. Now every non-trivial homomorphism $V_N \to U$ is surjective. Therefore U is a composition factor of V_N. Since V_N is semisimple, U is also isomorphic to a submodule of V_N.

(iii) Let $W \in \Gamma(G_U,U)$ and M be a maximal submodule of W^G. Then $V := W^G/M$ is a simple KG-module. According to Frobenius-Nakayama, $\mathrm{Hom}_{KG_U}(W,V_{G_U}) \neq 0$ and $W \le V_{G_U}$ up to isomorphism. This shows $U \le W_N \le V_N$ and $V \in \Gamma(G,U)$. From (ii) one obtains $e,f \in \mathbb{N}$ with

$$V_N \simeq \bigtimes_{r\in R} (r\otimes U)^e, \qquad\qquad W_N \simeq U^f.$$

Because of $W_N \le V_N$, $f \le e$ holds. On the other hand,

$$e|R|\dim U = \dim V \le \dim W^G = |G : G_U|\dim W \le |R| f \dim U.$$

This shows $e = f$ and $W^G \simeq V \in \Gamma(G, U)$. The multiplicity of U as a direct summand of W_N or $(W^G)_N$ is e in each case. In particular, W can also occur only once as a composition factor of $(W^G)_{G_U}$.

Assume there exists $W \not\simeq W' \in \Gamma(G_U, U)$ with $(W')^G \simeq V$. Then $W \oplus W' \leq V_{G_U}$ and U would have to occur with multiplicity $2e$ in V_N. This contradiction shows the injectivity of $W \mapsto W^G$.

Conversely, let $V \in \Gamma(G, U)$ be given. According to (i), $V \leq U^G = (U^{G_U})^G$ up to isomorphism. From Frobenius-Nakayama it follows that $\mathrm{Hom}_{KG_U}(V_{G_U}, U^{G_U}) \neq 0$. Therefore there exists a composition factor W of U^{G_U} with $\mathrm{Hom}_{KG}(V, W^G) \simeq \mathrm{Hom}_{KG_U}(V_{G_U}, W) \neq 0$. The Mackey formula yields $(U^{G_U})_N = \bigtimes_{gN \in G_U/N} (g \otimes U) \simeq U^{|G_U:N|}$. Thus all composition factors of W_N are isomorphic to U. In particular, $W \in \Gamma(G_U, U)$ and the first part of the proof shows $V \simeq W^G$. This shows the surjectivity of $W \mapsto W^G$. □

Corollary III.3.45. *Let V be a semisimple KG-module and $N \trianglelefteq G$. Then V_N is semisimple.*

Remark III.3.46.

(i) In the situation of Theorem III.3.44(ii), e is called the *ramification index* of U in G. In the case $e = 1$, $V_N = \bigoplus_{gG_U \in G/G_U} gU$, where the summands are permuted by G. In general, G only permutes the semisimple summands V_r in the above proof.

(ii) The bijection in (iii) is called the *Clifford correspondence*. Accordingly, W (resp. W^G) is called the *Clifford correspondent* of W^G (resp. W).

Theorem III.3.47 (Green's Indecomposability Theorem)**.** *Let K be an algebraically closed field of characteristic $p > 0$ and $N \trianglelefteq G$ such that G/N is a p-group. For every indecomposable KN-module U, U^G is then also indecomposable.*

Proof. Induction on $|G/N|$: In the case $G = N$ there is nothing to show. So let $N < G$ and $Z/N \leq \mathrm{Z}(G/N)$ with $|Z/N| = p$ (Theorem I.4.11). Then $Z \trianglelefteq G$ holds by the correspondence theorem. If the claim is already proven for smaller indices, then U^Z and $U^G \simeq (U^Z)^G$ are indecomposable. We can therefore assume $G = Z$, i. e. $|G/N| = p$.

Let $V \leq U^G$ be an indecomposable direct summand. Then

$$V_N \leq (U^G)_N = \bigoplus_{i=1}^{p} g^i \otimes U$$

for some $g \in G \setminus N$. First, let $G_U = N$. By Krull-Schmidt, there exists $1 \leq i \leq p$ with $g^i \otimes U \leq V_N$. Obviously, $g^{i+1} \otimes U = g(g^i \otimes U) \leq gV_N = V$ also holds. Since the $g^i \otimes U$ are pairwise non-isomorphic, it follows that $\dim V \geq p \dim U = \dim U^G$ and $V = U^G$. Thus U^G is indecomposable.

Now let $G_U = G$ and $(U^G)_N \simeq U^p$. By Remark II.12.12 it suffices to show that $E := \mathrm{End}_{KG}(U^G)$ is local. Let $\gamma \in E$ be the multiplication by g. Then

$$E = \{\varphi \in \mathrm{End}_{KN}(U^p) : \varphi\gamma = \gamma\varphi\}.$$

By Lemma II.7.20, $\mathrm{End}_{KN}(U^p) \cong \mathrm{End}_{KN}(U)^{p \times p}$. Here $F := \mathrm{End}_{KN}(U)$ is local and $F/\mathrm{J}(F) \cong K$, since K is algebraically closed. By Lemma II.12.26

$$\overline{F^{p \times p}} := F^{p \times p}/\mathrm{J}(F^{p \times p}) = F^{p \times p}/\mathrm{J}(F)^{p \times p} \cong K^{p \times p}.$$

Let

$$\overline{E} := (E + \mathrm{J}(F)^{p\times p})/\mathrm{J}(F)^{p\times p} \cong E/(E \cap \mathrm{J}(F)^{p\times p})$$

Since $E \cap \mathrm{J}(F)^{p\times p}$ is nilpotent, $E/\mathrm{J}(E) \cong \overline{E}/\mathrm{J}(\overline{E})$ holds. Thus it suffices to show that $\overline{E} \subseteq K^{p\times p}$ is local.

For $1 \leq i \leq p$ let $e_{i1}\colon g^i \otimes U \to g \otimes U$ be an isomorphism of KN-modules. For $j \in \mathbb{Z}$ we set $e_{i+jp,1} := e_{i1}$ and

$$e_{i+j,1+j} := \alpha^j e_{i1} \alpha^{-j}\colon g^{i+j} \otimes U \to g^{1+j} \otimes U.$$

We extend e_{ij} to $(U^G)_N$ by $e_{ij}(g^k \otimes U) = 0$ for $k \not\equiv i \pmod p$. For $x \in N$ and $u \in g^i \otimes U$ we have

$$\begin{aligned}(\alpha^j e_{i1}\alpha^{-j})(xu) &= \alpha^j(e_{i1}(g^{-j}xu)) = \alpha^j(e_{i1}(g^{-j}xg^j \cdot g^{-j}u)) = \alpha^j(g^{-j}xg^j e_{i1}(g^{-j}u))\\ &= xg^j e_{i1}(g^{-j}u) = x(\alpha^j e_{ij}\alpha^{-j})(u).\end{aligned}$$

This shows $e_{ij} \in \mathrm{End}_{KN}(U^p)$. Because of $\alpha^p e_{ij} = e_{ij}\alpha^p$, e_{ij} depends only on the residue classes $i + p\mathbb{Z}$ and $j + p\mathbb{Z}$. Furthermore, $\alpha e_{ij}\alpha^{-1} = e_{i+1,j+1}$ for all $i, j \in \mathbb{Z}$. Now let $1 \leq i, j \leq p$. The image $\overline{e_{ij}} \in K^{p\times p}$ of e_{ij} is 0 everywhere except at position (i, j). Therefore, every matrix $a \in K^{p\times p}$ can be uniquely written in the form $a = \sum_{i,j=1}^p a_{ij}\overline{e_{ij}}$ with $a_{ij} \in K$. Because of $\alpha a \alpha^{-1} = \sum a_{ij}e_{i+1,j+1}$, $a \in \overline{E}$ holds if and only if $a_{ij} = a_{i+1,j+1}$ for all i, j, where the indices are to be read modulo p. Let $P = (\delta_{i,j+1})_{i,j} \in K^{p\times p}$ be the permutation matrix of $(1, \ldots, p)$. Then

$$\overline{E} = \Big\{\sum_{i=1}^p \lambda_i P^i : \lambda_1, \ldots, \lambda_p \in K\Big\} \cong K[X]/(X^p - 1) = K[X]/(X - 1)^p \cong K[X]/(X)^p.$$

By Example II.12.9, $\overline{E}$ is local. □

Remark III.3.48. Green's Theorem does not hold for arbitrary fields: Since $\mathbb{F}_2$ has no primitive 3-rd root of unity, there exists a 2-dimensional simple $\mathbb{F}_2A_3$-module U. Because of $(\mathbb{F}_2A_3)^{S_3} \simeq \mathbb{F}_2S_3$, U^{S_3} is a projective-indecomposable module of dimension 4. According to Dickson, $\mathbb{F}_2S_3$ possesses only one further projective-indecomposable module. On the other hand,

$$1 = \big(1 + (1,2,3) + (1,3,2)\big) + \big(1 + (1,2) + (2,3) + (1,2,3)\big) + \big(1 + (1,2) + (2,3) + (1,3,2)\big)$$

is a decomposition into three pairwise orthogonal (primitive) idempotents (Exercise II.64). Thus U^{S_3} is decomposable.

III.4 Representations of the symmetric group

Remark III.4.1. We know from Exercise II.74 that the character table of the symmetric group S_n is integral. In this chapter, we construct the irreducible representations of S_n and provide an algorithm for determining the character table. It turns out that all representations can be realized over $\mathbb{Q}$, i. e. $\mathbb{Q}$ is a splitting field for S_n.

Definition III.4.2.

- A *partition* of $n \in \mathbb{N}$ is a sequence of natural numbers $\lambda = (\lambda_1, \ldots, \lambda_k)$ with $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k \geq 1$ and $\lambda_1 + \ldots + \lambda_k = n$. One calls λ_i the *parts* of λ. We often group identical parts in the form $(a, a, a, b, b, c, \ldots) = (a^3, b^2, c, \ldots)$. For technical reasons, we occasionally tacitly set $\lambda_{k+1} = \lambda_{k+2} = \ldots = 0$. Let the set of partitions of n be $P(n)$.
- The *lexicographical order* on $P(n)$ is defined by

$$\lambda < \mu \ :\Longleftrightarrow\ \exists k \in \mathbb{N} : \lambda_1 = \mu_1, \ldots, \lambda_{k-1} = \mu_{k-1}, \lambda_k < \mu_k.$$

- The *dominance order* on $P(n)$ is defined by

$$\lambda \trianglelefteq \mu \ :\Longleftrightarrow\ \forall k \in \mathbb{N} : \lambda_1 + \ldots + \lambda_k \leq \mu_1 + \ldots + \mu_k.$$

  As usual, we use $\leq$, $>$, $\geq$, $\lhd$, $\rhd$ and $\trianglerighteq$.

Example III.4.3. The partitions of 4 are $(1^4) < (2, 1^2) < (2^2) < (3, 1) < (4)$. In contrast to the lexicographical order, the dominance order is not total. The partitions of 6 are:

$$\begin{array}{ccccccccccccccc}
 & & & & & & (2^3) & & & & (3^2) & & & & \\
 & & & & & \rhd & & \rhd & & \rhd & & \rhd & & & \\
(1^6) & \lhd & (2,1^4) & \lhd & (2^2,1^2) & & & & (3,2,1) & & & & (4,2) & \lhd & (5,1) & \lhd & (6) \\
 & & & & & \rhd & & \rhd & & \rhd & & \rhd & & & \\
 & & & & & & (3,1^3) & & & & (4,1^2) & & & &
\end{array}$$

Lemma III.4.4. *If $\lambda \trianglelefteq \mu$ holds for $\lambda, \mu \in P(n)$, then also $\lambda \leq \mu$.*

Proof. In the case $\lambda = \mu$, the assertion is clear. So let $k \in \mathbb{N}$ be minimal with $\lambda_k \neq \mu_k$. Then

$$\lambda_k = (\lambda_1 + \ldots + \lambda_k) - (\mu_1 + \ldots + \mu_{k-1}) \leq (\mu_1 + \ldots + \mu_k) - (\mu_1 + \ldots + \mu_{k-1}) = \mu_k.$$

This shows $\lambda \leq \mu$. □

Definition III.4.5.

- The *Young diagram* Y of a partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ is an arrangement of n boxes with λ_i boxes in the i-th row (see Example III.4.6). By reflection across the diagonal, one obtains the *conjugate* Young diagram Y' corresponding to the partition $\lambda' = (\lambda'_1, \ldots, \lambda'_l)$ with $\lambda'_i := |\{j : \lambda_j \geq i\}|$ for $i = 1, \ldots, l$. Clearly $\lambda'' = \lambda$. In the case $\lambda' = \lambda$, λ is called *symmetric*.

- A (*Young*) *tableau* T is a filled Young diagram, where each of the numbers $1, \ldots, n$ is in exactly one box. By T' we denote the corresponding conjugate Young tableau (the rows of T' are the columns of T). The set of all tableaux for a partition λ is denoted by $T(\lambda)$.

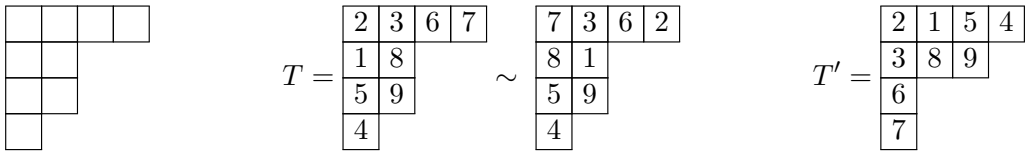
- Tableaux T, U are called equivalent (written $T \sim U$) if the numbers in each row of T and U coincide up to order. We denote the equivalence class of T by $[T]$ and let $T(\lambda)/\sim := \{[T] : T \in T(\lambda)\}$ be the set of equivalence classes.

- A tableau T with rows $T_1, \ldots, T_k$ determines a *Young subgroup*

$$S_T := \mathrm{Sym}(T_1) \times \ldots \times \mathrm{Sym}(T_k) \cong S_{\lambda_1} \times \ldots \times S_{\lambda_k}.$$

  Obviously S_T depends only on $[T]$.

Example III.4.6. The Young diagram of $\lambda = (4, 2^2, 1)$, a tableau, an equivalent tableau and the conjugate tableau are given by:



Remark III.4.7.

(i) Let T be a tableau. A canonical representative for $[T]$ is obtained by sorting the boxes in each row of T by size (ascending).

(ii) The cycle type of a permutation $\sigma \in S_n$ is obviously a partition of n. From Exercise II.74 one obtains a bijection $P(n) \to \mathrm{Cl}(S_n)$. Because of $k(S_n) = |\mathrm{Irr}(S_n)|$ we are looking for an analogous bijection $P(n) \to \mathrm{Irr}(S_n)$.

(iii) By permuting the numbers in the boxes, S_n acts on the set of all tableaux. The orbits are $T(\lambda)$ for $\lambda \in P(n)$. For a tableau T and $\sigma \in S_n$, it holds that $({}^{\sigma}T)' = {}^{\sigma}T'$. Equivalent tableaux are mapped to equivalent tableaux. Therefore, S_n also acts transitively on $T(\lambda)/\sim$. The stabilizer of an equivalence class $[T]$ is the Young subgroup S_T. In particular, $[T] = S_T T$, $|[T]| = |S_Y| = \lambda_1! \ldots \lambda_k!$ and

$$|T(\lambda)/\sim| = \frac{n!}{\lambda_1! \ldots \lambda_k!}.$$

Definition III.4.8. For $\lambda \in P(n)$ let M_λ be the $\mathbb{C}$-vector space with basis $T(\lambda)/\sim$. Through the action of S_n, M_λ becomes a $\mathbb{C}S_n$-permutation module. Let $(.,.)\colon M_\lambda \times M_\lambda \to \mathbb{C}$ be the Hermitian inner product with orthonormal basis $T(\lambda)/\sim$.

Example III.4.9. For $\lambda = (n) \in P(n)$ all tableaux are equivalent. Therefore, M_λ is the trivial module. For $\lambda = (1^n)$ the tableaux are pairwise non-equivalent and can be identified with the permutations of S_n. Then M_λ is the regular $\mathbb{C}S_n$-module. In the case $\lambda = (n, 1)$ the equivalence classes can be identified with the entry in the second row. Then $M_\lambda \simeq \mathbb{C}^n$ is the permutation module of the natural action of S_n on $\{1, \ldots, n\}$.

Definition III.4.10. For $W \subseteq S_n$ let (as before) $W^+ = \sum_{w \in W} w \in \mathbb{C}S_n$ and

$$W^- := \sum_{w \in W} \operatorname{sgn}(w) w \in \mathbb{C}S_n.$$

For $T \in T(\lambda)$ let

$$q(T) := S^-_{T'}[T] = \sum_{\sigma \in S_{T'}} \operatorname{sgn}(\sigma)[{}^\sigma T] \in M_\lambda.$$

One calls

$$Q_\lambda := \operatorname{Span}_{\mathbb{C}}\big\{q(T) : T \in T(\lambda)\big\} \leq M_\lambda$$

the *Specht module* of λ.

Remark III.4.11. For $T \in T(\lambda)$ and $\sigma \in S_n$, it holds (as for every stabilizer)

$$\begin{aligned}\sigma S_T \sigma^{-1} &= \sigma(\operatorname{Sym}(T_1) \times \ldots \times \operatorname{Sym}(T_k))\sigma^{-1} = \operatorname{Sym}({}^\sigma T_1) \times \ldots \times \operatorname{Sym}({}^\sigma T_k) \\ &= \operatorname{Sym}(({}^\sigma T)_1) \times \ldots \times \operatorname{Sym}(({}^\sigma T)_k) = S_{{}^\sigma T}.\end{aligned}$$

This shows

$$\sigma q(T) = (\sigma S_{T'} \sigma^{-1})^- \sigma[T] = S_{[{}^\sigma T']}[{}^\sigma T] = q({}^\sigma T) \in Q_\lambda.$$

Therefore, S_n indeed acts on Q_λ. Furthermore, Q_λ is generated as a $\mathbb{C}S_n$-module by any (arbitrary) $q(T)$. If one chooses a basis from the elements $q(T)$, one obtains a matrix representation $S_n \to \mathrm{GL}(d, \mathbb{Z})$, where we still have to determine $d = \dim Q_\lambda$.

Example III.4.12. Let $\lambda = (1^n)$ and $T \in T(\lambda)$. Then $S_{T'} = S_n$ and $q(T) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)[{}^\sigma T]$. For $\tau \in S_n$ it follows

$$\tau q(T) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)[{}^{\tau\sigma} T] = \sum_{\sigma \in S_n} \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)[{}^\sigma T] = \operatorname{sgn}(\tau) q(T).$$

Therefore, $Q_\lambda = \mathbb{C}q(T)$ is the module for the alternating representation. For $n = 3$, $Q_{(3)}$, $Q_{(2,1)}$ and $Q_{(1^3)}$ are representatives of the three simple $\mathbb{C}S_3$-modules.

Lemma III.4.13. *Let $\lambda, \mu \in P(n)$, $T \in T(\lambda)$ and $U \in T(\mu)$. If the numbers in each row of T lie in pairwise distinct columns of U, then $\lambda \trianglelefteq \mu$ holds.*

Proof. Let T_i and U_i be the i-th row of T and U, respectively. We can sort the entries in each column of U such that the numbers of T_1 lie in U_1. In particular, $\lambda_1 \leq \mu_1$ holds. In the same way, we can achieve that the entries of T_2 lie in $U_1 \cup U_2$. This shows $\lambda_1 + \lambda_2 \leq \mu_1 + \mu_2$ etc. (note: $\lambda_2 \leq \mu_2$ does not necessarily have to hold). □

Lemma III.4.14. *Let $\lambda \in P(n)$, $T \in T(\lambda)$ and $G \leq S_n$.*

(i) For $v, w \in M_\lambda$, $(G^- v, w) = (v, G^- w)$ holds.

(ii) If G contains the transposition (a,b), then there exists a $\gamma \in \mathbb{C}S_n$ with $G^- = \gamma(1-(a,b))$.

(iii) If a, b lie in the same row of T and $(a,b) \in G$, then $G^-[T] = 0$ holds.

Proof.

(i) For $\sigma \in G$ and $T, U \in T(\lambda)$, we have $(\sigma[T], \sigma[U]) = \delta_{[\sigma T],[\sigma U]} = \delta_{[T],[U]} = ([T],[U])$, i. e. σ operates unitarily on M_λ. It follows that

$$(G^- v, w) = \sum_{\sigma \in G} \operatorname{sgn}(\sigma)(\sigma v, w) = \sum_{\sigma \in G} \operatorname{sgn}(\sigma)(v, \sigma^{-1} w) = \sum_{\sigma \in G} \big(v, \operatorname{sgn}(\sigma^{-1})\sigma^{-1} w\big) = (v, G^- w).$$

(ii) Let $R \subseteq G$ be a system of representatives for $G/\langle (a,b) \rangle$. Then

$$G^- = \sum_{r \in R} (\operatorname{sgn}(r) r + \operatorname{sgn}(r(a,b)) r(a,b) = \sum_{r \in R} \operatorname{sgn}(r) r (1-(a,b)).$$

(iii) By assumption, $(a,b)[T] = [T]$. From (ii) it follows that $G^-[T] = \gamma([T] - (a,b)[T]) = 0$ for some $\gamma \in \mathbb{C}S_n$. □

Corollary III.4.15. *Let $\lambda, \mu \in P(n)$, $T \in T(\lambda)$ and $U \in T(\mu)$. Then*

(i) $S_{U'}^-[T] \neq 0 \Longrightarrow \lambda \trianglelefteq \mu$.

(ii) $\lambda = \mu$, $S_{U'}^-[T] \neq 0 \Longrightarrow S_{U'}^-[T] = \pm q(U)$.

(iii) $v \in M_\mu \Longrightarrow S_{U'}^- v \in \mathbb{C} q(U)$.

Proof.

(i) Let a, b be numbers from one row of T. Suppose a, b lie in the same column of U. Then $(a,b) \in S_{U'}$ and $S_{U'}^-[T] = 0$ by Lemma III.4.14. Thus a, b lie in different columns of U. From Lemma III.4.13 it follows that $\lambda \trianglelefteq \mu$.

(ii) As in (i), the entries in a row of T lie in different columns of U. As in the proof of Lemma III.4.13, there exists a $\sigma \in S_{U'}$ with $\sigma[T] = [U]$ (note $\lambda = \mu$). Now

$$S_{U'}^-[T] = (S_{U'}\sigma)^-[T] = \sum_{\tau \in S_{U'}} \operatorname{sgn}(\tau) \operatorname{sgn}(\sigma) \tau[U] = \operatorname{sgn}(\sigma) q(U).$$

(iii) For every $T \in T(\mu)$, we have $S_{U'}^-[T] \in \{0, \pm q(U)\}$ by (ii). The claim follows from this. □

Theorem III.4.16 (James' Submodule Theorem)**.** *Let $\lambda \in P(n)$ and $V \leq M_\lambda$. Then $Q_\lambda \leq V$ or $V \leq Q_\lambda^\perp$. In particular, Q_λ is simple.*

Proof. Let $T \in T(\lambda)$. First assume $S_{T'}^- V = 0$. For $v \in V$, we have $(v, q(T)) = (v, S_{T'}^-[T]) = (S_{T'}^- v, [T]) = 0$ by Lemma III.4.14. Since Q_λ is generated by $q(T)$, we have $V \leq Q_\lambda^\perp$.

Now let $S_{T'}^- V \neq 0$. By Corollary III.4.15, there exist $v \in V$ and $a \in \mathbb{C}^\times$ with $S_{T'}^- v = a q(T)$. Then $Q_\lambda = \mathbb{C}S_n q(T) = \mathbb{C}S_n a^{-1} S_{T'} v \leq V$.

For the second statement, let $V < Q_\lambda$. Then it follows that $V \leq Q_\lambda \cap Q_\lambda^\perp = 0$. Thus Q_λ is simple. □

Remark III.4.17. The Specht modules can be defined over arbitrary fields. Over fields with positive characteristic, however, it is not necessarily the case that $Q_\lambda \cap Q_\lambda^\perp = 0$. But one can show that $Q_\lambda/(Q_\lambda \cap Q_\lambda^\perp)$ is simple.

Lemma III.4.18. *Let $\lambda, \mu \in P(n)$. Then*

(i) $\operatorname{Hom}(Q_\lambda, M_\mu) \neq 0 \Longrightarrow \mu \trianglelefteq \lambda$.

(ii) $\operatorname{Hom}(Q_\lambda, M_\lambda) = \operatorname{End}(Q_\lambda) \cong \mathbb{C}$.

Proof. Let $0 \neq \varphi \in \operatorname{Hom}(Q_\lambda, M_\mu)$. Then there exists a $T \in T(\lambda)$ with $\varphi(q(T)) \neq 0$. Because $M_\lambda = Q_\lambda \oplus Q_\lambda^\perp$, φ can be extended to M_λ by defining $\varphi(Q_\lambda^\perp) = 0$. Now there exist $a_{[U]} \in \mathbb{C}$ with

$$0 \neq \varphi(q(T)) = \varphi(S_{T'}^-[T]) = S_{T'}^- \varphi([T]) = \sum_{U \in T(\mu)/\sim} a_{[U]} S_{T'}^-[U].$$

From Corollary III.4.15 one obtains $\mu \trianglelefteq \lambda$. In the case $\lambda = \mu$, $\varphi(q(T)) = bq(T) \in Q_\lambda$ holds for some $b \in \mathbb{C}^\times$ according to Corollary III.4.15. For all $\sigma \in S_n$, $\varphi(q({}^\sigma T)) = \sigma\varphi(q(T)) = b[{}^\sigma T]$. Since S_n acts transitively on $T(\lambda)$, it follows that $\varphi = b\,\mathrm{id} \in \operatorname{End}(Q_\lambda)$ and $\operatorname{End}(Q_\lambda) \cong \mathbb{C}$ (also follows from Schur's Lemma). □

Theorem III.4.19 (Frobenius-Young)**.** *Every irreducible $\mathbb{C}S_n$-module is isomorphic to exactly one Specht module.*

Proof. Since $|P(n)| = k(S_n) = |\operatorname{Irr}(S_n)|$, it suffices to show that Specht modules corresponding to different partitions $\lambda, \mu \in P(n)$ are not isomorphic. In the case $Q_\lambda \simeq Q_\mu$, it holds that $\operatorname{Hom}(Q_\lambda, M_\mu) \neq 0 \neq \operatorname{Hom}(Q_\mu, M_\lambda)$. From Lemma III.4.18 it follows that $\lambda = \mu$. □

Corollary III.4.20. *The field $\mathbb{Q}$ is a splitting field for S_n.*

Proof. According to Remark III.4.11, the Specht modules can be realized as $\mathbb{Q}$-representations. □

Corollary III.4.21. *For $\lambda \in P(n)$ we have*

$$M_\lambda = Q_\lambda \oplus \bigoplus_{\mu \rhd \lambda} m_\mu Q_\mu$$

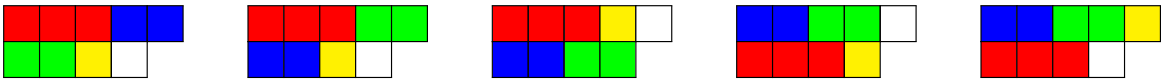
with $m_\mu \in \mathbb{N}_0$ for $\mu \rhd \lambda$.

Proof. From $Q_\mu \leq M_\lambda$ it follows that $\operatorname{Hom}(Q_\mu, M_\lambda) \neq 0$ and $\mu \trianglerighteq \lambda$ according to Lemma III.4.18. If Q_λ were to occur more than once in M_λ, then $\dim_{\mathbb{C}} \operatorname{Hom}(Q_\lambda, M_\lambda) \geq 2$ would hold, in contradiction to Lemma III.4.18. □

Definition III.4.22. For $\lambda \in P(n)$ let π_λ be the permutation character of M_λ and $\chi_\lambda \in \operatorname{Irr}(S_n)$ the character of Q_λ. For $g \in S_n$ of cycle type $\mu \in P(n)$ let $\pi_\lambda(\mu) := \pi_\lambda(g)$ and $\chi_\lambda(\mu) := \chi_\lambda(g)$ (this is well-defined according to Exercise II.74).

Theorem III.4.23. *Let $\lambda, \mu \in P(n)$. Then $\pi_\lambda(\mu)$ is the number of possibilities to distribute the rows of the Young diagram of μ onto the Young diagram of λ (see Example III.4.24).*

Example III.4.24. Let $\lambda = (5,4)$ and $\mu = (3,2^2,1^2)$. Then $\pi_\lambda(\mu) = 5$, illustrated by colored Young diagrams:



Proof of Theorem III.4.23. Let $\sigma = \sigma_1 \dots \sigma_k$ be of cycle type $\mu = (\mu_1, \dots, \mu_k)$ with disjoint cycles σ_i of length μ_i for $i = 1, \dots, k$. As is well known, $\pi_\lambda(\sigma)$ is the number of equivalence classes of tableaus $[T]$ with $[{}^\sigma T] = [T]$. This condition holds if and only if the digits of σ_i appear in one row of T for $i = 1, \dots, k$. This yields a distribution of the μ_i onto the rows of the Young diagram of λ. Since we only count equivalence classes of tableaus, the exact position of μ_i within a row is irrelevant. □

Remark III.4.25.

(i) Corollary III.4.21 and Theorem III.4.23 allow for the recursive calculation of the character table of S_n: It holds that $\chi_{(n)} = \pi_{(n)} = \mathbb{1}_{S_n}$ and

$$\boxed{\chi_\lambda = \pi_\lambda - \sum_{\mu \rhd \lambda} (\pi_\lambda, \chi_\mu)\chi_\mu.}$$

This allows χ_λ to also be expressed as an integer linear combination of the π_μ. The coefficients (π_λ, χ_μ) are called *Kostka numbers*. They are positive for all $\mu \trianglerighteq \lambda$ (without proof).

(ii) Since S_n acts transitively on $T(\lambda)/\!\sim$, it holds that $(\pi_\lambda, \mathbb{1}_{S_n}) = 1$ according to Exercise II.71. In particular, $\chi_{(n-1,1)} = \pi_{(n-1,1)} - \mathbb{1}_{S_n}$.

(iii) The equation $(\pi_\lambda, \chi_\lambda) = 1$ together with Lemma II.14.62 implies Corollary III.4.20.

(iv) Let $\mu = (\mu_1, \dots) = (1^{m_1}, \dots, n^{m_n})$ with $m_1, \dots, m_n \in \mathbb{N}_0$. A distribution of the μ_i into the rows of the Young diagram Y of λ is composed as follows: Choose $a_{ij} \in \mathbb{N}_0$ parts i and distribute them into the j-th row of Y. Then $a_{i,1} + \dots + a_{i,k} = m_i$ and $a_{1,j}1 + a_{2,j}2 + \dots + a_{n,j}n = \lambda_j$ for $i = 1, \dots, n$ and $j = 1, \dots, k$. Therefore, $\pi_\lambda(\mu)$ is the coefficient of $X_1^{\lambda_1} \dots X_k^{\lambda_k}$ in the symmetric polynomial

$$\prod_{i=1}^{n} (X_1^i + \dots + X_k^i)^{m_i} = \prod_{i=1}^{n} \sum_{a_{i1}+\dots+a_{ik}=m_i} \binom{m_i}{a_{i1}, \dots, a_{ik}} X_1^{a_{i1}} \dots X_k^{a_{ik}}.$$

Theorem III.4.26. *For $\lambda \in P(n)$, Q_λ is the unique common constituent of M_λ and $Q_{(1^n)} \otimes M_{\lambda'}$. In particular, $Q_{(1^n)} \otimes Q_\lambda \simeq Q_{\lambda'}$ and* $\boxed{\chi_{\lambda'} = \operatorname{sgn} \cdot \chi_\lambda.}$

Proof. Let $T \in T(\lambda)$. The permutation character π_λ of M_λ is, according to Example III.3.31, the induction of the trivial character $\mathbb{1}_{S_T}$. According to Example III.4.12, $Q_{(1^n)}$ is the module of the alternating representation with character sgn. According to Lemma III.3.34, it holds that $\operatorname{sgn} \cdot (\mathbb{1}_{S_{T'}})^{S_n} = (\operatorname{sgn}_{S_{T'}})^{S_n}$. This shows

$$(\chi_\lambda, \operatorname{sgn} \pi_{\lambda'}) = (\chi_\lambda, \operatorname{sgn}(\mathbb{1}_{S_{T'}})^{S_n}) = (\chi_\lambda, (\operatorname{sgn}_{S_{T'}})^{S_n}) \overset{\text{III.3.33}}{=} ((\chi_\lambda)_{S_{T'}}, \operatorname{sgn}_{S_{T'}}).$$

We can extend $q(T)$ to a basis of Q_λ. For $\sigma \in S_{T'}$, we have $\sigma q(T) = \operatorname{sgn}(\sigma) q(T)$. Therefore, $\operatorname{sgn}_{S_{T'}}$ is an irreducible constituent of $(\chi_\lambda)_{S_{T'}}$ and χ_λ is a constituent of $\operatorname{sgn}\pi_{\lambda'}$. For uniqueness, it suffices to show $(\pi_\lambda, \operatorname{sgn}\pi_{\lambda'}) = 1$. According to the Mackey formula, it holds that

$$\begin{aligned}(\pi_\lambda, \operatorname{sgn}\pi_{\lambda'}) &= (\mathbb{1}_{S_T}^{S_n}, (\operatorname{sgn}_{S_{T'}})^{S_n}) = ((\mathbb{1}_{S_T}^{S_n})_{S_{T'}}, \operatorname{sgn}_{S_{T'}}) \\ &= \sum_{S_{T'}\sigma S_T \in S_{T'}\backslash S_n / S_T} (\mathbb{1}_{D_\sigma}^{S_{T'}}, \operatorname{sgn}_{S_{T'}}) = \sum_{S_{T'}\sigma S_T \in S_{T'}\backslash S_n / S_T} (\mathbb{1}_{D_\sigma}, \operatorname{sgn}_{D_\sigma}) \qquad \text{(III.4.1)}\end{aligned}$$

with $D_\sigma := S_{T'} \cap \sigma S_T \sigma^{-1} = S_{T'} \cap S_{\sigma T}$. Let $(\mathbb{1}_{D_\sigma}, \operatorname{sgn}_{D_\sigma}) > 0$ for some $\sigma \in S_n$. Suppose there exist numbers a, b that lie in the same row of ${}^\sigma T$ and in the same column of T. Then the transposition (a, b) lies in D_σ and one obtains the contradiction $\mathbb{1}_{D_\sigma} \neq \operatorname{sgn}_{D_\sigma}$. Therefore, the numbers of a row of ${}^\sigma T$ are distributed over pairwise distinct columns of T. In particular, there exists a $\tau_1 \in S_{T'}$ such that the first rows of ${}^\sigma T$ and ${}^{\tau_1} T$ coincide as sets. Analogously, one finds a $\tau_2 \in S_{T'}$ such that the first two rows of ${}^\sigma T$ and ${}^{\tau_2\tau_1} T$ coincide, and so on. Finally, there exists a $\tau \in S_{T'}$ with ${}^\sigma T \sim {}^\tau T$, i. e. $\tau^{-1}\sigma \in S_T$ and $S_{T'}\sigma S_T = S_{T'} S_T$. Thus, one can assume $\sigma = 1$ in (III.4.1). Conversely, then $D_\sigma = 1$ and $(\mathbb{1}_{D_\sigma}, \operatorname{sgn}_{D_\sigma}) = 1$. From this, the first assertion follows.

For the second assertion, we observe that $\operatorname{sgn}\chi_\lambda$ and $\chi_{\lambda'}$ are common irreducible constituents of $\operatorname{sgn}\pi_\lambda = \operatorname{sgn}\pi_{\lambda''}$ and $\operatorname{sgn}^2 \pi_{\lambda'} = \pi_{\lambda'}$. According to the first part of the proof, they must be equal. □

Remark III.4.27. The decomposition of $Q_\lambda \otimes Q_\mu$ for $\lambda, \mu \in P(n)$ into simple modules is in general an open problem. The occurring multiplicities are called *Kronecker coefficients*.

Example III.4.28. Let $n = 5$. The partitions of 5 are $(5) \rhd (4,1) \rhd (3,2) \rhd (3,1^2) \rhd (2^2,1) \rhd (2,1^3) \rhd (1^5)$. Because of Theorem III.4.26 we only need to calculate π_λ for three partitions:

σ	(1^5)	$(2,1^3)$	$(2^2,1)$	$(3,1^2)$	$(3,2)$	$(4,1)$	(5)
$\lvert S_5 : \mathrm{C}_{S_5}(\sigma)\rvert$	1	10	15	20	20	30	24
$\pi_{(4,1)}$	5	3	1	2	0	1	0
$\pi_{(3,2)}$	10	4	2	1	1	0	0
$\pi_{(3,1^2)}$	20	6	0	2	0	0	0

The second row contains the lengths of the conjugacy classes. From Remark III.4.25 it follows that $\chi_{(4,1)} = \pi_{(4,1)} - \mathbb{1}_{S_5}$. Furthermore $(\pi_{(3,2)}, \chi_{(4,1)})_{S_5} = 1$ and $\chi_{(3,2)} = \pi_{(3,2)} - 1_{S_n} - \chi_{(4,1)}$. Finally $(\pi_{(3,1^2)}, \chi_{(3,2)})_{S_5} = 1$ and $(\pi_{(3,1^2)}, \chi_{(4,1)})_{S_5} = 2$. Thus $\chi_{(3,1^2)} = \varphi_{(3,1^2)} - 1_{S_5} - \chi_{(3,2)} - 2\chi_{(4,1)}$.

S_5	(1^5)	$(2,1^3)$	$(2^2,1)$	$(3,1^2)$	$(3,2)$	$(4,1)$	(5)
(5)	1	1	1	1	1	1	1
$(4,1)$	4	2	0	1	−1	0	−1
$(3,2)$	5	1	1	−1	1	−1	0
$(3,1^2)$	6	0	−2	0	0	0	1
$(2^2,1)$	5	−1	1	−1	−1	1	0
$(2,1^3)$	4	−2	0	1	1	0	−1
(1^5)	1	−1	1	1	−1	−1	1

Remark III.4.29. Next, we construct a canonical basis of Q_λ consisting of $q(T)$ for certain $T \in T(\lambda)$. Because of $q({}^\sigma T) = \operatorname{sgn}(\sigma) q(T)$ for $\sigma \in S_{T'}$, one only needs those T whose columns are sorted (in ascending order).

Definition III.4.30. A tableau T is called a *standard tableau*, if the digits in the rows and columns of T are each sorted in ascending order. Let $ST(\lambda)$ be the set of standard tableaux for the partition λ.

Example III.4.31. For every partition $\lambda \in P(n)$ there exists at least one standard tableau; for example, one can distribute the numbers $1, \ldots, n$ from left to right and from top to bottom into the boxes. In the case $\lambda \in \{(n), (1^n)\}$, this is the only possibility. In general, the number 1 is always at the top left. For $\lambda = (3^2)$ there are five standard tableaux:

1	2	3
4	5	6

1	2	4
3	5	6

1	2	5
3	4	6

1	3	4
2	5	6

1	3	5
2	4	6

Each equivalence class of tableaux contains at most one standard tableau.

Definition III.4.32.

- A *composition* of $n \in \mathbb{N}$ is a sequence $\lambda = (\lambda_1, \lambda_2, \ldots) \in \mathbb{N}_0^\infty$ with $\sum_{i=1}^\infty \lambda_i = n$. Let $K(n)$ be the set of all compositions of n. The *dominance order* for partitions carries over to compositions.
- For a tableau T and $k \in \mathbb{N}$, we define the composition $\lambda_T^{(k)} := (\lambda_1, \ldots)$, where λ_i is the number of integers $\leq k$ in the i-th row of T. Obviously, $\lambda_T^{(k)}$ depends only on $[T]$.
- For tableaux $T, U \in T(\lambda)$, let

$$[T] \trianglelefteq [U] \iff \lambda_T^{(k)} \trianglelefteq \mu_T^{(k)} \text{ for } k = 1, \ldots, n.$$

Example III.4.33. For

$$T = \begin{array}{|c|c|c|}\hline 3 & 4 & 7 \\ \hline 2 & 5 & 8 \\ \hline 1 & 6 \\ \cline{1-2} 9 \\ \cline{1-1} \end{array}$$

is

$\lambda_T^{(1)}$	$\lambda_T^{(2)}$	$\lambda_T^{(3)}$	$\lambda_T^{(4)}$	$\lambda_T^{(5)}$	$\lambda_T^{(6)}$	$\lambda_T^{(7)}$	$\lambda_T^{(8)}$	$\lambda_T^{(9)}$
$(0,0,1)$	$(0,1,1)$	$(1,1,1)$	$(2,1,1)$	$(2,2,1)$	$(2,2,2)$	$(3,2,2)$	$(3,3,2)$	$(3,3,2,1)$

Remark III.4.34. In contrast to partitions, compositions are not necessarily sorted in descending order. Due to the possibility $\lambda_i = 0$, there are therefore always infinitely many compositions of n. It is easy to check that $\trianglelefteq$ is an order relation on $K(n)$ and $T(\lambda)/\!\sim$.

Lemma III.4.35. *Let $T \in T(\lambda)$ and $k < l$, such that k appears in row s and l in row t of T with $s > t$. For the transposition $\sigma = (k, l) \in S_n$, it then holds that $[T] \trianglelefteq [{}^\sigma T]$.*

Proof. Let $U = {}^\sigma T$. For $i < k$ and $i \geq l$, certainly $\lambda_T^{(i)} = \lambda_U^{(i)}$ holds. So let $k \leq i < l$. Then $\lambda_U^{(i)}$ is obtained from $\lambda_T^{(i)} = (\lambda_1, \ldots)$ by decreasing λ_s by 1 and increasing λ_t by 1. Because of $s > t$, the claim follows. □

Lemma III.4.36. *For $T \in ST(\lambda)$ and $\sigma \in S_{T'}$, it holds that $[{}^\sigma T] \trianglelefteq [T]$.*

Proof. Wlog. let $\sigma \neq 1$. Since the columns of T are sorted, there exists a pair (k,l) as in Lemma III.4.35. Thus, one can replace σ by $(k,l)\sigma$. This reduces the number of pairs (k,l). After finitely many repetitions, one reaches $\sigma = 1$. □

Theorem III.4.37. *Let $\lambda \in P(n)$. Then $\{q(T) : T \in ST(\lambda)\}$ is linearly independent.*

Proof. Let $ST(\lambda) = \{T_1, \ldots, T_k\}$ with $[T_1] \rhd \ldots \rhd [T_k]$. Let $a_1, \ldots, a_k \in \mathbb{C}$ with $a_1 q(T_1) + \ldots + a_k q(T_k) = 0$. In the case $a_1 \neq 0$, $[T_1]$ must appear as a summand of a $q(T_i)$ with $i > 1$. Then there exists a $\sigma \in S_{T_i'}$ with $T_1 = {}^{\sigma}T_i$ and Lemma III.4.36 yields the contradiction $[T_1] \lhd [T_i]$. Thus $a_1 = 0$. One can now repeat the argument with a_2. In the end, $a_1 = \ldots = a_k = 0$. □

Definition III.4.38. Let $T = (t_{ij}) \in T(\lambda) \setminus ST(\lambda)$ with columns sorted in ascending order. Then there exist i, j with $t_{i,j} > t_{i,j+1}$. Let $A := \{t_{i,j}, t_{i+1,j}, \ldots, t_{l,j}\}$ and $B := \{t_{1,j+1}, t_{2,j+1}, \ldots, t_{i,j+1}\}$, where l is the length of the j-th column of T. Let $G_{i,j}$ be the set of permutations $\pi \in \mathrm{Sym}(A \cup B) \leq S_n$ such that the columns of ${}^{\pi}T$ are sorted in ascending order. One calls $G_{i,j}^- \in \mathbb{C}S_n$ the Garnir-*element* of T with respect to (i,j).

Remark III.4.39. For every subset $A' \subseteq A \cup B$ with $|A'| = |A|$ there is exactly one $\pi \in G_{i,j}$ with $\pi(A) = A'$. Therefore

$$|G_{i,j}| = \binom{|A \cup B|}{|A|} = \frac{(|A| + |B|)!}{|A|!|B|!}.$$

In fact, $G_{i,j}$ is a system of representatives for the left cosets of $\mathrm{Sym}(A) \times \mathrm{Sym}(B)$ in $\mathrm{Sym}(A \cup B)$.

Example III.4.40. Let

$$T = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 5 & 4 \\ \cline{1-2} 6 & 7 \\ \cline{1-2}\end{array}$$

with $(i,j) = (2,1)$, $A = \{5,6\}$ and $B = \{2,4\}$. Then $G_{i,j}$ consists of the following permutations:

π	1	$(4,5)$	$(4,6,5)$	$(2,4,5)$	$(2,4,6,5)$	$(2,5)(4,6)$
${}^{\pi}T$	$\begin{array}{\|c\|c\|c\|}\hline 1 & 2 & 3 \\ \hline 5 & 4 \\ \cline{1-2} 6 & 7 \\ \cline{1-2}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1 & 2 & 3 \\ \hline 4 & 5 \\ \cline{1-2} 6 & 7 \\ \cline{1-2}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1 & 2 & 3 \\ \hline 4 & 6 \\ \cline{1-2} 5 & 7 \\ \cline{1-2}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1 & 4 & 3 \\ \hline 2 & 5 \\ \cline{1-2} 6 & 7 \\ \cline{1-2}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1 & 4 & 3 \\ \hline 2 & 6 \\ \cline{1-2} 5 & 7 \\ \cline{1-2}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1 & 5 & 3 \\ \hline 2 & 6 \\ \cline{1-2} 4 & 7 \\ \cline{1-2}\end{array}$

Lemma III.4.41. *With the notation from Definition III.4.38, $G_{i,j}^- q(T) = 0$ holds.*

Proof. For abbreviation, let $S(A) := \mathrm{Sym}(A)$, $S(B) := \mathrm{Sym}(B)$ and $S(AB) := \mathrm{Sym}(A \cup B)$. Let $\sigma \in S_{T'}$. Then A and B are subsets of the j-th and $(j+1)$-th column of ${}^{\sigma}T$, respectively. Since $|A| + |B|$ is 1 greater than the length of the j-th column, there exist distinct $x, y \in A \cup B$ that stand in the same row of ${}^{\sigma}T$. Due to the transposition $\sigma = (x,y) \in S(AB)$, it follows that $S(AB)^-[{}^{\sigma}T] = 0$ according to Lemma III.4.14. The sum over $\sigma \in S_{T'}$ yields $S(AB)^- q(T) = 0$.

According to Remark III.4.39, $S(AB) = \bigcup_{\pi \in G_{i,j}} \pi S(A)S(B)$. For $\sigma \in S(A)S(B) \leq S_{T'}$, it holds that $\sigma q(T) = \mathrm{sgn}(\sigma) q(T)$. This shows $(S(A)S(B))^- q(T) = |A|!|B|! q(T)$. In total,

$$G_{i,j}^- q(T) = \frac{1}{|A|!|B|!} \sum_{\pi \in G_{i,j}} \mathrm{sgn}(\pi) \pi (S(A)S(B))^- q(T) = \frac{1}{|A|!|B|!} S(AB)^- q(T) = 0.$$ □

Theorem III.4.42 (Specht). *Let $\lambda \in P(n)$. Then $\{q(T) : T \in ST(\lambda)\}$ is a basis of Q_λ. In particular, $\chi_\lambda(1) = \dim Q_\lambda = |ST(\lambda)|$.*

Proof (Peel). Let $T = (t_{ij}) \in T(\lambda) \setminus ST(\lambda)$. According to Theorem III.4.37, it suffices to write $q(T)$ as a linear combination of the $q(U)$ with $U \in ST(\lambda)$. Because of $q({}^\sigma T) = \operatorname{sgn}(\sigma) q(T)$ for $\sigma \in S_{T'}$, we can assume that T has columns sorted in ascending order. We argue by induction on the dual dominance order on $T(\lambda)$, which is defined by $T \trianglelefteq' U \iff [T'] \trianglelefteq [U']$. One realizes that the largest element with respect to $\trianglelefteq'$ is given by the standard tableau T_0 whose boxes are numbered column-wise ascending from left to right and from top to bottom. Example:

$$T_0 = \begin{array}{|c|c|c|}\hline 1 & 5 & 8 \\ \hline 2 & 6 & 9 \\ \hline 3 & 7 \\ \cline{1-2} 4 \\ \cline{1-1} \end{array} \longrightarrow \begin{array}{cccccccc} \lambda^{(1)}_{T_0'} & \lambda^{(2)}_{T_0'} & \lambda^{(3)}_{T_0'} & \lambda^{(4)}_{T_0'} & \lambda^{(5)}_{T_0'} & \cdots & \lambda^{(9)}_{T_0'} \\ \hline (1) & (2) & (3) & (4) & (4,1) & \cdots & (4,3,2) \end{array}$$

Because $T \notin ST(\lambda)$, we have $T \lhd' T_0$. Therefore, there exist (i,j) as in Definition III.4.38. By assumption,

$$t_{1,j+1} < t_{2,j+1} < \ldots < t_{i,j+1} < t_{i,j} < t_{i+1,j} < \ldots < t_{l,j}.$$

For $\pi \in G_{i,j} \setminus \{1\}$, it follows that ${}^\pi T \rhd' T$ (cf. Lemma III.4.35). By induction, the $q({}^\pi T)$ can already be written as a linear combination of standard tableaux. According to Lemma III.4.41,

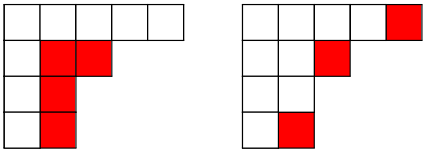
$$q(T) = q(T) - G^-_{i,j} q(T) = - \sum_{\pi \in G_{i,j} \setminus \{1\}} \operatorname{sgn}(\pi) q({}^\pi T). \qquad \square$$

Definition III.4.43. Let Y be a Young diagram of $\lambda \in P(n)$. The *hook* of Y at position (s,t) is the set of boxes

$$H_{st} := \big\{(s,j) : j \geq t\big\} \cup \big\{(i,t) : i \geq s\big\}$$

in Y. Let $h_{st} := |H_{st}| = \lambda_s + \lambda'_t - s - t + 1$ be the *length* of the hook. We call the box at position (s,t) a *corner* of Y if $h_{st} = 1$ holds (i. e. $\lambda_s = s$ and $\lambda'_t = t$). By removing this corner, one obtains a Young diagram of a partition $\mu \in P(n-1)$. Let $\lambda^- \subseteq P(n-1)$ be the set of all μ that arise by removing a corner. Analogously, let $\lambda^+ := \{\mu \in P(n+1) : \lambda \in \mu^-\} \subseteq P(n+1)$.

Example III.4.44. The hook $H_{2,2}$ with length 4 and the corners $(1,5)$, $(2,3)$ and $(4,2)$ in $\lambda = (5,3,2^2)$ are marked in red:



It holds that $\lambda^- = \big\{(4,3,2^2), (5,2^3), (5,3,2,1)\big\}$ and $\lambda^+ = \big\{(6,3,2^2), (5,4,2^2), (5,3^2,2)\big\}$.

Theorem III.4.45 (Branching rule). *For $\lambda \in P(n)$ it holds that*

$$(Q_\lambda)_{S_{n-1}} = \bigoplus_{\mu \in \lambda^-} Q_\mu \qquad (n \geq 2),$$
$$(Q_\lambda)^{S_{n+1}} = \bigoplus_{\mu \in \lambda^+} Q_\mu.$$

Proof. Let $e_1, \ldots, e_k$ be the corners of the Young diagram associated to λ. Let $\lambda^- = \{\mu_1, \ldots, \mu_k\}$, where μ_i is obtained by removing e_i. If n is in a corner e_i of $T \in T(\lambda)$, then by removing n one obtains a tableau $T_i \in T(\mu_i)$. We consider the linear map $\varphi_i \colon M_\lambda \to M_{\mu_i}$ with

$$\varphi_i([T]) := \begin{cases} [T_i] & \text{if } n \text{ lies in } e_i, \\ 0 & \text{otherwise,} \end{cases}$$

where we can assume that $T \in T(\lambda)$ has rows sorted in increasing order. For $\sigma \in S_{n-1}$ it clearly holds that $\varphi_i([{}^\sigma T]) = {}^\sigma \varphi_i([T])$, i. e. φ_i is a homomorphism of $\mathbb{C}S_{n-1}$-modules.

In every standard tableau, n clearly stands at one of the corners. Let

$$Q_i := \operatorname{Span}_{\mathbb{C}}\big\{q(T) : T \in ST(\lambda) \text{ with } n \text{ in corner } e_j \text{ where } j \leq i\big\}$$

for $i = 0, \ldots, k$. For $\sigma \in S_{n-1}$ and $q(T) \in Q_i$ it holds that $\sigma q(T) = q({}^\sigma T) \in Q_i$ according to Remark III.4.11, i. e. Q_i is a $\mathbb{C}S_{n-1}$-module. According to Specht, $0 = Q_0 \leq Q_1 \leq \ldots \leq Q_k = Q_\lambda$. Furthermore, $\varphi_i(Q_i) = Q_{\mu_i}$ with $Q_{i-1} \leq \operatorname{Ker}(\varphi_i)$. Since every standard tableau of λ is obtained by appending n to a standard tableau of some μ_i, it holds that

$$\begin{aligned} \dim Q_\lambda &= \sum_{i=1}^{k} \dim(Q_i/Q_{i-1}) \geq \sum_{i=1}^{k} \dim(Q_i/(Q_i \cap \operatorname{Ker}(\varphi_i))) = \sum_{i=1}^{k} \dim Q_{\mu_i} \\ &= \sum_{i=1}^{k} |ST(\mu_i)| = |ST(\lambda)| = \dim Q_\lambda. \end{aligned}$$

This shows $Q_i/Q_{i-1} = Q_i/(Q_i \cap \operatorname{Ker}(\varphi_i)) \cong \varphi_i(Q_i) \cong Q_{\mu_i}$ for $i = 1, \ldots, k$. From this follows the first claim. For the second claim let $\mu \in P(n+1)$. By Frobenius reciprocity it holds that

$$(\chi_\lambda^{S_{n+1}}, \chi_\mu) = (\chi_\lambda, (\chi_\mu)_{S_n}) = \sum_{\nu \in \mu^-} (\chi_\lambda, \chi_\nu) = \begin{cases} 1 & \text{if } \mu \in \nu^+ = \lambda^+, \\ 0 & \text{otherwise.} \end{cases} \quad \square$$

Remark III.4.46. In order to derive a handy formula for $\chi_\lambda(1)$, we need an identity of polynomials. A polynomial $\alpha \in K[X_1, \ldots, X_n]$ is called *homogeneous* (of degree d), if every monomial in α has the same degree (d). Products of homogeneous polynomials are again homogeneous, where the degrees add up. Clearly, the elementary symmetric polynomials are homogeneous.

Lemma III.4.47. *Let* $\Delta := \prod_{1 \leq i < j \leq m} (X_i - X_j) \in \mathbb{Q}[X_1, \ldots, X_m]$ *and*

$$\alpha := \sum_{i=1}^{m} X_i \Delta(X_1, \ldots, X_i + Y, \ldots, X_m) \in \mathbb{Q}[X_1, \ldots, X_m, Y].$$

Then it holds that

$$\alpha = \Big(X_1 + \ldots + X_m + \binom{m}{2} Y\Big)\Delta.$$

Proof. Let $i < j$ and $i \neq k \neq j$. Swapping i and j changes the sign of Δ (see proof of Theorem I.3.26). Thus $X_k \Delta(\ldots, X_k + Y, \ldots)$ also changes sign. By swapping i and j, the summands $X_i \Delta(\ldots, X_i + Y, \ldots)$ and $X_j \Delta(\ldots, X_j + Y, \ldots)$ are furthermore swapped and they additionally change their sign. Overall, α changes sign when swapping i and j. If one sets $X_i = X_j$, then $\alpha = 0$. As a polynomial in X_i, α therefore has the root X_j. One can thus split off the factor $X_i - X_j$ in the polynomial ring

$\mathbb{Q}(X_1,\dots,X_{i-1},X_{i+1},\dots,X_m)[X_i]$. Since $X_i - X_j$ is monic, no denominators occur during division. Therefore $X_i - X_j$ is a divisor of α in the factorial ring $\mathbb{Q}[X_1,\dots,X_m]$. Since the factors $X_i - X_j$ of Δ are irreducible and pairwise non-associated, α is also divisible by Δ. So let $\alpha = \beta\Delta$. Since α and Δ are homogeneous, β is homogeneous of degree 1. Since the statement holds for $Y = 0$, it follows that $\beta = X_1 + \ldots + X_m + cY$ for some $c \in \mathbb{Q}$. One obtains c by differentiating with respect to Y and then setting $Y = 0$. It holds that

$$\big(X_i\Delta(X_1,\dots,X_i+Y,\dots,X_m)\big)'(0) = X_i\Big(\sum_{j>i}\frac{\Delta}{X_i-X_j} - \sum_{j<i}\frac{\Delta}{X_j-X_i}\Big) = X_i\Delta\sum_{j\neq i}\frac{1}{X_i-X_j}$$

$$c = \sum_{i=1}^{m}\sum_{j\neq i}\frac{X_i}{X_i-X_j} = \sum_{i<j}\frac{X_i-X_j}{X_i-X_j} = \binom{m}{2}. \qquad \square$$

Remark III.4.48. For every partition λ let $f(\lambda) := |ST(\lambda)|$ (we allow here the partition (0) with the "empty" tableau). If $\lambda \in \mathbb{N}_0^m$ is an arbitrary sequence but not a partition, we set $f(\lambda) := 0$. Then f is uniquely determined by the recursion from the branching rule:

$$f(0) = 1, \tag{III.4.2}$$

$$f(\lambda_1,\dots,\lambda_m,0) = f(\lambda_1,\dots,\lambda_m) \qquad (\lambda \in \mathbb{N}_0^m), \tag{III.4.3}$$

$$f(\lambda_1,\dots,\lambda_m) = 0 \qquad (\exists i : \lambda_i + 1 = \lambda_{i+1}), \tag{III.4.4}$$

$$f(\lambda_1,\dots,\lambda_m) = f(\lambda_1-1,\lambda_2,\dots,\lambda_m) + \ldots + f(\lambda_1,\dots,\lambda_{m-1},\lambda_m-1) \qquad (\lambda_1 \geq \ldots \geq \lambda_m \geq 1). \tag{III.4.5}$$

Theorem III.4.49 (Hook length formula)**.** *For $\lambda \in P(n)$ with Young diagram Y it holds that*

$$\boxed{\chi_\lambda(1) = \dim Q_\lambda = |ST(\lambda)| = \frac{n!}{\prod\limits_{(s,t)\in Y} h_{st}}.} \tag{III.4.6}$$

Proof (Glass-Ng). Let $\lambda = (\lambda_1,\dots,\lambda_m)$. It suffices to show that the right-hand side of (III.4.6) satisfies the same recursion rule as the function f from Remark III.4.48. The product of the hook lengths in the k-th row of λ is (read from right to left):

$$\begin{gathered}[1\cdot 2\cdot\ldots\cdot(\lambda_k-\lambda_{k+1})][(\lambda_k-\lambda_{k+1}+2)\ldots(\lambda_k-\lambda_{k+2}+1)]\\ [(\lambda_k-\lambda_{k+2}+3)\ldots(\lambda_k-\lambda_{k+3}+2)]\ldots[(\lambda_k-\lambda_m+m-k+1)\ldots(\lambda_k+m-k)]\\ = \frac{(\lambda_k+m-k)!}{\prod_{l>k}(\lambda_k-\lambda_l-k+l)}.\end{gathered}$$

The right-hand side of (III.4.6) is therefore

$$g(\lambda) := n!\frac{\prod_{i<j}(\lambda_i-\lambda_j+j-i)}{\prod_{i=1}^m(\lambda_i+m-i)!} = \Big(\sum_{i=1}^m\lambda_i\Big)!\frac{\Delta(\lambda_1+m-1,\lambda_2+m-2,\dots,\lambda_m)}{\prod_{i=1}^m(\lambda_i+m-i)!}.$$

One easily sees that (III.4.2) holds for g. For $\lambda_m = 0$ we have

$$\begin{aligned}g(\lambda) &= n!\frac{\Delta(\lambda_1+m-1,\lambda_2+m-2,\dots,\lambda_{m-1}+1)\prod_{i=1}^{m-1}(\lambda_i+m-i)}{\prod_{i=1}^{m-1}(\lambda_i+m-i)!}\\ &= n!\frac{\Delta(\lambda_1+m-2,\lambda_2+m-3,\dots,\lambda_{m-1})}{\prod_{i=1}^{m-1}(\lambda_i+m-i-1)!} = g(\lambda_1,\dots,\lambda_{m-1}),\end{aligned}$$

i. e. (III.4.3) holds. For $\lambda_i + 1 = \lambda_{i+1}$ we have $\lambda_i + m - i = \lambda_{i+1} + m - (i+1)$ and with Δ also $g(\lambda)$ vanishes, i. e. (III.4.4) holds. Finally, we substitute $X_i := \lambda_i + m - i$ for $i = 1, \ldots, m$ and $Y = -1$ in Lemma III.4.47. Then on the one hand

$$\begin{aligned}\alpha &= \sum_{i=1}^{m} (\lambda_i + m - i)\Delta(\lambda_1 + m - 1, \ldots, \lambda_i + m - i - 1, \ldots, \lambda_m) \\ &= \frac{1}{(n-1)!} \prod_{i=1}^{m} (\lambda_i + m - i)! \sum_{i=1}^{m} g(\lambda_1, \ldots, \lambda_i - 1, \ldots, \lambda_m)\end{aligned}$$

and on the other hand

$$\begin{aligned}\alpha &= \Big(\sum_{i=1}^{m} (\lambda_i + m - i) - \binom{m}{2}\Big)\Delta(\lambda_1 + m - 1, \ldots, \lambda_m) = n\Delta(\lambda_1 + m - 1, \ldots, \lambda_m) \\ &= \frac{1}{(n-1)!} \prod_{i=1}^{m} (\lambda_i + m - i)! g(\lambda).\end{aligned}$$

Thus (III.4.5) also follows. □

Example III.4.50. We consider $\lambda = (4, 2^2, 1)$ and write the hook lengths into the Young diagram:

7	5	2	1
4	2		
3	1		
1			

One calculates

$$\chi_\lambda(1) = \frac{9!}{7 \cdot 5 \cdot 4 \cdot 3 \cdot 2^2} = 9 \cdot 8 \cdot 3 = 6^3 = 216.$$

Remark III.4.51. With the characters of S_n, powers of characters of arbitrary groups can be decomposed into smaller components. For this purpose, let G and H be general finite groups with representations $\Delta\colon G \to \mathrm{GL}(V)$ and $\Gamma\colon H \to \mathrm{GL}(V)$ on the same $\mathbb{C}$-vector space V, such that

$$\Delta(g)\Gamma(h) = \Gamma(h)\Delta(g) \qquad \forall g \in G, h \in H$$

holds. We can interpret $\Delta\Gamma$ as a representation of $G \times H$. Let $\Gamma = \bigoplus_{i=1}^{k} a_i\Gamma_i$ with pairwise non-similar irreducible representations $\Gamma_1, \ldots, \Gamma_k$ and $a_1, \ldots, a_k \in \mathbb{N}$. Let d_i be the degree of Γ_i. Then $\dim V = a_1d_1 + \ldots + a_kd_k$ holds. We write $\Delta(g)$ as a block matrix $\Delta(g) = (\Delta_{ij}(g))$ with $\Delta_{ij}(g) \in \mathbb{C}^{a_id_i \times a_jd_j}$. Each block can be further decomposed as $\Delta_{ij}(g) = (\Delta_{ij}^{st}(g))_{s,t}$ with $\Delta_{ij}^{st}(g) \in \mathbb{C}^{d_i \times d_j}$ for $s = 1, \ldots, a_i$ and $t = 1, \ldots, a_j$. From $\Delta(g)\Gamma(h) = \Gamma(h)\Delta(g)$ it follows that

$$\Delta_{ij}^{st}(g)\Gamma_j(h) = \Gamma_i(h)\Delta_{ij}^{st}(g) \qquad \forall g \in G, h \in H.$$

With Exercise II.70 it follows that $\Delta_{ij}(g) = 0$ for $i \neq j$ and $\Delta_{ii}^{st}(g) = \lambda_{ist}(g)1_{d_i}$ with $\lambda_{ist}(g) \in \mathbb{C}$. Thus, it holds that

$$\Delta(g)\Gamma(h) = \begin{pmatrix} \lambda_{1,1,1}(g)\Gamma_1(h) & & & & * \\ & \ddots & & & \\ & & \lambda_{1,a_1,a_1}\Gamma_1(h) & & \\ & & & \ddots & \\ * & & & & \lambda_{k,a_k,a_k}\Gamma_k(h) \end{pmatrix}.$$

Let $\Lambda_i(g) := (\lambda_{ist}(g))_{s,t} \in \mathbb{C}^{a_i \times a_i}$. Then there exists a permutation matrix T with

$$T\Delta(g)T^{-1} = \operatorname{diag}\big(\underbrace{\Lambda_1(g), \ldots, \Lambda_1(g)}_{d_1}, \ldots, \underbrace{\Lambda_k(g), \ldots, \Lambda_k(g)}_{d_k}\big).$$

Thus $\Lambda_1, \ldots, \Lambda_k$ are (not necessarily irreducible) representations of G and Δ is similar to $\bigoplus_{i=1}^k d_i\Lambda_i$. The degree and multiplicity of Γ_i and Λ_i behave inversely to each other. For the corresponding characters, it holds that

$$\chi_{\Delta\Gamma}(g,h) = \operatorname{tr}\big(\Delta(g)\Gamma(h)\big) = \sum_{i=1}^{k} \operatorname{tr}(\Gamma_i(h)) \sum_{s=1}^{a_i} \lambda_{iss} = \sum_{i=1}^{k} \chi_{\Gamma_i}(h) \operatorname{tr}(\Lambda_i(g)) = \sum_{i=1}^{k} \chi_{\Lambda_i}(g)\chi_{\Gamma_i}(h) \quad \text{(III.4.7)}$$

for $g \in G$ and $h \in H$.

Theorem III.4.52. *Let χ be a character of G and λ a character of $H \leq S_n$. For $h \in H$, let $c_i(h)$ be the number of i-cycles of h. Then G possesses a character (or the zero map) θ_λ with*

$$\boxed{\theta_\lambda(g) = \frac{1}{|H|} \sum_{h \in H} \lambda(h) \prod_{i=1}^{n} \chi(g^i)^{c_i(h)}} \qquad (g \in G)$$

$$\chi^n = \sum_{\lambda \in \operatorname{Irr}(H)} \lambda(1)\theta_\lambda.$$

Proof. Since the framed formula is linear in λ, we can assume $\lambda \in \operatorname{Irr}(H)$. Let W be a $\mathbb{C}G$-module for χ and $V := W \otimes \ldots \otimes W$ with n factors. Let Ψ be a representation for W and $\Delta := \Psi \otimes \ldots \otimes \Psi$ the diagonal representation on V, i. e.

$$\Delta(g)(v_1 \otimes \ldots \otimes v_n) = \Psi(v_1) \otimes \ldots \otimes \Psi(v_n)$$

for $g \in G$ and $v_1 \otimes \ldots \otimes v_n \in V$. Finally, let $\Gamma\colon H \to \mathrm{GL}(V)$ be the representation with

$$\Gamma(h)(v_1 \otimes \ldots \otimes v_n) := v_{h^{-1}(1)} \otimes \ldots \otimes v_{h^{-1}(n)}$$

(Exercise III.14). Obviously, $\Delta(g)\Gamma(h) = \Gamma(h)\Delta(g)$ holds for all $g \in G$ and $h \in H$. We can therefore apply Remark III.4.51. Each irreducible component Γ_i of Γ corresponds to a $\lambda \in \operatorname{Irr}(H)$ (we allow the multiplicity a_i to be 0). Accordingly, one has a representation Λ_i of G with character θ_λ or the zero map if $a_i = 0$. The multiplicity of Λ_i as a summand of Δ is $\lambda(1)$. This shows

$$\chi^n = \chi_\Delta = \sum_{\lambda \in \operatorname{Irr}(H)} \lambda(1)\theta_\lambda.$$

From Remark III.4.51 one obtains

$$\chi_{\Delta\Gamma}(g,h) = \sum_{\lambda \in \operatorname{Irr}(H)} \theta_\lambda(g)\chi_\lambda(h) \quad \text{(III.4.8)}$$

for $(g,h) \in G \times H$. We calculate this character in another way. Let $b_1, \ldots, b_d \in W$ be a basis of W. Let $[d] := \{1, \ldots, d\}$ and $[d]^n := \{f\colon [n] \to [d]\}$. Then

$$\big\{b_f := b_{f(1)} \otimes \ldots \otimes b_{f(n)} : f \in [d]^n\big\}$$

is a basis of V. With $\Psi(g) = (\alpha_{ij}(g)) \in \mathbb{C}^{d\times d}$ we have $\chi(g) = \sum_{i=1}^{d} \alpha_{ii}(g)$, $\chi(g^2) = \sum_{i,j=1}^{d} \alpha_{ij}(g)\alpha_{ji}(g)$ and inductively

$$\chi(g^k) = \sum_{f\in[d]^k} \alpha_{f(1),f(2)}(g)\alpha_{f(2),f(3)}(g)\dots\alpha_{f(k),f(1)}(g) \tag{III.4.9}$$

for $k \in \mathbb{N}$. We calculate

$$\begin{aligned}\Delta(g)\Gamma(h)b_f &= \Delta(g)(b_{fh^{-1}(1)} \otimes \dots \otimes b_{fh^{-1}(n)}) \\ &= \Big(\sum_{j=1}^{d} \alpha_{j,fh^{-1}(1)}b_j\Big) \otimes \dots \otimes \Big(\sum_{j=1}^{d} \alpha_{j,fh^{-1}(n)}b_j\Big) \\ &= \sum_{f'\in[d]^n} \alpha_{f'(1),fh^{-1}(1)}\dots\alpha_{f'(n),fh^{-1}(n)}b_{f'}.\end{aligned}$$

From this it follows that

$$\chi_{\Delta\Gamma}(g,h) = \sum_{f\in[d]^n} \alpha_{f(1),fh^{-1}(1)}\dots\alpha_{f(n),fh^{-1}(n)}.$$

Let $h = h_1\dots h_k$ be the decomposition into disjoint cycles (including cycles of length one), where k_i is the length of h_i. Let $[h_i]$ be the set of digits in h_i and $x_i \in [h_i]$. Instead of $1,\dots,n$, one can also multiply the α in the order of the cycles:

$$\begin{aligned}\chi_{\Delta\Gamma}(g,h) &= \sum_{f\in[d]^n}\prod_{i=1}^{k} \alpha_{f(x_i),fh^{-1}(x_i)}\alpha_{fh^{-1}(x_i),fh^{-2}(x_i)}\dots\alpha_{fh^{1-k_i}(x_i),f(x_i)} \\ &= \prod_{i=1}^{k}\Big(\sum_{f\in[h_i]^n} \alpha_{f(x_i),fh^{-1}(x_i)}\alpha_{fh^{-1}(x_i),fh^{-2}(x_i)}\dots\alpha_{fh^{1-k_i}(x_i),f(x_i)}\Big) \qquad \text{(III.4.10)} \\ &\overset{\text{(III.4.9)}}{=} \prod_{i=1}^{k}\chi(g^{k_i}) = \prod_{i=1}^{n}\chi(g^i)^{c_i(h)}.\end{aligned}$$

According to the first orthogonality relation, finally

$$\begin{aligned}\theta_\lambda(g) &= \sum_{\mu\in\mathrm{Irr}(H)} \theta_\mu(g)(\lambda,\mu) = \sum_{\mu\in\mathrm{Irr}(H)} \theta_\mu(g)\frac{1}{|H|}\sum_{h\in H}\lambda(h)\mu(h) = \frac{1}{|H|}\sum_{h\in H}\lambda(h)\sum_{\mu\in\mathrm{Irr}(H)}\theta_\mu(g)\mu(h) \\ &\overset{\text{(III.4.8)}}{=} \frac{1}{|H|}\sum_{h\in H}\lambda(h)\chi_{\Delta\Gamma}(g,h) \overset{\text{(III.4.10)}}{=} \frac{1}{|H|}\sum_{h\in H}\lambda(h)\prod_{i=1}^{n}\chi(g^i)^{c_i(h)}.\end{aligned}$$

□

Corollary III.4.53. *Let ψ be a character of G and $\lambda \in P(n)$. Then G has a character (or the zero map) θ_λ with*

$$\boxed{\theta_\lambda(g) = \frac{1}{n!}\sum_{\sigma\in S_n}\chi_\lambda(\sigma)\prod_{i=1}^{n}\psi(g^i)^{c_i(\sigma)}} \qquad (g\in G),$$

$$\psi^n = \sum_{\lambda\in P(n)} \chi_\lambda(1)\theta_\lambda.$$

Proof. Choose $H = S_n$ and χ_λ instead of λ in Theorem III.4.52. □

Remark III.4.54. In the situation of Corollary III.4.53, θ_λ is called the *symmetrizer* of ψ with respect to $\lambda \in P(n)$.

Example III.4.55.

(i) For linear characters ψ, we have

$$\theta_\lambda(g) = \frac{1}{n!}\sum_{\sigma\in S_n} \chi_\lambda(\sigma)\psi(g)^n = \begin{cases}\psi(g)^n & \text{if } \lambda = (n),\\ 0 & \text{otherwise.}\end{cases}$$

(ii) For $n = 2$, we have

$$\theta_{(2)}(g) = \frac{1}{2}\big(\psi(g)^2 + \psi(g^2)\big), \qquad \theta_{(1^2)}(g) = \frac{1}{2}\big(\psi(g)^2 - \psi(g^2)\big)$$

$\theta_{(2)}$ is called the *symmetric square* and $\theta_{(1^2)}$ the *alternating square* of ψ. They are relevant for Frobenius-Schur indicators (chapter A.14).

(iii) For $n = 3$, one obtains

$$\begin{aligned}\theta_{(3)}(g) &= \frac{1}{6}\big(\psi(g)^3 + 3\psi(g)\psi(g^2) + 2\psi(g^3)\big),\\ \theta_{(1^3)}(g) &= \frac{1}{6}\big(\psi(g)^3 - 3\psi(g)\psi(g^2) + 2\psi(g^3)\big),\\ \theta_{(2,1)}(g) &= \frac{1}{3}\big(\psi(g)^3 - \psi(g^3)\big).\end{aligned}$$

For $\psi(1) \le 2$, $\theta_{(1^3)} = 0$.

(iv) We choose $H = \langle(1,\dots,n)\rangle \le S_n$ in Theorem III.4.52 and $\lambda \in \mathrm{Irr}(H)$ faithful. For $d \mid n$, let $f(d)$ be the sum of the primitive d-th roots of unity. Then $f(1) = 1$ and $\sum_{d|n} f(d) = 0$ for $n > 1$. By Möbius inversion, it follows that $f = \mu$ and

$$\theta_\lambda(g) = \frac{1}{n}\sum_{d|n}\sum_{\substack{h\in H\\ |\langle h\rangle| = d}} \lambda(h)\psi(g^d)^{\frac{n}{d}} = \frac{1}{n}\sum_{d|n}\mu(d)\psi(g^d)^{\frac{n}{d}}.$$

In the case $n = p \in \mathbb{P}$, this simplifies to

$$\theta_\lambda(g) = \frac{1}{p}\big(\psi(g)^p - \psi(g^p)\big).$$

(v) For $H = V_4 \le S_4$ and $\lambda \in \mathrm{Irr}(H) \setminus \{\mathbb{1}_H\}$, one obtains

$$\theta_\lambda(g) = \frac{1}{4}\big(\psi(g)^4 - \psi(g^2)^2\big).$$

Definition III.4.56. For $\lambda \in P(n)$ and $d \in \mathbb{N}$,

$$\beta_\lambda := \frac{1}{n!}\sum_{\sigma\in S_n}\chi_\lambda(\sigma)\prod_{i=1}^{n}(X_1^i + \ldots + X_d^i)^{c_i(\sigma)}$$

is called the *Schur polynomial* associated with λ.

Remark III.4.57.

(i) Obviously β_λ is a symmetric polynomial, which (like the elementary symmetric polynomials) also depends on d. Let ψ be a character of G of degree d. For $g \in G$ there exist, as is well known, roots of unity $\zeta_1, \ldots, \zeta_d \in \mathbb{C}$ with $\psi(g^i) = \zeta_1^i + \ldots + \zeta_d^i$ for $i \in \mathbb{N}_0$. According to Corollary III.4.53, $\theta_\lambda(g) = \beta_\lambda(\zeta_1, \ldots, \zeta_d)$ holds.

(ii) We now determine the irreducible characters of the alternating group. Let $\xi \in \mathrm{Irr}(A_n)$ and $\chi_\lambda \in \mathrm{Irr}(S_n)$ be a constituent of ξ^{S_n}. In the case $\lambda \neq \lambda'$, $\chi_{\lambda'} = \operatorname{sgn}\chi_\lambda$ also occurs in ξ^{S_n}, because $((\chi_{\lambda'})_{A_n}, \xi) = ((\chi_\lambda)_{A_n}, \xi) \neq 0$. Obviously $\xi^{S_n} = \chi_\lambda + \chi_{\lambda'}$ and $\xi_\lambda := \xi = (\chi_\lambda)_{A_n}$ hold. In the case $\lambda' = \lambda$, however, $\xi^{S_n} = \chi_\lambda$ and

$$(\chi_\lambda) = \xi + {}^{(1,2)}\xi =: \xi_\lambda^+ + \xi_\lambda^-$$

according to Clifford (the assignment $\xi \leftrightarrow \xi_\lambda^+$ is arbitrary). Let $\sigma \in A_n$. If σ and ${}^{(1,2)}\sigma$ are conjugate in A_n, then $\xi(\sigma) = \frac{1}{2}\chi_\lambda(\sigma)$ holds. For the remaining character values, we must investigate the conjugacy classes of A_n that are not conjugacy classes of S_n.

Theorem III.4.58. *Let $\sigma \in A_n$ be of cycle type $(\lambda_1, \ldots, \lambda_k)$. σ is not conjugate to ${}^{(1,2)}\sigma$ in A_n if and only if the λ_i are odd and pairwise distinct.*

Proof. Let $\sigma \in C \in \mathrm{Cl}(A_n)$. $C \in \mathrm{Cl}(S_n)$ holds if and only if $|A_n : \mathrm{C}_{A_n}(\sigma)| = |K| = |S_n : \mathrm{C}_{S_n}(\sigma)|$. Because of $|A_n : \mathrm{C}_{A_n}(\sigma)| = |A_n : A_n \cap \mathrm{C}_{S_n}(\sigma)| = |A_n\mathrm{C}_{S_n}(\sigma) : \mathrm{C}_{S_n}(\sigma)|$ it follows that

$$C \notin \mathrm{Cl}(S_n) \iff \mathrm{C}_{S_n}(\sigma) \subseteq A_n.$$

Let $\sigma = \sigma_1 \ldots \sigma_k$ with disjoint cycles σ_i of length λ_i. If λ_i is even, then $\sigma_i \in \mathrm{C}_{S_n}(g) \setminus A_n$. Thus we can assume that all λ_i are odd. Let $\lambda_i = \lambda_j$ with $i \neq j$. We write $\sigma_i = (a_1, \ldots, a_{\lambda_i})$ and $\sigma_j = (b_1, \ldots, b_{\lambda_i})$. Then $\tau := (a_1, b_1)(a_2, b_2)\ldots(a_{\lambda_i}, b_{\lambda_i}) \in \mathrm{C}_{S_n}(\sigma) \setminus A_n$.

Conversely, let the λ_i be odd and pairwise distinct. We calculate $|S_n : \mathrm{C}_{S_n}(\sigma)|$ by counting the elements of cycle type $(\lambda_1, \ldots, \lambda_k)$. For the λ_1 elements of the cycle σ_1 there are $\frac{n!}{(n-\lambda_1)!}$ possibilities. However, λ_1 possibilities each yield the same element. Thus there are $\frac{n!}{\lambda_1(n-\lambda_1)!}$ possibilities for σ_1. Analogously, there are then $\frac{(n-\lambda_1)!}{\lambda_2(n-\lambda_1-\lambda_2)!}$ possibilities for σ_2 etc. This shows

$$|S_n : \mathrm{C}_{S_n}(\sigma)| = \frac{n!(n-\lambda_1)!(n-\lambda_1-\lambda_2)!\ldots(n-\lambda_1-\ldots-\lambda_{k-1})!}{\lambda_1\ldots\lambda_k(n-\lambda_1)!(n-\lambda_1-\lambda_2)!\ldots(\underbrace{n-\lambda_1-\ldots-\lambda_k}_{=0})!} = \frac{n!}{\lambda_1\ldots\lambda_k}$$

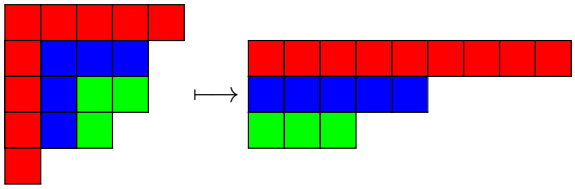
and $|\mathrm{C}_{S_n}(\sigma)| = \lambda_1\ldots\lambda_k$. Obviously $\langle\sigma_1\rangle\ldots\langle\sigma_k\rangle \subseteq \mathrm{C}_{S_n}(\sigma)$ and $|\langle\sigma_1\rangle\ldots\langle\sigma_k\rangle| = |\langle\sigma_1\rangle|\ldots|\langle\sigma_k\rangle| = \lambda_1\ldots\lambda_k$. Thus $\mathrm{C}_{S_n}(\sigma) = \langle\sigma_1\rangle\ldots\langle\sigma_k\rangle \subseteq A_n$. □

Example III.4.59. For $n \geq 3$ there is always a $C \in \mathrm{Cl}(A_n)$ with $C \notin \mathrm{Cl}(S_n)$. For odd n one can choose cycle type (n) in Theorem III.4.58 and for even n cycle type $(n-1, 1)$.

Remark III.4.60. As usual, $\langle(1,2)\rangle$ acts on $\mathrm{Irr}(A_n)$ and on $\mathrm{Cl}(A_n)$. According to Brauer's Permutation Lemma, there are exactly as many pairs ${}^{(1,2)}\xi_\lambda \neq \xi_\lambda \in \mathrm{Irr}(A_n)$ as there are pairs ${}^{(1,2)}C \neq C \in \mathrm{Cl}(A_n)$.

This can also be seen through the bijection:

$$\Phi\colon \{\lambda = \lambda' \in P(n)\} \longrightarrow \{\lambda = (\lambda_1, \ldots, \lambda_k) \in P(n) \text{ with } \lambda_i \text{ odd and pairwise distinct}\},$$
$$(\lambda_1, \ldots, \lambda_k) \longmapsto (h_{11}, h_{22}, \ldots) = (2\lambda_1 - 1, 2\lambda_2 - 3, 2\lambda_3 - 5, \ldots)$$



Let $\lambda = \lambda' \in P(n)$ and $g \in A_n$ of cycle type $\mu = (\mu_1, \ldots, \mu_k)$. With a suitable choice of ξ_λ, it holds that

$$\xi_\lambda^{\pm}(g) = \begin{cases} \frac{1}{2}\chi_\lambda(\mu) \pm \frac{1}{2}\sqrt{(-1)^{\frac{n-k}{2}}\mu_1 \ldots \mu_k} & \text{if } \mu = \Phi(\lambda) \\ \frac{1}{2}\chi_\lambda(\mu) & \text{if } \mu \neq \Phi(\lambda) \end{cases}$$

(without proof).

Example III.4.61. For $n = 5$, $\lambda = (3, 1^2) = \lambda'$ is the only symmetric partition and $\Phi(\lambda) = (5)$. From Example III.4.28 the character table of A_5:

A_5	(1^5)	$(2^2, 1)$	$(3, 1^2)$	$(5)^+$	$(5)^-$
(5)	1	1	1	1	1
$(4, 1)$	4	0	1	-1	-1
$(3, 2)$	5	1	-1	0	0
$(3, 1^2)^+$	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
$(3, 1^2)^-$	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

III.5 Category Theory

Remark III.5.1.

(i) A mathematical category is a generic term for almost all algebraic objects such as sets, groups, vector spaces, rings, modules etc. In this chapter, we develop an abstract theory for categories that unifies many of the proofs from previous chapters. With the help of the Yoneda embedding, every (locally small) category can be embedded into a larger category with "better" properties. We had already seen, for example, that one can prove theorems about finite groups by working with the corresponding group algebras. Group algebras or general rings can in turn be studied through their module category.

(ii) As is well known, the collection of all sets is not itself a set. In the following, we informally use the term *class* to describe collections of this kind. We use the usual rules of set theory for classes as well.

Definition III.5.2. A *category* $\mathcal{C}$ consists of

- a class $\mathrm{Ob}(\mathcal{C})$ of *objects*,
- classes $\mathrm{Hom}_{\mathcal{C}}(A, B)$ of *morphisms* for all $A, B \in \mathrm{Ob}(\mathcal{C})$.

The following hold:

- $\mathrm{Hom}_{\mathcal{C}}(A, B) \cap \mathrm{Hom}_{\mathcal{C}}(C, D) = \varnothing$ if $(A, B) \neq (C, D)$.
- For $A, B, C \in \mathrm{Ob}(\mathcal{C})$ there exists a composition

$$\mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) \to \mathrm{Hom}_{\mathcal{C}}(A, C), \qquad (f, g) \mapsto g \circ f$$

  with $f \circ (g \circ h) = (f \circ g) \circ h$ (whenever defined).
- For $A \in \mathrm{Ob}(\mathcal{C})$ there exists an *identity* $\mathrm{id}_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ with $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$ for all $B \in \mathrm{Ob}(\mathcal{C})$ and $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$.

Remark III.5.3.

(i) We frequently write morphisms $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ in the form $f\colon A \to B$, even if they do not have to be mappings. Likewise, we will occasionally omit the composition symbol $\circ$.

(ii) As usual, one shows that id_A is uniquely determined by the property $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$. Therefore, the objects of a category can be reconstructed from the morphisms.

(iii) A category $\mathcal{C}$ is called *locally small* if $\mathrm{Hom}_{\mathcal{C}}(A, B)$ is a set (instead of a class) for all $A, B \in \mathrm{Ob}(\mathcal{C})$. If additionally $\mathrm{Ob}(\mathcal{C})$ is a set, then $\mathcal{C}$ is called *small*.

Example III.5.4.

(i) The (locally small) category **Set** consists of all sets as objects and $\mathrm{Hom}(A, B)$ is the set of all mappings $f\colon A \to B$ for sets $A, B \in \mathrm{Ob}(\mathbf{Set})$ with the usual identity mapping. If one wants to allow only finite sets as objects, one obtains the *subcategory* **set**. Analogously, one can restrict oneself to injective, surjective or bijective morphisms. As is well known, neither **Set** nor **set** is small.

(ii) In a similar way, one obtains the categories **Grp**, **grp**, **Ab**, **Rng** of all groups, all finite groups, all abelian groups and all rings. Here, $\mathrm{Hom}(A, B)$ consists only of the corresponding homomorphisms. For a ring R, let ${}_R\mathbf{Mod}$, $\mathbf{Mod}_R$, ${}_R\mathbf{mod}$ be the categories of all R-left modules, all R-right modules and all finitely generated R-left modules.

(iii) Let R be a commutative ring and $\mathrm{Ob}(\mathcal{C}) = \mathbb{N}$. For $a, b \in \mathbb{N}$ let $\mathrm{Hom}(a, b) = R^{a\times b}$. With matrix multiplication as composition, R-**mat** $:= \mathcal{C}$ becomes a category.

(iv) Every group G can be understood as a category with one object A. Here, $\mathrm{Hom}(A, A) = G$ and $x \circ y = xy$ for $x, y \in G$.

(v) For every category $\mathcal{C}$ there is the *dual* category $\mathcal{C}^o$ with $\mathrm{Ob}(\mathcal{C}^o) := \mathrm{Ob}(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{C}^o}(A, B) := \mathrm{Hom}_{\mathcal{C}}(B, A)$ and $f \circ_{\mathcal{C}^o} g := g \circ_{\mathcal{C}} f$ for $f \in \mathrm{Hom}_{\mathcal{C}^o}(B, C)$ and $g \in \mathrm{Hom}_{\mathcal{C}^o}(A, B)$.

(vi) For categories $\mathcal{C}, \mathcal{D}$ one defines the *product category* $\mathcal{C} \times \mathcal{D}$ by $\mathrm{Ob}(\mathcal{C} \times \mathcal{D}) := \mathrm{Ob}(\mathcal{C}) \times \mathrm{Ob}(\mathcal{D})$, $\mathrm{Hom}_{\mathcal{C}\times\mathcal{D}}((A, B), (C, D)) := \mathrm{Hom}_{\mathcal{C}}(A, C)\times\mathrm{Hom}_{\mathcal{D}}(B, D)$, $\mathrm{id}_{(A,B)} := (\mathrm{id}_A, \mathrm{id}_B)$ and $(f, g)\circ(f', g') := (f \circ f', g \circ g')$.

Definition III.5.5. A morphism $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ of a category $\mathcal{C}$ is called

- *Monomorphism*, if for all $C \in \mathrm{Ob}(\mathcal{C})$ and $g, h \in \mathrm{Hom}_{\mathcal{C}}(C, A)$ it holds that $f \circ g = f \circ h \Longrightarrow g = h$.
- *Epimorphism*, if for all $C \in \mathrm{Ob}(\mathcal{C})$ and $g, h \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ it holds that $g \circ f = h \circ f \Longrightarrow g = h$.
- *Isomorphism*, if there exists a $g \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ with $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$. If applicable, one writes $A \cong_{\mathcal{C}} B$ (for $\mathcal{C} = {}_R\mathbf{Mod}$ we continue to use $\simeq$). In the case $A = B$, f is called an *Automorphism*.

Example III.5.6.

(i) Every isomorphism is obviously a mono- and epimorphism. The monomorphisms (resp. epimorphisms) in $\mathcal{C}$ correspond to the epimorphisms (resp. monomorphisms) in $\mathcal{C}^o$.

(ii) For all $A \in \mathrm{Ob}(\mathcal{C})$, id_A is an isomorphism. Let $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ be an isomorphism. As usual, there exists exactly one $g \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ with $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$. We write $f^{-1} := g$. Obviously, f^{-1} is also an isomorphism. If $f\colon A \to B$ and $g\colon B \to C$ are isomorphisms, then so is $g \circ f$. Therefore, the automorphisms of A form a group $\mathrm{Aut}_{\mathcal{C}}(A)$.

(iii) One easily shows that the mono-, epi- and isomorphisms in **Set** are exactly the injective, surjective and bijective maps.

(iv) Let $\mathrm{Ob}(\mathcal{C}) = \{A, B\}$ with $\mathrm{Hom}_{\mathcal{C}}(A, A) = \{\mathrm{id}_A\}$, $\mathrm{Hom}_{\mathcal{C}}(B, B) = \{\mathrm{id}_B\}$, $\mathrm{Hom}_{\mathcal{C}}(A, B) = \varnothing$. Then every morphism $B \to A$ is a mono- and epimorphism, but not an isomorphism. In particular, monomorphisms do not have to be injective and epimorphisms do not have to be surjective (if morphisms are maps between sets).

(v) Let $f\colon \mathbb{Q} \to R$ be a ring homomorphism. For $a, b \in \mathbb{Z}$ with $b \neq 0$, it holds that $f(b)f(\frac{1}{b}) = f(b \cdot \frac{1}{b}) = 1$ and $f(\frac{a}{b}) = f(a)f(b)^{-1}$. Therefore, f is already uniquely determined by $f(a)$ for $a \in \mathbb{Z}$. Thus $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is a non-surjective epimorphism in **Rng**.

Theorem III.5.7. *In* **Grp**, **Ab** *and* ${}_R\mathbf{Mod}$*, the mono-, epi- and isomorphisms are exactly the injective, surjective and bijective homomorphisms, respectively.*

Proof. Let $\mathcal{C} \in \{\mathbf{Grp}, \mathbf{Ab}, {}_R\mathbf{Mod}\}$. Obviously, injective, surjective and bijective homomorphisms are monomorphisms, epimorphisms and isomorphisms in $\mathcal{C}$, respectively. Now let $f\colon A \to B$ be a monomorphism in $\mathcal{C}$. Let $x \in \mathrm{Ker}(f)$ and $K := \langle x \rangle$. Then there exist homomorphisms $g, h\colon K \to A$ with $g(x) = x$ and $h(x) = 1$ (or $h(x) = 0$ in ${}_R\mathbf{Mod}$). From $f \circ g = f \circ h$ it follows that $g = h$ and $x = 1$ (or 0). Thus f is injective.

Finally, let $f\colon A \to B$ be an epimorphism in $\mathcal{C}$. In the case $\mathcal{C} \in \{\mathbf{Ab}, {}_R\mathbf{Mod}\}$, there exist the trivial homomorphism $g\colon B/f(A) \to B/f(A)$ and $h := \mathrm{id}_{B/f(A)}$. From $g \circ f = h \circ f$ it follows that $f = h$ and $B = f(A)$, i. e. f is surjective. Now let $\mathcal{C} = \mathbf{Grp}$. Let $\Omega := B/f(A) \dot\cup \{\omega\}$ and

$$g\colon B \to \mathrm{Sym}(B/f(A)) \hookrightarrow \mathrm{Sym}(\Omega)$$

be the action by left multiplication on $B/f(A)$. Let $t\colon \mathrm{Sym}(\Omega) \to \mathrm{Sym}(\Omega)$ be the inner automorphism induced by the transposition $(1f(A), \omega)$. For $h := t \circ g$ it then holds that $g \circ f = h \circ f$, because $g(f(A))$ is in the stabilizer of $1f(A)$. Since B acts transitively on $B/f(A)$, it must hold that $f(A) = B$, i. e. f is surjective. □

Definition III.5.8. A *functor* between categories $\mathcal{C}$ and $\mathcal{D}$ is a class of maps $\Phi\colon \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ and $\Phi\colon \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Phi(B))$ with the following properties:

- $\Phi(\mathrm{id}_A) = \mathrm{id}_{\Phi(A)}$,
- $\Phi(g \circ f) = \Phi(g) \circ \Phi(f)$ for $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ and $g \in \mathrm{Hom}_{\mathcal{C}}(B, C)$.

We write $\Phi\colon \mathcal{C} \to \mathcal{D}$ if applicable. One calls Φ

- *full*, if $\Phi\colon \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Phi(B))$ is surjective for all $A, B \in \mathrm{Ob}(\mathcal{C})$.
- *faithful*, if $\Phi\colon \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Phi(B))$ is injective for all $A, B \in \mathrm{Ob}(\mathcal{C})$.

The *image* of Φ is the category $\Phi(\mathcal{C})$ with $\mathrm{Ob}(\Phi(\mathcal{C})) = \{\Phi(A) : A \in \mathrm{Ob}(\mathcal{C})\}$ and $\mathrm{Hom}_{\Phi(\mathcal{C})}(A, B) = \{\Phi(f) : f \in \mathrm{Hom}_{\mathcal{C}}(A, B)\}$.

Example III.5.9.

(i) The *identity functor* $\mathrm{id}_{\mathcal{C}}\colon \mathcal{C} \to \mathcal{C}$ with $A \mapsto A$ and $f \mapsto f$ for $A \in \mathrm{Ob}(\mathcal{C})$ and $f \in \mathrm{Hom}(A, B)$ is full and faithful.

(ii) For $D \in \mathrm{Ob}(\mathcal{D})$ there exists the *constant* functor $\Phi_D\colon \mathcal{C} \to \mathcal{D}$ with $\Phi(A) := D$ and $\Phi(f) := \mathrm{id}_D$ for $A \in \mathrm{Ob}(\mathcal{C})$ and $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$. In general, Φ_D is neither full nor faithful.

(iii) So-called *forgetful functors* $\Phi\colon \mathbf{Rng} \to \mathbf{Ab}$, $\mathbf{Ab} \to \mathbf{Grp}$, $\mathbf{Grp} \to \mathbf{Set}$, … with $\Phi(A) = A$ and $\Phi(f) = f$ for $f \in \mathrm{Hom}(A, B)$. The functor thus "forgets" the algebraic structure of an (abelian) group or a ring. They are faithful, but in general not full. Although they are faithful, the map $\Phi\colon \mathrm{Ob}(\mathbf{Grp}) \to \mathrm{Ob}(\mathbf{Set})$ is not injective.

(iv) For a locally small category $\mathcal{C}$ and $A \in \mathrm{Ob}(\mathcal{C})$ there exists the *Hom-functor*

$$\mathrm{Hom}(A,.)\colon \mathcal{C} \to \mathbf{Set}, \qquad B \mapsto \mathrm{Hom}_{\mathcal{C}}(A,B)$$

with $\mathrm{Hom}(A,f)(g) := f \circ g$ for $f \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ and $g \in \mathrm{Hom}_{\mathcal{C}}(A,B)$.

(v) $\mathrm{GL}(n,.)\colon \mathbf{Rng} \to \mathbf{Grp}$, $R \mapsto \mathrm{GL}(n,R)$ and $\mathrm{GL}(n,f)(a_{ij}) := (f(a_{ij}))$ for $f \in \mathrm{Hom}(R,S)$.

(vi) $\Phi_K\colon \mathbf{grp} \to \mathbf{Rng}$, $G \mapsto KG$ for a field K. For $f\colon G \to H$ is $\Phi_K(f)(\sum_{g\in G} \alpha_g g) := \sum_{g\in G} \alpha_g f(g)$.

(vii) Let G be a group and $\mathcal{C}$ the corresponding category from Example III.5.4(iv) with $\mathrm{Ob}(\mathcal{C}) = \{A\}$. Let $\Phi\colon \mathcal{C} \to \mathbf{Set}$ be a functor and $\Omega := \Phi(A)$. For $g,h \in G$ we have $\Phi(gh) = \Phi(g)\Phi(h)$. Therefore $\Phi\colon G \to \mathrm{Sym}(\Omega)$ is a group action. Analogously, every functor $\mathcal{C} \to K\text{-}\mathbf{mat}$ corresponds to a representation of G.

(viii) If $\Phi\colon \mathcal{C} \to \mathcal{D}$ and $\Psi\colon \mathcal{D} \to \mathcal{E}$ are functors, then so is $\Psi \circ \Phi\colon \mathcal{C} \to \mathcal{E}$. One calls Φ an *isomorphism* of categories if a functor $\Psi\colon \mathcal{D} \to \mathcal{C}$ with $\Psi \circ \Phi = \mathrm{id}_{\mathcal{C}}$ and $\Phi \circ \Psi = \mathrm{id}_{\mathcal{D}}$ exists. If applicable, we write $\mathcal{C} \cong \mathcal{D}$.

(ix) Transposing yields an (inverse to itself) isomorphism $\Phi\colon K\text{-}\mathbf{mat} \to K\text{-}\mathbf{mat}^o$, $n \mapsto n$, $A \mapsto A^{\mathrm{t}}$.

(x) For a ring R we have ${}_R\mathbf{Mod} \cong \mathbf{Mod}_{R^o}$, because according to Example II.6.4 every R-left module M is an R^o-right module and every R-homomorphism is an R^o-homomorphism.

(xi) The locally small categories are the objects of the category **Cat**. The morphisms of **Cat** are exactly the functors between locally small categories.[1]

Remark III.5.10. Functors according to Definition III.5.8 are occasionally called *covariant*, while a *contravariant* functor between $\mathcal{C}$ and $\mathcal{D}$ is a functor of the form $\mathcal{C}^o \to \mathcal{D}$. For such a functor, $\Phi(f) \in \mathrm{Hom}_{\mathcal{C}}(B,A)$ and $\Phi(g \circ f) = \Phi(f) \circ \Phi(g)$ holds for $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ and $g \in \mathrm{Hom}_{\mathcal{C}}(B,C)$. For example, the Hom-functor in the first component $\mathrm{Hom}(.,B)\colon \mathcal{C} \to \mathbf{Set}$, $A \mapsto \mathrm{Hom}_{\mathcal{C}}(A,B)$ with $\mathrm{Hom}(f,B)(g) := f \circ g$ is contravariant. For a field K, one specifically obtains the (contravariant) functor ${}_K\mathbf{mod} \to {}_K\mathbf{mod}$, which maps V to its dual space $V^* := \mathrm{Hom}(V,K)$ and $f\colon V \to W$ to the dual map $f^*\colon W^* \to V^*$.

Definition III.5.11.

(i) A *congruence* of a category $\mathcal{C}$ is a class of equivalence relations $\sim_{A,B}$ on $\mathrm{Hom}_{\mathcal{C}}(A,B)$ for $A,B \in \mathrm{Ob}(\mathcal{C})$ with the following properties:

- For $f,g \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ and $h \in \mathrm{Hom}_{\mathcal{C}}(B,C)$, it holds that $f \sim_{A,B} g \Longrightarrow h \circ f \sim_{A,C} h \circ g$.
- For $f,g \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ and $h \in \mathrm{Hom}_{\mathcal{C}}(C,A)$, it holds that $f \sim_{A,B} g \Longrightarrow f \circ h \sim_{C,B} g \circ h$.

(ii) Let $\sim$ be a congruence of a category $\mathcal{C}$. For $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$, let $[f]$ be the equivalence class with respect to $\sim_{A,B}$. The *quotient category* $\mathcal{C}/\!\sim$ of $\mathcal{C}$ consists of the same objects as $\mathcal{C}$ and

$$\mathrm{Hom}_{\mathcal{C}/\sim}(A,B) := \{[f] : f \in \mathrm{Hom}_{\mathcal{C}}(A,B)\}$$

for $A,B \in \mathrm{Ob}(\mathcal{C})$. Here, $[f] \circ [g] := [f \circ g]$ holds (one should check the well-definedness).

[1] One must restrict oneself to locally small categories to avoid subtle problems of type theory.

Theorem III.5.12 (Homomorphism Theorem)**.** *Let $\Phi\colon \mathcal{C} \to \mathcal{D}$ be a functor. For $f, g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$,*

$$f \sim_{A,B} g \ :\Longleftrightarrow\ \Phi(f) = \Phi(g)$$

defines a congruence on $\mathcal{C}$. Let $\mathcal{C}/\mathrm{Ker}(\Phi) := \mathcal{C}/\sim$ be the corresponding quotient category. Then there exists an isomorphism $\overline{\Phi}\colon \mathcal{C}/\mathrm{Ker}(\Phi) \to \Phi(\mathcal{C})$.

Proof. Clearly, $\sim_{A,B}$ is an equivalence relation. For $h \in \mathrm{Hom}_{\mathcal{C}}(B, C)$, it holds that

$$f \sim_{A,B} g \implies \Phi(h \circ f) = \Phi(h)\Phi(f) = \Phi(h)\Phi(g) = \Phi(h \circ g) \implies h \circ f \sim_{A,C} h \circ g$$

and analogously for $f \circ h = g \circ h$. Thus $\sim$ is a congruence. By definition, the functor $\overline{\Phi}\colon \mathcal{C}/\mathrm{Ker}(\Phi) \to \Phi(\mathcal{C})$, $A \mapsto A$, $[f] \mapsto \Phi(f)$ is well-defined. Furthermore, $\Psi\colon \Phi(\mathcal{C}) \to \mathcal{C}/\mathrm{Ker}(\Phi)$, $A \mapsto A$, $\Phi(f) \mapsto [f]$ is a functor with $\overline{\Phi}\Psi = \mathrm{id}$ and $\Psi\overline{\Phi} = \mathrm{id}$. □

Definition III.5.13. Let $\Phi, \Psi\colon \mathcal{C} \to \mathcal{D}$ be functors between categories $\mathcal{C}$, $\mathcal{D}$. A *natural transformation* α between Φ and Ψ is a class of morphisms $\alpha_A \in \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Psi(A))$ for $A \in \mathrm{Ob}(\mathcal{C})$ with $\alpha_B \circ \Phi(f) = \Psi(f) \circ \alpha_A$ for $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, i. e. the following diagram is commutative:

$$\begin{array}{ccc} \Phi(A) & \xrightarrow{\alpha_A} & \Psi(A) \\ {\scriptstyle \Phi(f)}\downarrow & & \downarrow{\scriptstyle \Psi(f)} \\ \Phi(B) & \xrightarrow[\alpha_B]{} & \Psi(B) \end{array}$$

We write $\alpha\colon \Phi \Rightarrow \Psi$ if necessary.

Remark III.5.14. As always, there is the *identity* transformation $\mathrm{id}_\Phi\colon \Phi \Rightarrow \Phi$ with $(\mathrm{id}_\Phi)_A = \mathrm{id}_{\Phi(A)}$ for all $A \in \mathrm{Ob}(\mathcal{C})$. If $\alpha\colon \Phi \Rightarrow \Psi$ and $\beta\colon \Psi \Rightarrow \Gamma$ are natural transformations of functors $\Phi, \Psi, \Gamma\colon \mathcal{C} \to \mathcal{D}$, then so is $\gamma := \beta \circ \alpha\colon \Phi \Rightarrow \Gamma$ with $\gamma_A := \beta_A \circ \alpha_A$, because

$$\gamma_B \circ \Phi(f) = \beta_B \circ (\alpha_B \circ \Phi(f)) = (\beta_B \circ \Psi(f)) \circ \alpha_A = \Gamma(f) \circ \beta_A \circ \alpha_A = \Gamma(f) \circ \gamma_A$$

for $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$. In this way, the class of functors between $\mathcal{C}$ and $\mathcal{D}$ becomes a category $\mathcal{D}^{\mathcal{C}}$, whose morphisms are the natural transformations. One calls $\mathcal{D}^{\mathcal{C}}$ the *functor category* between $\mathcal{C}$ and $\mathcal{D}$. An isomorphism $\alpha\colon \Phi \Rightarrow \Psi$ is called a *natural isomorphism*. This means that α_A are isomorphisms for all $A \in \mathrm{Ob}(\mathcal{C})$. If necessary, one calls Φ and Ψ *isomorphic* and writes $\Phi \cong_{\mathcal{D}^{\mathcal{C}}} \Psi$.

Example III.5.15.

(i) Let K be a field and $\mathcal{C} := {}_K\mathbf{mod}$ the category of finite-dimensional K-vector spaces. Let $\Phi := \mathrm{id}_{\mathcal{C}}$ be the identity functor and $\Psi\colon \mathcal{C} \to \mathcal{C}$, $V \mapsto V^{**} := \mathrm{Hom}(\mathrm{Hom}(V, K), K)$ (bidual space of V) with $\Psi(f) := f^{**}$ (bidual map). For $F \in V^{**}$ and $\lambda \in W^*$ we have

$$f^{**}(F)(\lambda) = (F \circ f^*)(\lambda) = F(\lambda \circ f).$$

For $V \in \mathrm{Ob}(\mathcal{C})$ let $\alpha_V \in \mathrm{Hom}_K(V, V^{**})$ with $(\alpha_V(v))(\lambda) := \lambda(v)$ for $v \in V$ and $\lambda \in V^*$. For $f \in \mathrm{Hom}_K(V, W)$, $v \in V$ and $\lambda \in W^*$ we have

$$(\alpha_W \circ f)(v)(\lambda) = \lambda(f(v)) = \alpha_V(v)(\lambda \circ f) = (f^{**} \circ \alpha_V)(v)(\lambda) = (\Psi(f) \circ \alpha_V)(v)(\lambda).$$

Thus $\alpha\colon \mathrm{id}_{\mathcal{C}} \Rightarrow \Psi$ is a natural transformation. Since α_V is an isomorphism, α is even a natural isomorphism.

(ii) Let **CRng** be the category of commutative rings and $\mathrm{GL}(n,.)\colon \mathbf{CRng} \to \mathbf{Grp}$ as well as $.^\times\colon \mathbf{CRng} \to \mathbf{Grp}$, $R \mapsto R^\times$ be functors. For $f\colon R \to S$ let $f^\times := f_{|R^\times}$ be the restriction to $R^\times$. Then $\det\colon \mathrm{GL}(n,.) \Rightarrow .^\times$ is a natural transformation with $\det_R\colon \mathrm{GL}(n,R) \to R^\times$, $A \mapsto \det(A)$, because

$$(\det_S \circ \mathrm{GL}(n,f))(A) = \det(f(A)) = f_{|R^\times}(\det(A)) = (f^\times \circ \det_R)(A)$$

for $A \in \mathrm{GL}(n,R)$ and every ring homomorphism $f\colon R \to S$.

Lemma III.5.16 (Yoneda)**.** *Let $\mathcal{C}$ be a locally small category, $A \in \mathrm{Ob}(\mathcal{C})$ and $\Phi\colon \mathcal{C} \to \mathbf{Set}$ a functor. Then the map*

$$\begin{aligned}\mathrm{Hom}_{\mathbf{Set}^{\mathcal{C}}}\big(\mathrm{Hom}(A,.),\Phi\big) &\to \Phi(A),\\ \alpha &\mapsto \alpha_A(\mathrm{id}_A)\end{aligned}$$

is a bijection.

Proof. According to Remark III.5.14, $\Omega := \mathrm{Hom}_{\mathbf{Set}^{\mathcal{C}}}\big(\mathrm{Hom}(A,.),\Phi\big)$ is the class of natural transformations $\mathrm{Hom}(A,.) \Rightarrow \Phi$. Since $\mathcal{C}$ is locally small, Ω is a set. For $\alpha \in \Omega$, we have $\alpha_A\colon \mathrm{Hom}_{\mathcal{C}}(A,A) \to \Phi(A)$ and $\alpha_A(\mathrm{id}_A) \in \Phi(A)$ as claimed. For $x \in \Phi(A)$, let $\beta^x_B\colon \mathrm{Hom}_{\mathcal{C}}(A,B) \to \Phi(B)$, $f \mapsto \Phi(f)(x)$. For $f \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ and $\varphi \in \mathrm{Hom}_{\mathcal{C}}(A,B)$, it holds that

$$\big(\beta^x_C \circ \mathrm{Hom}(A,f)\big)(\varphi) = \beta^x_C(f\circ\varphi) = \Phi(f\circ\varphi)(x) = \Phi(f)\big(\Phi(\varphi)(x)\big) = (\Phi(f)\circ\beta^x_B)(\varphi).$$

Thus $\beta^x\colon \mathrm{Hom}(A,.) \Rightarrow \Phi$ is a natural transformation.

Applying the given map to $\alpha = \beta$, we obtain $\beta^x_A(\mathrm{id}_A) = \Phi(\mathrm{id}_A)(x) = \mathrm{id}_{\Phi(A)}(x) = x$. Conversely, let $x = \alpha_A(\mathrm{id}_A)$. For $B \in \mathrm{Ob}(\mathcal{C})$ and $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$, it holds that

$$\beta^x_B(f) = \Phi(f)(x) = (\Phi(f)\circ\alpha_A)(\mathrm{id}_A) = \big(\alpha_B \circ \mathrm{Hom}(A,f)\big)(\mathrm{id}_A) = \alpha_B(f).$$

Therefore $\Phi(A) \to \Omega$, $x \mapsto \beta^x$ is the inverse map to $\Omega \to \Phi(A)$, $\alpha \mapsto \alpha_A(\mathrm{id}_A)$. □

Theorem III.5.17 (Yoneda embedding)**.** *For every locally small category $\mathcal{C}$, there exists a full and faithful functor $\mathcal{C} \to \mathbf{Set}^{\mathcal{C}^o}$, $A \mapsto \mathrm{Hom}(.,A)$.*

Proof. According to Remark III.5.10, $\mathrm{Hom}(.,A)$ is a contravariant functor for $A \in \mathrm{Ob}(\mathcal{C})$, hence a functor $\mathcal{C}^o \to \mathbf{Set}$. We prove the statement for $\mathcal{C}^o$ instead of $\mathcal{C}$. So let $\Gamma\colon \mathcal{C}^o \to \mathbf{Set}^{\mathcal{C}}$, $A \mapsto \mathrm{Hom}(A,.)$. Let $A,B \in \mathrm{Ob}(\mathcal{C})$. Yoneda's Lemma with $\Phi = \mathrm{Hom}(B,.)$ yields a bijection

$$\Delta_{A,B}\colon \mathrm{Hom}_{\mathbf{Set}^{\mathcal{C}}}\big(\mathrm{Hom}(A,.),\mathrm{Hom}(B,.)\big) \to \mathrm{Hom}_{\mathcal{C}}(B,A) = \mathrm{Hom}_{\mathcal{C}^o}(A,B).$$

For $f \in \mathrm{Hom}_{\mathcal{C}^o}(A,B)$, let $\Gamma(f) := \Delta^{-1}_{A,B}(f)$. From the proof of Yoneda's Lemma, one obtains

$$\Gamma(f)_C\colon \mathrm{Hom}_{\mathcal{C}}(A,C) \to \mathrm{Hom}_{\mathcal{C}}(B,C), \qquad \varphi \mapsto \mathrm{Hom}(B,\varphi)(f) = \varphi\circ f$$

for $C \in \mathrm{Ob}(\mathcal{C})$. In particular, $\Gamma(\mathrm{id}_A) = \mathrm{id}_{\mathrm{Hom}(A,.)}$ for $A \in \mathrm{Ob}(\mathcal{C})$. For $g \in \mathrm{Hom}_{\mathcal{C}^o}(B,C)$, $D \in \mathrm{Ob}(\mathcal{C})$ and $\varphi \in \mathrm{Hom}_{\mathcal{C}}(A,D)$, it follows that

$$\Gamma(g\circ_{\mathcal{C}^o} f)_D(\varphi) = \varphi\circ(g\circ_{\mathcal{C}^o} f) = (\varphi\circ f)\circ g = \big(\Gamma(g)_D\circ\Gamma(f)_D\big)(\varphi).$$

This shows that Γ is a functor.

Now let a natural transformation $\alpha\colon \operatorname{Hom}(A,.) \Rightarrow \operatorname{Hom}(B,.)$ be given. For $f := \Delta_{A,B}(\alpha) \in \operatorname{Hom}_{\mathcal{C}}(B,A)$, it then holds that $\Gamma(f) = \alpha$. Thus Γ is full. Finally, let $f, g \in \operatorname{Hom}_{\mathcal{C}^o}(A,B)$ with $\Gamma(f) = \Gamma(g)$. Then it follows that $f = \Delta_{A,B}(\Gamma(f)) = \Delta_{A,B}(\Gamma(g)) = g$ and Γ is faithful. □

Lemma III.5.18. *Let the functor $\Phi\colon \mathcal{C} \to \mathcal{D}$ be full and faithful. Then $A \cong_{\mathcal{C}} B \iff \Phi(A) \cong_{\mathcal{D}} \Phi(B)$ holds for $A, B \in \operatorname{Ob}(\mathcal{C})$.*

Proof. Let $f\colon A \to B$ be an isomorphism in $\mathcal{C}$. Then

$$\Phi(f) \circ \Phi(f^{-1}) = \Phi(f \circ f^{-1}) = \Phi(\mathrm{id}_B) = \mathrm{id}_{\Phi(B)}$$

and analogously $\Phi(f^{-1}) \circ \Phi(f) = \mathrm{id}_{\Phi(A)}$. This shows that $\Phi(f)\colon \Phi(A) \to \Phi(B)$ is an isomorphism in $\mathcal{D}$. Conversely, let $g\colon \Phi(A) \to \Phi(B)$ be an isomorphism in $\mathcal{D}$. Since Φ is full, there exist $f \in \operatorname{Hom}_{\mathcal{C}}(A,B)$ and $f' \in \operatorname{Hom}_{\mathcal{C}}(B,A)$ with $\Phi(f) = g$ and $\Phi(f') = g^{-1}$. It follows that $\Phi(f \circ f') = g \circ g^{-1} = \mathrm{id}_{\Phi(B)} = \Phi(\mathrm{id}_B)$. Since Φ is faithful, one obtains $f \circ f' = \mathrm{id}_B$. Analogously $f' \circ f = \mathrm{id}_A$. Thus f is an isomorphism in $\mathcal{C}$. □

Corollary III.5.19. *Let $\mathcal{C}$ be a locally small category and $A, B \in \operatorname{Ob}(\mathcal{C})$. Then*

$$\operatorname{Hom}(A,.) \cong_{\mathbf{Set}^{\mathcal{C}}} \operatorname{Hom}(B,) \implies A \cong_{\mathcal{C}} B.$$

Proof. Let $\alpha\colon \operatorname{Hom}(A,.) \Rightarrow \operatorname{Hom}(B,.)$ be a natural isomorphism of functors $\mathcal{C} \to \mathbf{Set}$. For $C \in \operatorname{Ob}(\mathcal{C})$, the $\alpha_C\colon \operatorname{Hom}_{\mathcal{C}^o}(C,A) \to \operatorname{Hom}_{\mathcal{C}^o}(C,B)$ are then bijections. For $f \in \operatorname{Hom}_{\mathcal{C}^o}(C,D)$ and $\varphi \in \operatorname{Hom}_{\mathcal{C}^o}(C,A)$, it holds that $\operatorname{Hom}(f,A)(\varphi) = \varphi \circ_{\mathcal{C}^o} f = f \circ \varphi = \operatorname{Hom}(A,f)(\varphi)$. Thus $\alpha\colon \operatorname{Hom}(.,A) \Rightarrow \operatorname{Hom}(.,B)$ is a natural isomorphism of functors $\mathcal{C}^o \to \mathbf{Set}$. According to Lemma III.5.18, the preimages of the Yoneda embedding are also isomorphic, i. e. $A \cong_{\mathcal{C}} B$. □

Example III.5.20. Let G, H be groups. For all groups X, let there exist a bijection $\alpha_X\colon \operatorname{Hom}(G,X) \to \operatorname{Hom}(H,X)$ with

$$\alpha_Y(f \circ \varphi) = f \circ \alpha_X(\varphi)$$

for all group homomorphisms $f\colon X \to Y$ and $\varphi\colon G \to X$. Then $\alpha\colon \operatorname{Hom}(G,.) \Rightarrow \operatorname{Hom}(H,.)$ is a natural isomorphism and Corollary III.5.19 shows $G \cong H$.

Definition III.5.21. A functor $\Phi\colon \mathcal{C} \to \mathcal{D}$ is called an *equivalence*, if a functor $\Psi\colon \mathcal{D} \to \mathcal{C}$ with $\Phi \circ \Psi \cong \mathrm{id}_{\mathcal{D}}$ and $\Psi \circ \Phi \cong \mathrm{id}_{\mathcal{C}}$ exists. If applicable, we call $\mathcal{C}$ and $\mathcal{D}$ equivalent and write $\mathcal{C} \approx \mathcal{D}$.

Remark III.5.22.

(i) Isomorphic categories are equivalent, but not vice versa (see Example III.5.24). We show in the following that many algebraic concepts are preserved by equivalences.

(ii) By definition, $\approx$ is reflexive and symmetric. From Lemma III.5.23 it follows easily that $\approx$ is also transitive. It is therefore an equivalence relation.

(iii) $\Phi\colon \mathcal{C} \to \mathcal{D}$ is an equivalence if and only if $\Phi\colon \mathcal{C}^o \to \mathcal{D}^o$ is an equivalence.

(iv) Let $\alpha\colon \Psi\Phi \Rightarrow \mathcal{C}$ be a natural isomorphism and $A \in \mathrm{Ob}(\mathcal{C})$. Then $\alpha_A\colon \Psi(\Phi(A)) \to A$ is an isomorphism in $\mathcal{C}$. For $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ we have

$$\Psi(\Phi(f)) = \alpha_B^{-1} \circ f \circ \alpha_A,$$

i.e. f and $\Psi(\Phi(f))$ differ only by isomorphisms from the left and right. This shows

- f monomorphism $\iff$ $\Phi(f)$ monomorphism.
- f epimorphism $\iff$ $\Phi(f)$ epimorphism.
- f isomorphism $\iff$ $\Phi(f)$ isomorphism.

Lemma III.5.23. *A functor $\Phi\colon \mathcal{C} \to \mathcal{D}$ is an equivalence if and only if Φ is full and faithful and for all $D \in \mathrm{Ob}(\mathcal{D})$ there exists a $C \in \mathrm{Ob}(\mathcal{C})$ with $\Phi(C) \cong D$.*

Proof. Let Φ be an equivalence and $\Psi\colon \mathcal{D} \to \mathcal{C}$ with natural isomorphisms $\alpha\colon \Psi\Phi \Rightarrow \mathrm{id}_{\mathcal{C}}$ and $\beta\colon \Phi\Psi \Rightarrow \mathrm{id}_{\mathcal{D}}$. Let $f, g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ with $\Phi(f) = \Phi(g)$. Then

$$f = \alpha_B \circ \Psi\Phi(f) \circ \alpha_A^{-1} = \alpha_B \circ \Psi\Phi(g) \circ \alpha_A^{-1} = g$$

holds and Φ is faithful. Analogously, Ψ is also faithful. Now let $g \in \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Phi(B))$ be given. For $f := \alpha_B \Psi(g) \alpha_A^{-1} \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ it then holds that

$$\Psi(g) = \alpha_B^{-1} \circ f \circ \alpha_A = \Psi\Phi(f).$$

Since Ψ is faithful, it follows that $g = \Phi(f)$ and Φ is full. Finally, let $D \in \mathrm{Ob}(\mathcal{D})$ be given. Set $C := \Psi(D) \in \mathrm{Ob}(\mathcal{C})$. Then $\beta_D\colon \Phi(C) \to D$ is an isomorphism.

Conversely, let Φ be full and faithful and for all $D \in \mathrm{Ob}(\mathcal{D})$ let there exist a $C_D \in \mathrm{Ob}(\mathcal{C})$ with $\Phi(C_D) \cong D$. We set $\Psi(D) := C_D$ and choose isomorphisms $\beta_D\colon \Phi(\Psi(D)) \to D$. For $g \in \mathrm{Hom}_{\mathcal{D}}(D, E)$ let

$$\Psi(g) := \Phi^{-1}(\beta_E^{-1} \circ g \circ \beta_D) \in \mathrm{Hom}_{\mathcal{C}}(\Psi(D), \Psi(E)).$$

Then $\Psi(\mathrm{id}_D) = \mathrm{id}_{\Psi(D)}$ holds. For $h \in \mathrm{Hom}_{\mathcal{D}}(E, F)$ we have

$$\begin{aligned}\Psi(h \circ g) &= \Phi^{-1}(\beta_E^{-1} h \beta_E \circ \beta_E^{-1} g \beta_D) = \Phi^{-1}(\Phi(\Phi^{-1}(\beta_E^{-1} h \beta_E)) \circ \Phi(\Phi^{-1}(\beta_E^{-1} g \beta_D))) \\ &= \Phi^{-1}(\beta_E^{-1} h \beta_E) \circ \Phi^{-1}(\beta_E^{-1} g \beta_D) = \Psi(h) \circ \Psi(g).\end{aligned}$$

Thus $\Psi\colon \mathcal{D} \to \mathcal{C}$ is a functor. Furthermore, $\beta_E \circ \Phi\Psi(g) = g \circ \beta_D$ and $\beta\colon \Phi\Psi \to \mathrm{id}_{\mathcal{D}}$ is a natural isomorphism. By construction, Ψ is faithful. For $f \in \mathrm{Hom}_{\mathcal{C}}(\Psi(D), \Psi(E))$ let $g := \beta_E \Phi(f) \beta_D^{-1} \in \mathrm{Hom}_{\mathcal{D}}(D, E)$. Then $\Psi(g) = f$ holds and Ψ is full. Let $A \in \mathrm{Ob}(\mathcal{C})$ be given. By definition of Ψ there exists a $C \in \mathcal{C}$ with $\Phi(C) = \Phi(A)$ and $\Psi(\Phi(A)) = C$. Now $\Phi^{-1}(\mathrm{id}_{\Phi(A)})\colon A \to C$ is an isomorphism. Thus Ψ satisfies the same requirements as Φ. By what has already been shown, there exists a natural isomorphism $\alpha\colon \Psi\Phi \Rightarrow \mathrm{id}_{\mathcal{C}}$. □

Example III.5.24.

(i) Let K be a field and $\Phi\colon K\text{-}\mathbf{mat}^o \to {}_K\mathbf{mod}$, $n \mapsto K^n$ with $\Phi(A)(v) := Av \in K^m$ for $A \in K^{m \times n}$ and $v \in K^n$. Obviously, Φ is a full and faithful functor. Since every finite-dimensional K-vector space is isomorphic to some K^n, Φ is an equivalence according to Lemma III.5.23. Since there are uncountably many (finite-dimensional) vector spaces, $K\text{-}\mathbf{mat}^o$ and ${}_K\mathbf{mod}$ cannot be isomorphic.

(ii) Suppose there exists an equivalence $\Phi\colon \mathbf{Set} \to \mathbf{Set}^o$. Let A and B be sets with $|A| = 1$ and $|B| = 2$. Then

$$2 = |\operatorname{Hom}_{\mathbf{Set}}(A, B)| = |\operatorname{Hom}_{\mathbf{Set}^o}(\Phi(A), \Phi(B))| = |\operatorname{Hom}_{\mathbf{Set}}(\Phi(B), \Phi(A)|.$$

From this it follows that $|\Phi(B)| = 1$ and $|\Phi(A)| = 2$ and one has the contradiction $|\operatorname{Hom}_{\mathbf{Set}}(A, A)| \neq |\operatorname{Hom}_{\mathbf{Set}}(\Phi(A), \Phi(A))|$. Thus $\mathbf{Set} \not\approx \mathbf{Set}^o$ holds.

Definition III.5.25. Let $\mathcal{C}$ be a small category. One obtains a *skeleton category* $\bar{\mathcal{C}}$ of $\mathcal{C}$ by choosing a system of representatives for the isomorphism classes of objects in $\mathcal{C}$ for $\operatorname{Ob}(\mathcal{C})$ and setting $\operatorname{Hom}_{\bar{\mathcal{C}}}(A, B) := \operatorname{Hom}_{\mathcal{C}}(A, B)$.[2]

Theorem III.5.26. *For small categories $\mathcal{C}$ and $\mathcal{D}$, $\mathcal{C} \approx \bar{\mathcal{C}}$ and $\mathcal{C} \approx \mathcal{D} \iff \bar{\mathcal{C}} \cong \bar{\mathcal{D}}$ hold.*

Proof. Lemma III.5.23 shows that the embedding $\Phi\colon \bar{\mathcal{C}} \to \mathcal{C}$, $A \mapsto A$, $f \mapsto f$ is an equivalence. Now let $\Phi\colon \mathcal{C} \to \mathcal{D}$ be an equivalence and $\bar{\mathcal{D}} := \Phi(\bar{\mathcal{C}})$ a subcategory of $\mathcal{D}$. According to Lemma III.5.23, for every $D \in \operatorname{Ob}(\mathcal{D})$ there exists a $C \in \operatorname{Ob}(\mathcal{C})$ with $\Phi(C) = D$. Let $\alpha_C\colon C \to \overline{C} \in \bar{\mathcal{C}}$ be an isomorphism. Then $\Phi(\alpha_C)\colon D \to \Phi(\overline{C})$ is also an isomorphism. Let also $\overline{B} \in \operatorname{Ob}(\bar{\mathcal{C}})$ with $\Phi(\overline{B}) \cong D$. Then $\overline{B} = \overline{C}$ and $B = C$ follows from Lemma III.5.18. This shows that $\bar{\mathcal{D}}$ is a skeleton category of $\mathcal{D}$. Furthermore, the restricted functor $\overline{\Phi}\colon \bar{\mathcal{C}} \to \bar{\mathcal{D}}$ is an isomorphism according to Exercise III.23.

Now assume that an isomorphism $\overline{\Phi}\colon \bar{\mathcal{C}} \to \bar{\mathcal{D}}$ between skeleton categories is given. For $C \in \operatorname{Ob}(\mathcal{C})$ and $D \in \operatorname{Ob}(\mathcal{D})$ we choose isomorphisms $\alpha_C\colon C \to \overline{C} \in \operatorname{Ob}(\bar{\mathcal{C}})$ and $\beta_D\colon D \to \overline{D} \in \operatorname{Ob}(\bar{\mathcal{D}})$. Let $\Phi\colon \mathcal{C} \to \mathcal{D}$, $C \mapsto \overline{\Phi}(\overline{C})$ with $\Phi(f) := \overline{\Phi}(\alpha_B f \alpha_A^{-1})$ for $f \in \operatorname{Hom}_{\mathcal{C}}(A, B)$. Obviously, Φ is a functor. Since $\overline{\Phi}$ is full and faithful, Φ is as well. For every $D \in \operatorname{Ob}(\mathcal{D})$ there also exists a $\overline{C} \in \operatorname{Ob}(\bar{\mathcal{C}})$ with $\Phi(\overline{C}) = \overline{D} \cong D$. According to Lemma III.5.23, Φ is an equivalence. □

Remark III.5.27. According to Theorem III.5.26, a skeleton category of a small category $\mathcal{C}$ is uniquely determined up to equivalence. It is also the "smallest" category equivalent to $\mathcal{C}$.

Definition III.5.28. Let $\Phi\colon \mathcal{C} \to \mathcal{D}$ and $\Psi\colon \mathcal{D} \to \mathcal{C}$ be functors between locally small categories $\mathcal{C}, \mathcal{D}$. One calls Φ *left adjoint* to Ψ (and Ψ *right adjoint* to Φ), if the functors

$$\operatorname{Hom}(\Phi(.), .)\colon \mathcal{C}^o \times \mathcal{D} \to \mathbf{Set},\ (A, B) \mapsto \operatorname{Hom}_{\mathcal{D}}(\Phi(A), B),\ \operatorname{Hom}(\Phi(f_A), f_B)(\varphi) = f_B \circ \varphi \circ \Phi(f_A),$$
$$\operatorname{Hom}(., \Psi(.))\colon \mathcal{C}^o \times \mathcal{D} \to \mathbf{Set},\ (A, B) \mapsto \operatorname{Hom}_{\mathcal{C}}(A, \Psi(B)),\ \operatorname{Hom}(f_A, \Psi(f_B))(\varphi) = \Psi(f_B) \circ \varphi \circ f_A$$

are isomorphic.

Example III.5.29. Let $\mathcal{C} := \mathbf{Set}$ and $\mathcal{D} := {}_K\mathbf{Mod}$ be the category of K-vector spaces for a field K. Let $\Psi\colon \mathcal{D} \to \mathcal{C}$ be the forgetful functor and $\Phi\colon \mathcal{C} \to \mathcal{D}$, $B \mapsto \coprod_{b \in B} K$. We consider B as the standard basis of $\Phi(B)$. For $f\colon B \to C$ let $\Phi(f)\colon \coprod_{b \in B} K \to \coprod_{c \in C} K$, $(x_b)_{b \in B} \mapsto \sum_{b \in B} x_{f(b)}$. Obviously, Φ is a functor. For $B \in \operatorname{Ob}(\mathcal{D})$ and $V \in \operatorname{Ob}(\mathcal{C})$ let

$$\alpha_{(B,V)}\colon \operatorname{Hom}_{\mathcal{D}}(\Phi(B), V) \to \operatorname{Hom}_{\mathcal{C}}(B, V), \qquad f \mapsto f_{|B}$$

be the restriction. Since every homomorphism $\Phi(B) \to V$ is uniquely determined by the images of B, $\alpha_{(B,V)}$ is bijective. For $f = (f_B, f_V) \in \operatorname{Hom}_{\mathcal{C}^o \times \mathcal{D}}((B, V), (C, W))$ and $\varphi \in \operatorname{Hom}_{\mathcal{D}}(\Phi(B), V)$ it holds that

$$\big(\alpha_{(C,W)} \circ \operatorname{Hom}(\Phi(f_B), f_V)\big)(\varphi) = (f_V \varphi \Phi(f_B))_C = f_V \varphi_{|B} f_C = \big(\operatorname{Hom}(f_B, \Psi(f_V)) \circ \alpha_{(B,V)}\big)(\varphi).$$

[2] The assumption "small" can be generalized so that, for example, $\overline{\mathbf{Grp}}$ is also well-defined.

Therefore $\alpha\colon \mathrm{Hom}(\Phi(.),.) \Rightarrow \mathrm{Hom}(.,\Psi(.))$ is a natural isomorphism and Φ is left-adjoint to Ψ.

Definition III.5.30. Let $(A_i)_{i\in I}$ be a family of objects of a category $\mathcal{C}$.

- One calls $P \in \mathrm{Ob}(\mathcal{C})$ a *product* of (A_i), if morphisms $p_i\colon P \to A_i$ for $i \in I$ exist with the following universal property: For every family of morphisms $f_i\colon C \to A_i$ there exists exactly one morphism $f\colon C \to P$ with $p_i \circ f = f_i$ for $i \in I$. If applicable, one calls p_i the i-th *projections* of P.
- One calls $Q \in \mathrm{Ob}(\mathcal{C})$ a *coproduct* of (A_i), if morphisms $q_i\colon A_i \to Q$ for $i \in I$ exist with the following universal property: For every family of morphisms $f_i\colon A_i \to C$ there exists exactly one morphism $f\colon Q \to C$ with $f \circ q_i = f_i$ for $i \in I$. If applicable, one calls q_i the i-th *injections* of Q.

Remark III.5.31.

(i) (Co)products do not have to exist in every category.

(ii) A product (resp. coproduct) of (A_i) in $\mathcal{C}$ corresponds to a coproduct (resp. product) of (A_i) in $\mathcal{C}^o$ (all arrows are reversed).

Lemma III.5.32. *Let $(A_i)_{i\in I}$ be a family of objects of a category $\mathcal{C}$.*

(i) If $P, P' \in \mathrm{Ob}(\mathcal{C})$ are products of (A_i) w.r.t. p_i resp. p_i', then there exists exactly one isomorphism $f\colon P' \to P$ with $p_i f = p_i'$ for $i \in I$.

(ii) If $Q, Q' \in \mathrm{Ob}(\mathcal{C})$ are coproducts of (A_i) w.r.t. q_i resp. q_i', then there exists exactly one isomorphism $f\colon Q' \to Q$ with $f q_i' = q_i$ for $i \in I$.

Proof.

(i) The universal property of P applied to $f_i = p_i'$ yields exactly one $f\colon P' \to P$ with $p_i f = p_i'$ for $i \in I$. Analogously, there exists a $g\colon P' \to P$ with $p_i' g = p_i$ for $i \in I$. For $fg\colon P \to P$, it now holds that $p_i fg = p_i$. According to the universal property of P, id_P is the only morphism with this property. This shows $fg = \mathrm{id}_P$ and analogously $gf = \mathrm{id}_{P'}$. Thus f is an isomorphism and is uniquely determined by the equation $p_i f = p_i'$.

(ii) Applying (i) to the products Q and Q' of (A_i) in $\mathcal{C}^o$, one obtains exactly one isomorphism $f\colon Q' \to Q$ in $\mathcal{C}^o$ with $q_i f = q_i'$ for $i \in I$. Now $f\colon Q \to Q'$ is an isomorphism in $\mathcal{C}$ with $f q_i = q_i'$ for $i \in I$. The specified isomorphism is f^{-1}. □

Example III.5.33.

(i) The product of (A_i) in **Set**, **Grp** or **Ab** is the usual Cartesian (direct) product $\bigtimes_{i\in I} A_i$. The coproduct in **Set** is the disjoint union $\bigsqcup_{i\in I} A_i$, while in **Ab** it is the well-known coproduct $\coprod_{i\in I} A_i$ (in the case $|I| < \infty$, the product and coproduct coincide here). In **Grp**, however, the coproduct is the *free product*, the existence of which must first be proven.[3]

(ii) Let P be the product of $A_i := A$ for $i \in I$ with respect to p_i. Then there exists exactly one $d\colon A \to P$ with $p_i d = \mathrm{id}_A$ for $i \in I$. One calls d the *diagonal morphism* with respect to P. For the coproduct Q of A_i, there exists analogously the *codiagonal morphism* $c\colon Q \to A$ with $c q_i = \mathrm{id}_A$ for all $i \in I$.

[3] See lecture notes Combinatorial Group Theory

III.6 Morita Theory

Remark III.6.1. Groups and rings can, as is well known, be studied through their representations and modules. Morita theory is the study of the module category of an arbitrary ring R. In contrast to general categories, ${}_R\mathbf{Mod}$ has the additional property that one can add morphisms (with $f, g\colon M \to N$, as is well known, $f+g\colon M \to N$, $m \mapsto f(m)+g(m)$ is also a homomorphism).[1] Furthermore, $M \times N$ is both the product and the coproduct of R-modules with respect to the canonical projections and injections. We show that equivalent module categories preserve some useful properties. With Morita's Theorem, we provide a handy criterion to recognize when the module categories of two rings are equivalent.

Lemma III.6.2. *Let R, S be rings and $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ an equivalence. For every family of R-modules $(M_i)_{i\in I}$ it holds that*

$$\Phi\Big(\bigtimes_{i\in I} M_i\Big) \simeq \bigtimes_{i\in I} \Phi(M_i), \qquad \Phi\Big(\coprod_{i\in I} M_i\Big) \simeq \coprod_{i\in I} \Phi(M_i).$$

Proof. Let $M := \bigtimes_{i\in I} M_i$, $N := \bigtimes_{i\in I} \Phi(M_i)$ and $p_i\colon M \to M_i$, $p_i'\colon N \to \Phi(M_i)$ be the i-th projections. Let $\Psi\colon {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$, and $\alpha\colon \Psi\Phi \Rightarrow \mathrm{id}_{{}_R\mathbf{Mod}}$ be a natural isomorphism. Because of $\Phi(p_i) \in \mathrm{Hom}_S(\Phi(M), \Phi(M_i))$, $\Psi(p_i') \in \mathrm{Hom}_R(\Psi(N), \Psi(\Phi(M_i))$ and $\alpha_{M_i} \in \mathrm{Hom}_R(\Psi(\Phi(M_i)), M_i)$,

$$\begin{aligned} f\colon \Phi(M) \to N, &\qquad x \mapsto \big(\Phi(p_i)(x)\big)_{i\in I}, \\ g\colon \Psi(N) \to M, &\qquad y \mapsto \big((\alpha_{M_i} \circ \Psi(p_i'))(y)\big)_{i\in I} \end{aligned}$$

are S- and R-linear respectively. Since Ψ is faithful, we can define $h := \Psi^{-1}(\alpha_M^{-1} \circ g) \in \mathrm{Hom}_S(N, \Phi(M))$. Then it holds that

$$\begin{aligned} \Psi(p_i' \circ f \circ h) &= \Psi(\Phi(p_i) \circ h) = \Psi(\Phi(p_i)) \circ \Psi(h) = \Psi(\Phi(p_i)) \circ \alpha_M^{-1} \circ g \\ &= \alpha_{M_i}^{-1} \circ p_i \circ g = \alpha_{M_i}^{-1} \circ \alpha_{M_i} \circ \Psi(p_i') = \Psi(p_i'). \end{aligned}$$

This implies $p_i' f h = p_i'$. Since this holds for all $i \in I$, one obtains $fh = \mathrm{id}_N$.

Analogously, it holds that

$$p_i \circ g \circ \Psi(f) = \alpha_{M_i} \circ \Psi(p_i') \circ \Psi(f) = \alpha_{M_i} \circ \Psi(p_i' \circ f) = \alpha_{M_i} \circ \Psi(\Phi(p_i)) = p_i \circ \alpha_M$$

for all $i \in I$. It follows that $g \circ \Psi(f) = \alpha_M$ and

$$\Psi(h \circ f) = \Psi(h) \circ \Psi(f) = \alpha_M^{-1} \circ g \circ \Psi(f) = \mathrm{id}_{\Psi\Phi(M)} = \Psi(\mathrm{id}_{\Phi(M)}).$$

This shows $hf = \mathrm{id}_{\Phi(M)}$ and $f\colon \Phi(M) \to N$ is an S-isomorphism. The same proof shows the corresponding isomorphism for the coproduct. □

[1] One speaks of *abelian* categories.

Lemma III.6.3. *Let R, S be rings and $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ an equivalence. For R-modules A, B it holds that:*

(i) For the trivial module $A = 0$, $\Phi(A) = 0$ also holds.

(ii) For the trivial map $f\colon A \to B$, $a \mapsto 0$, $\Phi(f)$ is also trivial.

(iii) $\Phi\colon \mathrm{Hom}_R(A, B) \to \mathrm{Hom}_S(\Phi(A), \Phi(B))$ is a group isomorphism.

Proof.

(i) Every module $B \neq 0$ possesses, besides id_B, the trivial map $B \to B$. Therefore, the trivial module A is the only object in ${}_R\mathbf{Mod}$ with $|\mathrm{Hom}(A, A)| = 1$. Since Φ is full and faithful, it follows that $|\mathrm{Hom}(\Phi(A), \Phi(A))| = 1$ and $\Phi(A) = 0$.

(ii) The trivial map f is the only morphism with $g \circ f = f$ for all morphisms $g\colon B \to B$. Since Φ is full, $\Phi(f)$ must also be trivial.

(iii) According to Lemma III.5.23, $\Phi\colon \mathrm{Hom}_R(A, B) \to \mathrm{Hom}_S(\Phi(A), \Phi(B))$ is bijective. It remains to show

$$\Phi(f + g) = \Phi(f) + \Phi(g)$$

for $f, g \in \mathrm{Hom}_R(A, B)$. Let $A_1 := A =: A_2$. Let $p_i\colon A_1 \times A_2 \to A_i$, $p_i'\colon \Phi(A_1) \times \Phi(A_2) \to \Phi(A_i)$ and $q_i\colon A_i \to A_1 \times A_2$, $q_i'\colon \Phi(A_i) \to \Phi(A_1) \times \Phi(A_2)$ be the projections and injections. The proof of Lemma III.6.2 yields the isomorphism

$$\gamma\colon \Phi(A_1 \times A_2) \to \Phi(A_1) \times \Phi(A_2), \qquad x \mapsto \big(\Phi(p_1)(x), \Phi(p_2)(x)\big).$$

Thus $p_i'\gamma = \Phi(p_i)$ holds for $i = 1, 2$. According to (ii), $\Phi(p_i q_j) = 0$ for $i \neq j$. From this it follows that

$$\gamma\Phi(q_i) = (q_1'p_1' + q_2'p_2')\gamma\Phi(q_i) = q_1'\Phi(p_1)\Phi(q_i) + q_2'\Phi(p_2)\Phi(q_i) = q_i'\Phi(p_i q_i) = q_i'\Phi(\mathrm{id}_{A_i}) = q_i'$$

for $i = 1, 2$. Let $d\colon A \to A_1 \times A_2$, $a \mapsto (a, a)$ be the diagonal morphism (Example III.5.33) and $c\colon A_1 \times A_2 \to B$, $(x, y) \mapsto f(x) + g(y)$. Then $f + g = c \circ d$ holds. For

$$d' := \gamma\Phi(d)\colon \Phi(A) \to \Phi(A_1) \times \Phi(A_2)$$

we have $p_i'd' = \Phi(p_i d) = \Phi(\mathrm{id}_{A_i}) = \mathrm{id}_{\Phi(A_i)}$ and it follows that $d'(x) = (x, x)$ for $x \in \Phi(A)$. For

$$c' := \Phi(c)\gamma^{-1}\colon \Phi(A_1) \times \Phi(A_2) \to \Phi(B)$$

one has $c'q_i' = \Phi(c)\Phi(q_i) = \Phi(f_i)$ with $f_1 = f$ and $f_2 = g$. This shows $c'(x, y) = \Phi(f)(x) + \Phi(g)(y)$ and

$$\Phi(f + g) = \Phi(c \circ d) = \Phi(c) \circ \Phi(d) = c'd' = \Phi(f) + \Phi(g). \qquad \square$$

Remark III.6.4. Not every functor $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ satisfies $\Phi(f + g) = \Phi(f) + \Phi(g)$. Let for example $\Phi(A) := S$ and $\Phi(f) := \mathrm{id}_S$ for all R-modules A and R-homomorphisms f. Obviously Φ is a functor and $\Phi(f + f) = \mathrm{id}_S \neq 2\,\mathrm{id}_S = \Phi(f) + \Phi(f)$.

Theorem III.6.5. *Let R, S be rings and $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ an equivalence. Then there exists for every R-module M a bijection $\hat{\Phi}\colon \{N : N \leq M\} \to \{N : N \leq \Phi(M)\}$ with*

$$N \leq N' \Longleftrightarrow \hat{\Phi}(N) \leq \hat{\Phi}(N'), \qquad \hat{\Phi}(N + N') = \hat{\Phi}(N) + \hat{\Phi}(N'), \qquad \hat{\Phi}(N \cap N') = \hat{\Phi}(N) \cap \hat{\Phi}(N').$$

Proof. Since $N \leq M$ does not necessarily imply $\Phi(N) \leq \Phi(M)$, we must take a detour. Let $\Psi\colon {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$, and $\alpha\colon \Psi\Phi \Rightarrow \mathrm{id}_{{}_R\mathbf{Mod}}$ be a natural equivalence. For submodules $N \leq M$ let $\nu_N^M\colon N \hookrightarrow M$ be the inclusion map. Then $\Phi(\nu_N^M) \in \mathrm{Hom}_S(\Phi(N), \Phi(M))$. We define

$$\begin{aligned}
&\hat{\Phi}\colon \{N : N \leq M\} \to \{N : N \leq \Phi(M)\}, \qquad N \mapsto \Phi(\nu_N^M)(\Phi(N)),\\
&\hat{\Psi}\colon \{N : N \leq \Phi(M)\} \to \{N : N \leq \Psi\Phi(M)\}, \qquad N \mapsto \Psi(\nu_N^{\Phi(M)})(\Psi(N)),\\
&\hat{\alpha}\colon \{N : N \leq \Psi\Phi(M)\} \to \{N : N \leq M\}, \qquad N \mapsto \alpha_M(N).
\end{aligned}$$

With ν_N^M, $\Phi(\nu_N^M)$ is injective (Theorem III.5.7+Remark III.5.22). Thus there exists an S-isomorphism $f\colon \Phi(N) \to \hat{\Phi}(N)$ with $\Phi(\nu_N^M) = \nu_{\hat{\Phi}(N)}^{\Phi(M)} \circ f$. This shows

$$\begin{aligned}
\hat{\alpha}\big(\hat{\Psi}(\hat{\Phi}(N))\big) &= \big(\alpha_M \circ \Psi(\nu_{\hat{\Phi}(N)}^{\Phi(M)})\big)(\Psi(\hat{\Phi}(N))) = \big(\alpha_M \circ \Psi(\nu_{\hat{\Phi}(N)}^{\Phi(M)}) \circ \Psi(f)\big)(\Psi\Phi(N))\\
&= \big(\alpha_M \circ \Psi(\nu_{\hat{\Phi}(N)}^{\Phi(M)} \circ f)\big)(\Psi\Phi(N)) = \big(\alpha_M \circ \Psi(\Phi(\nu_N^M))\big)(\Psi\Phi(N))\\
&= \big(\nu_N^M \circ \alpha_N)\big)(\Psi\Phi(N)) = \nu_N^M(N) = N
\end{aligned}$$

and $\hat{\alpha}\hat{\Psi}\hat{\Phi} = \mathrm{id}$. Since α_M is bijective, $\hat{\alpha}$ is also bijective. Therefore $\hat{\Psi}$ is surjective and $\hat{\Phi}$ is injective. Since a natural isomorphism $\beta\colon \Phi\Psi \Rightarrow \mathrm{id}$ also exists, one analogously obtains the injectivity of $\hat{\Psi}$ and the surjectivity of $\hat{\Phi}$. Overall, $\hat{\Phi}$ is bijective.

From $N \leq N'$ follows $\nu_N^M = \nu_{N'}^M \circ \nu_N^{N'}$ and

$$\hat{\Phi}(N) = \Phi(\nu_N^M)(\Phi(N)) \leq \Phi(\nu_{N'}^M)(\Phi(N')) = \hat{\Phi}(N').$$

For $\hat{\Phi}(N) \leq \hat{\Phi}(N')$, analogously $\hat{\Psi}\hat{\Phi}(N) \leq \hat{\Psi}\hat{\Phi}(N')$ and

$$N = \alpha_M(\hat{\Psi}\hat{\Phi}(N)) \leq \alpha_M(\hat{\Psi}\hat{\Phi}(N')) = N'.$$

For arbitrary submodules $N, N' \leq M$, $N + N'$ is the smallest (w.r.t. inclusion) submodule of M containing N and N'. Therefore $\Phi(N + N')$ is the smallest submodule of $\hat{\Phi}(M)$ containing $\hat{\Phi}(N)$ and $\hat{\Phi}(N')$. This shows $\hat{\Phi}(N + N') = \hat{\Phi}(N) + \hat{\Phi}(N')$. Since $N \cap N'$ is the largest submodule contained in N and in N', it follows accordingly that $\hat{\Phi}(N \cap N') = \hat{\Phi}(N) \cap \hat{\Phi}(N')$. □

Theorem III.6.6. *Let R, S be rings and $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ an equivalence. For every R-module M:*

(i) M finitely generated $\iff$ $\Phi(M)$ finitely generated.

(ii) M (semi)simple $\iff$ $\Phi(M)$ (semi)simple.

(iii) M indecomposable $\iff$ $\Phi(M)$ indecomposable.

(iv) M projective $\iff$ $\Phi(M)$ projective.

(v) M Noetherian (Artinian) $\iff$ $\Phi(M)$ Noetherian (Artinian).

Proof. Let $\Psi\colon {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$ be an equivalence with $\Psi\Phi \cong \mathrm{id}$. Because of $M \simeq \Psi\Phi(M)$, it suffices to show "⇒" in each case.

(i) Let $f\colon \coprod_{i\in I} S \to \Phi(M)$ be an epimorphism. According to Theorem III.5.7, Remark III.5.22 and Lemma III.6.2, there exists an epimorphism

$$g\colon \coprod_{i\in I} \Psi(S) \simeq \Psi\Big(\coprod_{i\in I} S\Big) \xrightarrow{\Psi(f)} \Psi\Phi(M) \simeq M.$$

Since M is finitely generated, there exists a finite subset $J \subseteq I$ with $g\big(\coprod_{j\in J} \Psi(S)\big) = M$. Therefore, there is an epimorphism

$$\coprod_{j\in J} S \simeq \coprod_{j\in J} \Phi\Psi(S) \simeq \Phi\Big(\coprod_{j\in J} \Psi(S)\Big) \to \Phi(M).$$

Consequently, $\Phi(M)$ is finitely generated.

(ii) According to Theorem III.6.5, M is simple if and only if $\Phi(M)$ is simple. If M is semisimple, i.e., a coproduct of simple modules, then so is $\Phi(M)$ according to Lemma III.6.2.

(iii) Follows from Lemma III.6.2.

(iv) Let M be projective, $f \in \mathrm{Hom}_S(\Phi(M), N)$ and $g\colon L \to N$ an S-epimorphism. Since $\Psi\Phi(M)$ is projective, there exists an $\hat{h} \in \mathrm{Hom}_S(\Psi\Phi(M), \Psi(L))$ with $\Psi(g) \circ \hat{h} = \Psi(f)$. Since Ψ is full, there exists $h \in \mathrm{Hom}_R(\Phi(M), \Psi(L))$ with $\Psi(h) = \hat{h}$. Now $\Psi(g \circ h) = \Psi(f)$ and $g \circ h = f$, since Ψ is faithful. Thus $\Phi(M)$ is projective.

(v) Follows from Theorem III.6.5. □

Remark III.6.7. Attention: If M is free, then $\Phi(M)$ does not necessarily have to be free in the situation of Theorem III.6.6. Likewise, there is no connection between the minimal number of generators of M and $\Phi(M)$ (Remark III.6.43).

Theorem III.6.8. *Let R and S be rings with ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$. Then there exists a bijection $\Omega\colon \{I : I \trianglelefteq R\} \to \{I : I \trianglelefteq S\}$ with*

$$I \subseteq J \Longleftrightarrow \Omega(I) \subseteq \Omega(J), \qquad \Omega(I+J) = \Omega(I) + \Omega(J),$$
$$\Omega(I \cap J) = \Omega(I) \cap \Omega(J), \qquad \Omega(\mathrm{J}(R)) = \mathrm{J}(S).$$

Proof. With the usual notation, let $\Psi\Phi \cong \mathrm{id}$ be a natural isomorphism. For $I \trianglelefteq R$ and $J \trianglelefteq S$ we define $\Omega(I) := \mathrm{Ann}_S(\Phi(R/I)) \trianglelefteq S$ and $\Delta(J) := \mathrm{Ann}_R(\Psi(S/J)) \trianglelefteq R$. With a generating system X of $\Psi(S/J)$ one obtains an R-epimorphism

$$\coprod_{x\in X} R/\Delta(J) \to \Psi(S/J), \qquad (r_x + \Phi(S/J))_x \mapsto \sum_{x\in X} r_x x$$

and an R-monomorphism

$$R/\Delta(J) \to \prod_{x\in X} \Psi(S/J), \qquad r + \Delta(J) \mapsto (rx)_{x\in X}.$$

By applying Φ, an S-epimorphism and an S-monomorphism result:

$$\coprod_{x\in X} \Phi(R/\Delta(J)) \simeq \Phi\Big(\coprod_{x\in X} R/\Delta(J)\Big) \to \Phi\Psi(S/J) \simeq S/J,$$
$$\Phi(R/\Delta(J)) \to \Phi\Big(\prod_{x\in X} \Psi(S/J)\Big) \simeq \coprod_{x\in X} \Phi\Psi(S/J) \simeq \coprod_{x\in X} S/J.$$

This shows

$$J = \mathrm{Ann}_S(S/J) = \mathrm{Ann}_S\Big(\prod_{x\in X} S/J\Big) \subseteq \mathrm{Ann}_S(\Phi(R/\Delta(J))) = \mathrm{Ann}_S\Big(\coprod_{x\in X} \Phi(R/\Delta(J))\Big) \subseteq \mathrm{Ann}_S(S/J)$$

and $J = \Omega(\Delta(J))$. Completely analogously, $I = \Delta(\Omega(I))$ results for $I \trianglelefteq R$. Now let $I \subseteq I'$. Then $f\colon R/I \to R/I'$, $r + I \mapsto r + I'$ and $\Phi(f)$ are epimorphisms. This shows

$$\Omega(I) = \mathrm{Ann}_S(\Phi(R/I)) \subseteq \mathrm{Ann}_S(\Phi(R/I')) = \Omega(I').$$

Conversely, from $\Omega(I) \subseteq \Omega(I')$ it follows that $I = \Delta(\Omega(I)) \subseteq \Delta(\Omega(I')) = I'$. From this follows $\Omega(I + I') = \Omega(I) + \Omega(I')$ and $\Omega(I \cap I') = \Omega(I) \cap \Omega(I')$ as in Theorem III.6.5.

For the last assertion, let N be a simple S-module. According to Theorem III.6.6, $\Psi(N)$ is a simple R-module. For $x \in \Psi(N) \setminus \{0\}$, $R/\mathrm{J}(R) \to \Psi(N)$, $r + \mathrm{J}(R) \mapsto rx$ is a well-defined R-epimorphism according to Lemma II.8.11. Thus $\Phi(R/\mathrm{J}(R)) \to \Phi\Psi(N) \simeq N$ is also an epimorphism and it follows that $\Omega(\mathrm{J}(R)) \subseteq \mathrm{Ann}_S(N)$. From Lemma II.8.11 one obtains $\Omega(\mathrm{J}(R)) \subseteq \mathrm{J}(S)$. Analogously, $\mathrm{J}(R) = \Delta(\Omega(\mathrm{J}(R))) \subseteq \Delta(\mathrm{J}(S)) \leq \mathrm{J}(R)$ and $\Omega(\mathrm{J}(R)) = \mathrm{J}(S)$ hold. □

Theorem III.6.9. *Let R and S be rings with ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$. Then*

(i) R is (semi)simple $\iff$ S is (semi)simple.

(ii) R is Noetherian (Artinian) $\iff$ S is Noetherian (Artinian).

Proof. According to Theorem III.6.8, R is simple if and only if S is simple. The other statements follow from Lemma II.8.4 and Theorem III.6.6. □

Remark III.6.10. If R is local, then S does not necessarily have to be local in the situation of Theorem III.6.9 (Example III.6.36).

Definition III.6.11. Let R and S be rings.

- An *R-S-bimodule* M is an R-left module and at the same time an S-right module with $(rm)s = r(ms)$ for all $m \in M$, $r \in R$ and $s \in S$.
- An *R-S-homomorphism* $f\colon M \to N$ between R-S-bimodules M and N is an R-homomorphism and at the same time an S-homomorphism, i. e. $f(r(m + m')s) = rf(m)s + rf(m')s$ for $r \in R$, $s \in S$ and $m, m' \in M$.

Let ${}_R\mathbf{Mod}_S$ (resp. ${}_R\mathbf{mod}_S$) be the category of (finitely generated) R-S-bimodules.

Example III.6.12.

(i) Every ideal $I \trianglelefteq R$ is an R-R-bimodule and the inclusion $I \hookrightarrow R$ is an R-R-homomorphism.

(ii) As is well known, every R-left module is an R^o-right module. Therefore, an R-S-bimodule is an S^o-R^o-bimodule.

(iii) Since every R-left module M is an abelian group with respect to $+$, M is an R-$\mathbb{Z}$-bimodule. All statements about bimodules can thus be transferred to left or right modules. If R is commutative, then M is an R-R-bimodule with $m \cdot r := rm$ for $r \in R$ and $m \in M$.

(iv) For $n, m \in \mathbb{N}$, $R^{n\times m}$ is an $R^{n\times n}$-$R^{m\times m}$-bimodule, because matrix multiplication is associative.

(v) Let M be an S-right module and $R := \mathrm{End}_S(M)$. By $\varphi \cdot m := \varphi(m)$ for $\varphi \in R$ and $m \in M$, M becomes an R-left module (Remark II.6.11). Because of $(\varphi m)s = \varphi(m)s = \varphi(ms) = \varphi(ms)$ for $s \in S$, M is an R-S-bimodule.

(vi) Let M be an R-S-bimodule and N be an R-T-bimodule. Then $\mathrm{Hom}_R(M,N)$ is an S-T-bimodule with $(s\varphi t)(m) := \varphi(ms)t$ for $s \in S$, $t \in T$ and $m \in M$ (verify). If N is a T-S-bimodule, then $\mathrm{Hom}_S(M,N)$ is a T-R-bimodule with $(t\varphi r)(m) := t\varphi(rm)$.

(vii) As usual, one defines submodules of bimodules and mono-, epi- and isomorphisms. The homomorphism theorem and the isomorphism theorems naturally also hold for bimodules.

Remark III.6.13. In Definition III.3.16, we introduced the tensor product of modules over group algebras. In Exercise II.53, the tensor product for modules over commutative rings was constructed. For arbitrary rings, the tensor product of modules is in general only a $\mathbb{Z}$-module. With the help of bimodules, one can improve the situation.

Definition III.6.14. Let R, S, T be rings, M an R-S-bimodule and N an S-T-bimodule.

- Let A be the free abelian group with basis $\{e_{m,n} : (m,n) \in M \times N\}$. Let B be the subgroup of A generated by the elements

$$e_{m+m',n} - e_{m,n} - e_{m',n}, \qquad e_{m,n+n'} - e_{m,n} - e_{m,n'}, \qquad e_{ms,n} - e_{m,sn}$$

  with $m, m' \in M$, $n, n' \in N$ and $s \in S$. We define the *tensor product*

$$M \otimes_S N := A/B$$

  and $m \otimes n := e_{m,n} + B \in M \otimes_S N$.

- Let C be an arbitrary abelian group. A map $f\colon M \times N \to C$ is called *balanced*, if

$$f(m+m',n) = f(m,n) + f(m',n), \quad f(m,n+n') = f(m,n) + f(m,n'), \quad f(ms,n) = f(m,sn)$$

  holds for $m, m' \in M$, $n, n' \in N$ and $r \in R$.

Remark III.6.15.

(i) The elements $m \otimes n$ form a generating set of $M \otimes_S N$, but in general not a basis. Furthermore, not every element in $M \otimes_S N$ has the form $m \otimes n$. Maps between tensor products are therefore defined via a universal property to guarantee well-definedness.

(ii) By construction, $M \times N \to M \otimes_S N$, $(m,n) \mapsto m \otimes n$ is balanced.

Lemma III.6.16 (Universal property of the tensor product)**.** *Let $f\colon M \times N \to C$ be balanced with the notation from Definition III.6.14. Then there exists exactly one $\mathbb{Z}$-homomorphism $\hat{f}\colon M \otimes_S N \to C$ with $\hat{f}(m \otimes n) = f(m,n)$ for $m \in M$ and $n \in N$.*

Proof. We first define $\varphi\colon A \to C$ by $\varphi(e_{m,n}) := f(m,n)$. Since f is balanced, $B \subseteq \mathrm{Ker}(\varphi)$. Using the homomorphism theorem, one obtains $\hat{f}\colon M \otimes_S N = A/B \to C$ with $\hat{f}(m \otimes n) = \varphi(e_{m,n}) = f(m,n)$. Since $M \otimes_S N$ is generated by the elements $m \otimes n$, $\hat{f}$ is uniquely determined by f. □

Lemma III.6.17. *By $r(m \otimes n) := rm \otimes n$ and $(m \otimes n)t := m \otimes nt$ for $r \in R$, $t \in T$, $m \in M$ and $n \in N$, $M \otimes_S N$ becomes an R-T-bimodule.*

Proof. For $r \in R$, the map $f_r \colon M \times N \to M \otimes_S N$, $(m,n) \mapsto rm \otimes n$ is balanced. According to the universal property, there exists a $\mathbb{Z}$-homomorphism $\hat{f}_r \colon M \otimes_S N \to M \otimes_S N$. For $x \in M \otimes_S N$ and $r \in R$, $r \cdot x := \hat{f}_r(x)$ is now well-defined. With $x := \sum_{i=1}^{k} m_i \otimes n_i$ and $y \in M \otimes_S N$, it follows that

$$\begin{aligned} 1x = \hat{f}_1(x) &= x, \\ (r+s)x = \hat{f}_{r+s}(x) &= \sum_{i=1}^{k} (r+s)m_i \otimes n_i = \hat{f}_r(x) + \hat{f}_s(x) = rx + sx, \\ r(s(x)) &= \sum_{i=1}^{k} \hat{f}_r(sm \otimes n) = \sum_{i=1}^{k} rsm \otimes n = \hat{f}_{rs}(x) = (rs)x, \\ r(x+y) &= \hat{f}_r(x+y) = \hat{f}_r(x) + \hat{f}_r(y) = rx + ry. \end{aligned}$$

Thus $M \otimes_S N$ is an R-left module. Completely analogously, one shows that $M \otimes_S N$ is a T-right module. Because of $(r(m \otimes n))s = (rm \otimes n)s = rm \otimes ns = r(m \otimes ns) = r((m \otimes n)s)$, it is an R-T-bimodule. □

Example III.6.18.

(i) Let M be an R-S-bimodule. The balanced map $R \times M \to M$, $(r,m) \mapsto rm$ induces a $\mathbb{Z}$-homomorphism $f \colon R \otimes_R M \to M$, $r \otimes m \to rm$. Obviously, f is an R-S-isomorphism with inverse map $M \to R \otimes_R M$, $m \mapsto 1 \otimes m$. In particular, $\boxed{R \otimes_R M \simeq M.}$

(ii) Let $R := \mathbb{Z}$, $M := \mathbb{Z}/m\mathbb{Z}$ and $N := \mathbb{Z}/n\mathbb{Z}$ with $m, n \in \mathbb{N}_0$. Let $g := \gcd(m,n)$ and $L := \mathbb{Z}/g\mathbb{Z}$. Then $M \times N \to L$, $(x + m\mathbb{Z}, y + n\mathbb{Z}) \mapsto xy + g\mathbb{Z}$ is well-defined and balanced. Thus there exists a homomorphism

$$\varphi \colon M \otimes_{\mathbb{Z}} N \to L, \qquad (x + m\mathbb{Z}) \otimes (y + n\mathbb{Z}) \mapsto xy + g\mathbb{Z}.$$

Conversely,

$$\psi \colon L \to M \otimes_{\mathbb{Z}} N, \qquad z + g\mathbb{Z} \mapsto (z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) = (1 + m\mathbb{Z}) \otimes (z + n\mathbb{Z})$$

is a well-defined homomorphism with $\psi \circ \varphi = \mathrm{id}_{M \otimes_{\mathbb{Z}} N}$ and $\varphi \circ \psi = \mathrm{id}_L$. This shows

$$\boxed{(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/\gcd(m,n)\mathbb{Z}.}$$

(iii) Let K be a field, G a finite group and $R = KG$ the group algebra. Finite-dimensional R-modules M, N can be viewed as an R-K-bimodule and a K-R^o-bimodule, respectively. The R-R^o-bimodule $M \otimes_K N$ becomes an R-left module via

$$r \cdot (m \otimes n) := r(m \otimes n)r = rm \otimes rn$$

Let $b_1, \ldots, b_k$ be a K-basis of M and $c_1, \ldots, c_l$ be a K-basis of N. Apparently, $\{b_i \otimes b_j : 1 \leq i \leq k, 1 \leq j \leq l\}$ is then a generating set of $M \otimes_K N$ as a K-vector space. Let A be the free abelian group with basis $\{e_{m,n} : m \in M, n \in N\}$ and B the corresponding subgroup as in Definition III.6.14. By $\lambda e_{m,n} := e_{\lambda m,n}$ for $\lambda \in K$, A and A/B become K-vector spaces. For comparison, let $T := M \otimes N$ be the tensor product defined in Definition III.3.16. Then there exists a K-epimorphism $\varphi \colon A \to T$, $e_{m,n} \mapsto m \otimes n$ with $B \subseteq \mathrm{Ker}(\varphi)$. This shows

$$kl = \dim T = \dim A - \dim \mathrm{Ker}(\varphi) \leq \dim A/B = \dim M \otimes_K N \leq kl.$$

Thus $b_i \otimes c_j$ also form a K-basis of $M \otimes_S N$ and one obtains an R-isomorphism $M \otimes_S N \simeq T$.

Lemma III.6.19. *Let $f\colon M \to M'$ and $g\colon N \to N'$ be homomorphisms between R-S-bimodules M, M' and S-T-bimodules N, N', respectively. Then there exists exactly one R-T-homomorphism $f \otimes g\colon M \otimes_S M' \to N \otimes_T N'$, $m \otimes n \mapsto f(m) \otimes g(n)$.*

Proof. The balanced map $M \times N \to M' \otimes_S N'$, $(m, n) \mapsto f(m) \otimes g(n)$ extends to the specified $\mathbb{Z}$-homomorphism $f \otimes g$. For $r \in R$, $t \in T$, $m \in M$ and $n \in N$ we have

$$\begin{aligned}(f \otimes g)(r(m \otimes n)t) = (f \otimes g)(rm \otimes nt) = f(rm) \otimes g(nt) = rf(m) \otimes g(n)t \\ = r(f(m) \otimes g(n))t = r(f \otimes g)(m \otimes n)t.\end{aligned}$$

Therefore $f \otimes g$ is an R-T-homomorphism. □

Remark III.6.20. With suitable notation, the following hold:

$$\begin{aligned} 0 \otimes g = 0, \qquad f \otimes 0 = 0, \qquad & (f \otimes g) \circ (f' \otimes g') = (f \circ f') \otimes (g \circ g'), \\ f \otimes (g + g') = f \otimes g + f \otimes g', \qquad & (f + f') \otimes g = f \otimes g + f' \otimes g. \end{aligned}$$

Lemma III.6.21. *Let R, S, T, U be rings and A, B, C be bimodules with respect to (R, S), (S, T), (T, U). Then there exists an R-U-isomorphism*

$$A \otimes_S (B \otimes_T C) \to (A \otimes_S B) \otimes_T C, \qquad a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c.$$

Proof. For $a \in A$ there exists as usual an S-T-homomorphism $f_a\colon B \otimes_T C \to (A \otimes_S B) \otimes_T C$, $b \otimes c \mapsto (a \otimes b) \otimes c$. One easily shows that $f\colon A \times (B \otimes_T C) \to (A \otimes_S B) \otimes_T C$, $(a, x) \mapsto f_a(x)$ is balanced. This yields an R-U-homomorphism

$$\hat{f}\colon A \otimes_S (B \otimes_T C) \to (A \otimes_S B) \otimes_T C, \qquad a \otimes (b \otimes c) \mapsto f_a(b \otimes c) = (a \otimes b) \otimes c.$$

Completely analogously, one obtains an R-T-homomorphism $g\colon (A \otimes_S B) \otimes_T C \to A \otimes_S (B \otimes_T C)$, $(a \otimes b) \otimes c \mapsto a \otimes (b \otimes c)$. Obviously $fg = \mathrm{id}$ and $gf = \mathrm{id}$. □

Lemma III.6.22. *For families of R-S-bimodules $(M_i)_{i \in I}$ and S-T-bimodules $(N_j)_{j \in J}$ there exists an R-T-isomorphism*

$$\Big(\coprod_{i \in I} M_i\Big) \otimes_S \Big(\coprod_{j \in J} N_j\Big) \to \coprod_{i \in I} \coprod_{j \in J} (M_i \otimes_S N_j), \qquad (m_i)_i \otimes (n_j)_j \mapsto (m_i \otimes n_j)_{i,j}.$$

Proof. As usual, $\Big(\coprod_{i \in I} M_i\Big) \times \Big(\coprod_{j \in J} N_j\Big) \to \coprod_{i \in I} \coprod_{j \in J} (M_i \otimes_S N_j)$, $((m_i)_i, (n_j)_j) \mapsto (m_i \otimes n_j)_{i,j}$ is balanced and the specified map is an R-T-homomorphism. The inverse map is obtained by

$$\coprod_{i \in I} \coprod_{j \in J} (M_i \otimes_S N_j), (x_{ij})_{i,j} \mapsto \sum_{i \in I} \sum_{j \in J} x_{ij}$$

(only finitely many summands are different from 0). □

Theorem III.6.23. *For bimodules A, B, C with respect to (R, S), (S, T), (U, T) there exists a U-R-isomorphism*

$$\mathrm{Hom}_T(A \otimes_S B, C) \simeq \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C)).$$

Proof. For $f \in \mathrm{Hom}_T(A \otimes_S B, C)$ and $a \in A$, $f_a \colon B \to C$, $b \mapsto f(a \otimes b)$ is a homomorphism of T-right modules. Furthermore, $\Delta(f) \colon A \to \mathrm{Hom}_T(B, C)$, $a \mapsto f_a$ is a homomorphism of S-right modules, because

$$\Delta(f)(as)(b) = f_{as}(b) = f(as \otimes b) = f(a \otimes sb) = f_a(sb) = (f_a s)(b) = (\Delta(f)(a)s)(b).$$

For $g \in \mathrm{Hom}_T(A \otimes_S B, C)$, we have $\Delta(f+g) = \Delta(f) + \Delta(g)$. For $u \in U$ and $r \in R$, it holds that

$$\begin{aligned}\Delta(ufr)(a)(b) &= (ufr)_a(b) = (ufr)(a \otimes b) = f(ra \otimes b)u \\ &= f_{ra}(b)u = (\Delta(f)(ra)u)(b) = (u\Delta(f)r)(a)(b).\end{aligned}$$

Overall, $\Delta \colon \mathrm{Hom}_T(A \otimes_S B, C) \to \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C))$ is a U-R-homomorphism.

Conversely, let $\varphi \in \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C))$ be given. Then $A \times B \to C$, $(a, b) \mapsto \varphi(a)(b)$ is balanced and one obtains a $\mathbb{Z}$-homomorphism $\Gamma(\varphi) \colon A \otimes_S B \to C$, $a \otimes b \mapsto \varphi(a)(b)$. One easily verifies that $\Gamma(\varphi)$ is a homomorphism of T-right modules. For $\psi \in \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C))$, we have $\Gamma(\varphi + \psi) = \Gamma(\varphi) + \Gamma(\psi)$. For $u \in U$ and $r \in R$, one calculates

$$\Gamma(u\varphi r)(a \otimes b) = (u\varphi r)(a)(b) = (\varphi(ra)u)(b) = \varphi(ra)(b)u = \Gamma(\varphi)(ra \otimes b)u = (u\Gamma(\varphi)r)(a \otimes b).$$

Therefore, $\Gamma \colon \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C)) \to \mathrm{Hom}_T(A \otimes_S B, C)$ is a U-R-homomorphism.

Finally, it holds that

$$\begin{aligned}\Gamma(\Delta(f))(a \otimes b) &= \Delta(f)(a)(b) = f_a(b) = f(a \otimes b), \\ \Delta(\Gamma(\varphi))(a)(b) &= \Gamma(\varphi)_a(b) = \Gamma(\varphi)(a \otimes b) = \varphi(a)(b),\end{aligned}$$

i. e. $\Gamma\Delta = \mathrm{id}$ and $\Delta\Gamma = \mathrm{id}$. □

Remark III.6.24. Because of

$$(f \circ g) \otimes \mathrm{id} = (f \circ g) \otimes (\mathrm{id} \circ \mathrm{id}) = (f \otimes \mathrm{id}) \circ (g \otimes \mathrm{id})$$

$. \otimes_S B \colon {}_R\mathbf{Mod}_S \to {}_R\mathbf{Mod}_T$, $A \mapsto A \otimes_S B$ with $f \otimes_S B := f \otimes \mathrm{id}_B$ for $f \colon A \to A'$ is a functor. As is well known, $\mathrm{Hom}(B, .) \colon {}_R\mathbf{Mod}_T \to {}_R\mathbf{Mod}_S$ is also a functor. The bijection $\alpha_{(A,C)} := \Delta \colon \mathrm{Hom}_T(A \otimes_S B, C) \to \mathrm{Hom}_S(A, \mathrm{Hom}_T(B, C))$ constructed in the proof of Theorem III.6.23 satisfies

$$\begin{aligned}\big(\alpha_{(A',C')} \circ \mathrm{Hom}((f_A \otimes B), f_C)\big)(\varphi)(a)(b) &= \alpha_{(A',C')}\big(f_C \circ \varphi \circ (f_A \otimes \mathrm{id}_B)\big)(a)(b) \\ &= f_C\big(\varphi(f_A(a) \otimes b)\big) = (f_C \circ \varphi_{f_A(a)})(b) = \big(\mathrm{Hom}(B, f_C) \circ \alpha_{(A,C)}(\varphi) \circ f_A\big)(a)(b) \\ &= \big(\mathrm{Hom}(f_A, \mathrm{Hom}(B, f_C)) \circ \alpha_{(A,C)}\big)(\varphi)(a)(b)\end{aligned}$$

for $f = (f_A, f_C) \in \mathrm{Hom}_{({}_S\mathbf{Mod}_R)^o \times {}_R\mathbf{Mod}_T}(A \times C, A' \times C')$, $\varphi \in \mathrm{Hom}_T(A \otimes_S B, C)$, $a \in A'$, $b \in B$. Therefore, α is a natural isomorphism and $. \otimes_S B$ is left-adjoint to $\mathrm{Hom}(B, .)$.

Definition III.6.25. An R-module P is called (R-)*generator*, if the functor $\mathrm{Hom}(P, .) \colon {}_R\mathbf{Mod} \to \mathbf{Ab}$ is faithful (for right modules one considers $\mathrm{Hom}(P, .) \colon \mathbf{Mod}_R \to \mathbf{Ab}$).

Remark III.6.26. Let P be a generator. For R-modules M, N, the map

$$\Gamma \colon \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{\mathbf{Ab}}\big(\mathrm{Hom}_R(P, M), \mathrm{Hom}_R(P, N)\big)$$

with $\Gamma(f)(g) = f \circ g$ for $f \in \mathrm{Hom}_R(M, N)$ and $g \in \mathrm{Hom}_R(P, M)$ is then injective. Since Γ is a group homomorphism, injectivity is equivalent to $\mathrm{Ker}(\Gamma) = 0$.

Lemma III.6.27. *For every R-module P, the following statements are equivalent:*

(1) P is a generator.

(2) The regular R-module is (up to isomorphism) a direct summand of P^n for some $n \in \mathbb{N}$.

(3) Every R-module is isomorphic to a factor module of $\coprod_{i\in I} P$, where I is an index set.

Proof.

(1) $\Rightarrow$ (2): Let $P^* := \mathrm{Hom}_R(P, R)$ and $J := \sum_{f\in P^*} f(P) \leq R$. Suppose $J < R$ holds. Then the canonical epimorphism $\pi\colon R \to R/J$ is non-trivial. Since P is a generator, there exists $g \in P^*$ with $\pi \circ g \neq 0$, i. e. $g(P) \not\subseteq J$. This contradiction shows $J = R$. Since R is generated by 1, there exist $f_1, \ldots, f_n \in P^*$ with $R = f_1(P) + \ldots + f_n(P)$. This yields an epimorphism $\varphi\colon P^n \to R$. Since R is projective, $P^n = \mathrm{Ker}(\varphi) \oplus Q$ with $Q \cong R$ (Theorem II.12.13).

(2) $\Rightarrow$ (3): For every R-module M there exists a free module, say $F := \coprod_{b\in B} R$, and an epimorphism $F \to M$. According to (2), one obtains an epimorphism $\coprod_{b\in B} P^n \to F$ via projection. The composition of these maps shows (3).

(3) $\Rightarrow$ (1): Let $f \in \mathrm{Hom}_R(M, N)$ be non-trivial and $\pi\colon \coprod_{i\in I} P \to M$ an epimorphism (guaranteed by (3)). Then $f \circ \pi \neq 0$ also holds and one finds a projection $\rho\colon P \to \coprod_{i\in I} P$ with $f \circ \pi \circ \rho \neq 0$. For $g := \pi \circ \rho \in \mathrm{Hom}_R(P, M)$ we thus have $f \circ g \neq 0$ and P is a generator. □

Remark III.6.28. A finitely generated projective module P satisfies the property dual to Lemma III.6.27(2): P is (up to isomorphism) a direct summand of R^n. To combine both properties, we call a finitely generated projective (R-)generator an (R-)*progenerator*.

Example III.6.29.

(i) Every finitely generated free R-module is a progenerator.

(ii) If A is a finite-dimensional K-algebra and $P_1, \ldots, P_n$ is a system of representatives for the non-isomorphic projective-indecomposable A-modules, then $P_1 \times \ldots \times P_n$ is a progenerator.

(iii) If P is a generator and $Q \to P$ is an R-epimorphism, then Q is also a generator (use Lemma III.6.27(3)).

(iv) Let $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ be an equivalence and P an R-generator. For every S-module N there exists an R-module M with $\Phi(M) \simeq N$. Since M is a factor module of $\coprod_{i\in I} P$, N is a factor module of $\Phi\big(\coprod_{i\in I} P\big) \simeq \coprod_{i\in I} \Phi(P)$. Thus $\Phi(P)$ is an S-generator. With Theorem III.6.6 it follows: P is an R-progenerator $\iff$ $\Phi(P)$ is an S-progenerator.

Definition III.6.30. Let R and S be rings. A *Morita context* is a 6-tuple $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ with the following properties:

- M is an R-S-bimodule and N is an S-R-bimodule.
- $\mathfrak{R}\colon M \otimes_S N \to R$ is an R-R-homomorphism and $\mathfrak{S}\colon N \otimes_R M \to S$ an S-S-homomorphism.
- $\mathfrak{R}(m \otimes n)m' = m\mathfrak{S}(n \otimes m')$ and $n\mathfrak{R}(m \otimes n') = \mathfrak{S}(n \otimes m)n'$ for $m, m' \in M$ and $n, n' \in N$.[2]

Theorem III.6.31. *Let $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ be a Morita context with surjective $\mathfrak{R}$. Then:*

(i) $\mathfrak{R}$ is an R-R-isomorphism.

[2] Mnemonic: The variables m, n, m' and n, m, n' are cyclically permuted.

(ii) *M and N are finitely generated projective S-modules.*

(iii) *M and N are R-generators.*

(iv) *$\Omega\colon R \to \mathrm{End}_S(M)$, $r \mapsto \Omega_r$ with $\Omega_r(m) := rm$ and $\Omega'\colon R^o \to \mathrm{End}_R(N)$, $r \mapsto \Omega'_r$ with $\Omega'_r(n) := nr$ are ring isomorphisms.*

Proof. By assumption, there exist $m_1, \ldots, m_k \in M$ and $n_1, \ldots, n_k \in N$ with $\mathfrak{R}\big(\sum_{i=1}^k m_i \otimes n_i\big) = 1_R$.

(i) Let $x_1, \ldots, x_l \in M$ and $y_1, \ldots, y_l \in N$ with $\mathfrak{R}(\sum_{i=1}^l x_i \otimes y_i) = 0$. Then it holds that

$$\begin{aligned}\sum_{j=1}^{l} x_j \otimes y_j &= \sum_{j=1}^{l}\sum_{i=1}^{k}(x_j \otimes y_j)\mathfrak{R}(m_i \otimes n_i) = \sum_{j=1}^{l}\sum_{i=1}^{k} x_j \otimes y_j\mathfrak{R}(m_i \otimes n_i)\\ &= \sum_{j=1}^{l}\sum_{i=1}^{k} x_j \otimes \mathfrak{S}(y_j \otimes m_i)n_i = \sum_{j=1}^{l}\sum_{i=1}^{k} x_j\mathfrak{S}(y_j \otimes m_i) \otimes n_i\\ &= \sum_{j=1}^{l}\sum_{i=1}^{k} \mathfrak{R}(x_j \otimes y_j)m_i \otimes n_i = \mathfrak{R}\Big(\sum_{j=1}^{l} x_j \otimes y_j\Big)\sum_{i=1}^{k} m_i \otimes n_i = 0.\end{aligned}$$

Thus $\mathfrak{R}$ is injective.

(ii) The maps

$$\begin{aligned} f\colon S^k \to M, &\qquad (s_1, \ldots, s_k) \mapsto m_1s_1 + \ldots + m_ks_k,\\ g\colon M \to S^k, &\qquad m \mapsto (\mathfrak{S}(n_1 \otimes m), \ldots, \mathfrak{S}(n_k \otimes m))\end{aligned}$$

are S-homomorphisms with

$$f(g(m)) = \sum_{i=1}^{k} m_i\mathfrak{S}(n_i \otimes m) = \sum_{i=1}^{k} \mathfrak{R}(m_i \otimes n_i)m = m$$

for $m \in M$. In particular, f is surjective and $M = \langle m_1, \ldots, m_k\rangle$ is a finitely generated S-module. Furthermore, g is injective and $S^k = \mathrm{Ker}(f) \oplus g(M)$. Thus $M \simeq g(M)$ is projective as an S-module. For the second claim, one considers analogously $f\colon S^k \to N$, $(s_1, \ldots, s_k) \mapsto s_1n_1 + \ldots + s_kn_k$ and $g\colon N \to S^k$, $n \mapsto (\mathfrak{S}(n \otimes m_1), \ldots, \mathfrak{S}(n \otimes m_k))$.

(iii) The map $f\colon M^k \to R$, $(x_1, \ldots, x_k) \mapsto \mathfrak{R}\big(\sum_{i=1}^k x_i \otimes n_i\big)$ is an R-epimorphism because of $f(m_1, \ldots, m_k) = 1_R$. Since R is a generator, M^k and M are also generators (Example III.6.29). For N, one considers analogously $N^k \to R$, $(y_1, \ldots, y_k) \mapsto \mathfrak{R}\big(\sum_{i=1}^k m_i \otimes y_i\big)$.

(iv) One easily shows that Ω and Ω' are ring homomorphisms (note $\Omega'(r \cdot r') = \Omega'_{r'r} = \Omega'_r \circ \Omega'_{r'}$). For $r \in \mathrm{Ker}(\Omega)$ it holds that

$$r = \sum_{i=1}^{k} r\mathfrak{R}(m_i \otimes n_i) = \sum_{i=1}^{k} \mathfrak{R}(rm_i \otimes n_i) = \sum_{i=1}^{k} \mathfrak{R}(\Omega_r(m) \otimes n_i) = 0,$$

i. e. Ω is injective. Let $\varphi \in \mathrm{End}_S(M)$ be given. Then

$$\begin{aligned}\varphi(m) &= \sum_{i=1}^{k} \varphi(\mathfrak{R}(m_i \otimes n_i)m) = \sum_{i=1}^{k} \varphi(m_i)\mathfrak{S}(n_i \otimes m)\\ &= \sum_{i=1}^{k} \varphi(m_i)\mathfrak{S}(n_i \otimes m) = \sum_{i=1}^{k} \mathfrak{R}(\varphi(m_i) \otimes n_i)m.\end{aligned}$$

It follows that $\Omega\big(\sum_{i=1}^k \mathfrak{R}(\varphi(m_i) \otimes n_i)\big) = \varphi$. The bijectivity of Ω' is proven analogously. □

Remark III.6.32. For reasons of symmetry, Theorem III.6.31 also holds if one interchanges $(R, M, \mathfrak{R})$ and $(S, N, \mathfrak{S})$.

Example III.6.33. Let M be an arbitrary R-left module, $S := \mathrm{End}_R(M)^o$ and $N := \mathrm{Hom}_R(M, R)$. As is well known, M is an $\mathrm{End}_R(M)$-left module and thus an R-S-bimodule. According to Example III.6.12, N is an S-R-bimodule with

$$r \cdot m \cdot \varphi = \varphi(rm) = r\varphi(m), \qquad \varphi \cdot \lambda \cdot r = (\lambda \circ \varphi)r = \lambda r \circ \varphi$$

for $r \in R$, $\varphi \in S$, $m \in M$ and $\lambda \in N$. Because of $\lambda(m\varphi) = (\lambda \circ \varphi)(m) = (\varphi\lambda)(m)$, the map $M \times N \to R$, $(m, \lambda) \mapsto \lambda(m)$ is balanced with respect to S. According to the universal property of the tensor product, it induces a $\mathbb{Z}$-homomorphism

$$\mathfrak{R}\colon M \otimes_S N \to R, \qquad m \otimes \lambda \mapsto \lambda(m).$$

Because of $r\lambda(m)r' = \lambda(rm)r' = (\lambda r')(rm)$ for $r, r' \in R$, $\mathfrak{R}$ is an R-R-homomorphism. For fixed m and λ, the map $\mathfrak{S}_{\lambda,m}\colon M \to M$, $x \mapsto \lambda(x)m$ is an R-homomorphism, thus an element of S. Because of

$$\mathfrak{S}_{\lambda r,m}(x) = (\lambda r)(x)m = \lambda(x)rm = \mathfrak{S}_{\lambda,rm}(x)$$

one obtains a balanced map $N \times M \to S$, $(\lambda, m) \mapsto \mathfrak{S}_{\lambda,m}$. Thus there exists a $\mathbb{Z}$-homomorphism

$$\mathfrak{S}\colon N \otimes_R M \to S, \qquad \lambda \otimes m \mapsto \mathfrak{S}_{\lambda,m}.$$

For $\varphi, \psi \in S$ we have

$$\mathfrak{S}_{\varphi\lambda,m\psi}(x) = (\varphi\lambda)(x)(m\psi) = \lambda(\varphi(x))\psi(m) = \psi\big(\lambda(\varphi(x))m\big) = \psi\big(\mathfrak{S}_{\lambda,m}(\varphi(x))\big) = (\varphi \cdot \mathfrak{S}_{\lambda,m} \cdot \psi)(x),$$

i. e. $\mathfrak{S}$ is an S-S-homomorphism.

For $m, m' \in M$ and $\lambda, \lambda' \in N$ we finally have

$$\begin{aligned} \mathfrak{R}(m \otimes \lambda)m' &= \lambda(m)m' = \mathfrak{S}_{\lambda,m'}(m) = m\mathfrak{S}(\lambda \otimes m'), \\ (\lambda\mathfrak{R}(m \otimes \lambda'))(m') &= (\lambda\lambda'(m))(m') = \lambda(m')\lambda'(m) = \lambda'(\lambda(m')m) \\ &= (\lambda' \circ \mathfrak{S}_{\lambda,m})(m') = (\mathfrak{S}_{\lambda,m}\lambda')(m') = (\mathfrak{S}(\lambda \otimes m)\lambda')(m'). \end{aligned}$$

Thus $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ is a Morita context.

Theorem III.6.34. *For the concrete Morita context from Example III.6.33, the following holds:*

(i) If M is a finitely generated projective R-module, then $\mathfrak{S}$ is surjective.

(ii) If M is an R-generator, then $\mathfrak{R}$ is surjective.

Proof.

(i) By assumption, there exist $k \in \mathbb{N}$ and R-homomorphisms $f\colon R^k \to M$ and $g\colon M \to R^k$ with $f \circ g = \mathrm{id}_M$. Let $e_1, \ldots, e_k \in R^k$ be the canonical basis of R^k and $\pi_i\colon R^k \to R$ the i-th projection. Thus $x = \sum_{i=1}^k \pi_i(x)e_i$ holds for $x \in R^k$. For $m \in M$ it follows that

$$m = f(g(m)) = \sum_{i=1}^k f\big(\pi_i(g(m))e_i\big) = \sum_{i=1}^k \pi_i(g(m))f(e_i).$$

With $m_i := f(e_i) \in M$ and $\lambda_i := \pi_i \circ g \in N$ it follows that

$$1_S = \mathrm{id}_M = \sum_{i=1}^{k} \mathfrak{S}_{\lambda_i, m_i} = \mathfrak{S}\Big(\sum_{i=1}^{k} \lambda_i \otimes m_i\Big) \in \mathfrak{S}(N \otimes_R M).$$

Therefore $\mathfrak{S}$ is surjective.

(ii) According to Lemma III.6.27, there exists an index set I and an R-epimorphism $f\colon \coprod_{i\in I} M \to R$. Let $(m_i)_{i\in I} \in \coprod_{i\in I} M$ with $f\big((m_i)_i\big) = 1_R$. Then $J := \{i \in I : m_i \neq 0\}$ is finite. Let $q_i\colon M \to \coprod_{i\in I} M$ be the i-th injection. Then

$$1_R = \sum_{j\in J} f(q_j(m_j)) = \mathfrak{R}\Big(\sum_{j\in J} m_j \otimes (f \circ q_j)\Big) \in \mathfrak{R}(M \otimes_S N)$$

and $\mathfrak{R}$ is surjective. □

Theorem III.6.35 (Morita)**.** *For rings R and S, the following are equivalent:*

(1) ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$.

(2) There exists an R-progenerator M with $\mathrm{End}_R(M) \cong S^o$.

(3) There exists an R-S-bimodule M and an S-R-bimodule N with $R \simeq M \otimes_S N$ and $S \simeq N \otimes_R M$ as bimodules.

If applicable, R and S are called Morita equivalent.

Proof.

(1) ⇒ (2)**:** Let $\Psi\colon {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$ be an equivalence. According to Example III.6.29, $M := \Psi(S)$ is an R-progenerator. According to Lemma II.7.20, $S^o \cong \mathrm{End}_S(S)$. According to Lemma III.5.23 and Lemma III.6.3, $\Psi\colon \mathrm{End}_S(S) \to \mathrm{End}_R(M)$ is a ring isomorphism.

(2) ⇒ (3)**:** According to Example III.6.33, $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ is a Morita context with $N = \mathrm{Hom}_R(M, R)$. According to Theorem III.6.34, Theorem III.6.31 and Remark III.6.32, $\mathfrak{R}$ and $\mathfrak{S}$ are the desired isomorphisms.

(3) ⇒ (1)**:** Let $\varphi\colon M \otimes_S N \to R$ and $\psi\colon N \otimes_R M \to S$ be isomorphisms of bimodules. We define $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$, $A \mapsto N \otimes_R A$ with $\Phi(f) := \mathrm{id}_N \otimes f$ for $f \in \mathrm{Hom}_R(A, B)$. According to Remark III.6.20, Φ is a functor. Analogously, $\Psi\colon {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$, $A \mapsto M \otimes_S A$ with $\Psi(f) := \mathrm{id}_M \otimes f$ is a functor. For every R-module A, it holds that

$$\Psi\Phi(A) = M \otimes_S \Phi(A) \overset{\text{III.6.21}}{\simeq} M \otimes_S N \otimes_R A \simeq R \otimes_R A \overset{\text{III.6.18}}{\simeq} A.$$

Let $\alpha_A\colon \Psi\Phi(A) \to A$, $m \otimes n \otimes a \mapsto \varphi(m \otimes n)a$ be a corresponding R-isomorphism. For $f \in \mathrm{Hom}_R(A, B)$, $a \in A$, $m \in M$ and $n \in N$, it holds that

$$\begin{aligned}\big(\alpha_B \circ \Psi\Phi(f)\big)(m \otimes n \otimes a) &= \alpha_B\big(m \otimes \Phi(f)(n \otimes a)\big) = \alpha_A\big(m \otimes n \otimes f(a)\big)\\ &= \varphi(m \otimes n)f(a) = f(\varphi(m \otimes n)a) = (f \circ \alpha_A)(m \otimes n \otimes a).\end{aligned}$$

Thus $\alpha\colon \Psi\Phi \Rightarrow \mathrm{id}$ is a natural isomorphism. Analogously, one shows that $\beta_A\colon \Phi\Psi(A) \to A$, $n \otimes m \otimes a \mapsto \psi(n \otimes m)a$ defines a natural isomorphism $\beta\colon \Phi\Psi \Rightarrow \mathrm{id}$. □

Example III.6.36.

(i) For every ring R and $n \in \mathbb{N}$, R^n is a progenerator with $\mathrm{End}_R(R^n)^o \cong R^{n\times n}$ (Lemma II.7.20). Therefore R and $R^{n\times n}$ are Morita equivalent.

(ii) Let R be semisimple and $M_1, \ldots, M_k$ a system of representatives for the non-isomorphic simple R-modules. Then $M = M_1 \times \ldots \times M_k$ is a progenerator with $\mathrm{End}_R(M)^o \cong Q_1 \times \ldots \times Q_k$ for the division rings $Q_i := \mathrm{End}_R(M_i)^o$. Thus R and $Q_1 \times \ldots \times Q_k$ are Morita equivalent.

(iii) Let R and S be Morita equivalent local rings. Let M be an R-progenerator with $S \cong \mathrm{End}_R(M)^o$. Since the regular R-module is indecomposable, M is free, say $M = R^n$ with $n \in \mathbb{N}$. Now $S \cong \mathrm{End}_R(R^n)^o \cong R^{n\times n}$. For $n > 1$, $R^{n\times n} \simeq R^{n\times 1} \times \ldots \times R^{n\times 1}$ is not local. This shows $n = 1$ and $S \cong \mathrm{End}_R(R)^o \cong R$.

Theorem III.6.37. *For rings R and S, the following hold:*

(i) ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod} \iff {}_{R^o}\mathbf{Mod} \approx {}_{S^o}\mathbf{Mod} \iff \mathbf{Mod}_R \approx \mathbf{Mod}_S \iff {}_R\mathbf{mod} \approx {}_S\mathbf{mod}$.

(ii) $R \cong S \implies {}_R\mathbf{Mod} \cong {}_S\mathbf{Mod} \implies {}_R\mathbf{Mod} \approx {}_S\mathbf{Mod} \implies \mathrm{Z}(R) \cong \mathrm{Z}(S)$.

Proof.

(i) If ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$, then by Morita there exists an R-progenerator M and one obtains the Morita context $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ from Example III.6.33. According to Theorem III.6.31, the S-right module M is a progenerator. Therefore, M is also a progenerator as an S^o-left module. For this module, $\mathrm{End}_{S^o}(M) = \mathrm{End}_S(M) \cong R$ holds according to Theorem III.6.31. By Morita, it follows that ${}_{R^o}\mathbf{Mod} \approx {}_{S^o}\mathbf{Mod}$. This is known to be equivalent to $\mathbf{Mod}_R \approx \mathbf{Mod}_S$. Now let $\Phi\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ be an equivalence. According to Theorem III.6.6, the restriction of Φ yields an equivalence ${}_R\mathbf{mod} \to {}_S\mathbf{mod}$. Conversely, let an equivalence $\Psi\colon {}_S\mathbf{mod} \to {}_R\mathbf{mod}$ be given. Then $M := \Psi(R)$ is finitely generated and projective as an object of ${}_R\mathbf{mod}$. It is easy to check that Theorem II.12.13 remains correct in ${}_R\mathbf{mod}$. Therefore, M is a direct summand of a (finitely generated) free module. Thus, M is also projective in ${}_R\mathbf{Mod}$. In the same way, one sees with Lemma III.6.27 that M is an R-generator. Furthermore, $\mathrm{End}_R(M) \cong \mathrm{End}_S(S) \cong S^o$ according to Lemma III.6.3. By Morita, R and S are Morita equivalent.

(ii) Let $\varphi\colon R \to S$ be a ring isomorphism. Every R-module M becomes an S-module via $s \cdot m := \varphi^{-1}(s)m$ for $s \in S$ and $m \in M$. An R-homomorphism is in this way also an S-homomorphism. The identity functor ${}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ is thus an isomorphism. From ${}_R\mathbf{Mod} \cong {}_S\mathbf{Mod}$ it follows as is well known that ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$.

Now assume ${}_R\mathbf{Mod} \approx {}_S\mathbf{Mod}$. As in the proof of Theorem III.6.35, there exists a Morita context $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ with isomorphisms $\mathfrak{R}$ and $\mathfrak{S}$. Theorem III.6.31 yields $\mathrm{Z}(R) \cong \mathrm{Z}(\mathrm{End}_S(M))$. Applied to the Morita context $(S, R, N, M, \mathfrak{S}, \mathfrak{R})$, the theorem also yields $\mathrm{Z}(S) \cong \mathrm{Z}(S^o) \cong \mathrm{Z}(\mathrm{End}_S(M))$. Therefore, $\mathrm{Z}(R) \cong \mathrm{Z}(S)$ holds. □

Corollary III.6.38. *Commutative rings are Morita equivalent if and only if they are isomorphic.*

Example III.6.39.

(i) According to Exercise II.39, there exists a Noetherian ring R such that R^o is not Noetherian. According to Theorem III.6.9, ${}_R\mathbf{Mod} \not\approx {}_{R^o}\mathbf{Mod}$ holds.

(ii) For a ring $R \neq 0$, the dual category $({}_R\mathbf{Mod})^o$ usually has no relation to modules. Let us assume, for example, that there exists a ring S and an equivalence $\Phi\colon {}_S\mathbf{Mod} \to ({}_R\mathbf{Mod})^o$. Let $P := \times_{i\in\mathbb{N}} S$ be the product and $Q := \coprod_{i\in\mathbb{N}} S$ the coproduct of countably many copies of S. Then the canonical monomorphism $f\colon Q \to P$ is mapped to a monomorphism $\Phi(f)\colon \Phi(Q) \to \Phi(P)$. Here, $\Phi(Q)$ is a coproduct and $\Phi(P)$ is a product. In ${}_R\mathbf{Mod}$, one obtains an epimorphism $\Phi(P) \to \Phi(Q)$, where $\Phi(P)$ is now a coproduct and $\Phi(Q)$ a product of countably many copies of $\Phi(S)$ (cf. Lemma III.6.2). Since S is finitely generated, so is $\Phi(S)$. If R is now countable (e. g. $R = \mathbb{Z}$), then so is $\Phi(P)$. On the other hand, $\Phi(Q)$ is always uncountable. Therefore, no epimorphism $\Phi(P) \to \Phi(Q)$ can exist. [3]

Theorem III.6.40. *Finite-dimensional K-algebras are Morita equivalent if and only if their basic algebras are isomorphic.*

Proof. Let A and B be finite-dimensional Morita equivalent K-algebras. Let $P_1, \ldots, P_k$ be the projective-indecomposable A-modules up to isomorphism. Then $P := P_1 \times \ldots \times P_k$ is a progenerator and A is Morita equivalent to the basic algebra $A^b = \mathrm{End}_A(P)^o$. We can therefore assume $A = A^b$ and $B = B^b$. Let M be an arbitrary A-progenerator with $B \cong \mathrm{End}_A(M)^o$. Since M is projective, $M \simeq P_1^{a_1} \times \ldots \times P_k^{a_k}$ holds with $a_1, \ldots, a_k \in \mathbb{N}_0$. Since M is a generator, $a_1, \ldots, a_k \geq 1$ holds. Thus $A \simeq P_1 \times \ldots \times P_k$ is a direct summand of M and $A \cong \mathrm{End}_A(A)^o$ is a subalgebra of $\mathrm{End}_A(M)^o$. This shows $\dim B \geq \dim A$. By symmetry, $\dim A \geq \dim B$ and $A \cong B$ also hold. □

Example III.6.41. For finite groups G and H, ${}_{\mathbb{C}G}\mathbf{Mod} \approx {}_{\mathbb{C}H}\mathbf{Mod} \iff k(G) = k(H)$ holds (Remark II.13.30). The bijection $G \to G$, $g \mapsto g^{-1}$ extends to a ring isomorphism $KG \to (KG)^o$. Therefore, ${}_{KG}\mathbf{Mod} \cong \mathbf{Mod}_{KG}$ holds.

Theorem III.6.42. *If A and B are finite-dimensional K-algebras, then A is symmetric if and only if B is symmetric.*

Proof. Let A be symmetric and $e \in A$ be a basic idempotent. According to Example II.13.3, $B^b \cong A^b \cong eAe$ is symmetric. According to Theorem II.12.25, there exists an $n \in \mathbb{N}$ and an idempotent $e \in (B^b)^{n\times n}$ with $B \cong e(B^b)^{n\times n}e$. As in Example II.13.10, one shows that $(B^b)^{n\times n}$ is symmetric. Thus, B is also symmetric. □

Remark III.6.43. Let A and B be Morita equivalent K-algebras and M an A-progenerator with $B \cong \mathrm{End}_A(M)^o$. As in the proof of Theorem III.6.35, one obtains an equivalence $\Psi\colon {}_B\mathbf{Mod} \to {}_A\mathbf{Mod}$, $L \mapsto M \otimes_B L$. With $d := \dim M$, it thus holds that $\dim \Psi(L) = d \dim L$ for all B-modules L. According to Theorem III.6.6, the dimensions of the simple A-modules are proportional to the dimensions of the simple B-modules. Furthermore, A and B have the same Cartan matrix (with suitable ordering) according to Theorem II.12.24.

[3] There are, however, rings in which such an epimorphism exists: With Exercise III.28, one can construct rings with $R \simeq \times_{i\in\mathbb{N}} R$ as in Example II.9.6.

III.7 Central Simple Algebras

Remark III.7.1. For every Artinian ring R, $R/\mathrm{J}(R)$ is semisimple (Lemma II.8.13). According to Artin-Wedderburn, every semisimple ring is a direct product of simple rings. Every simple Artinian ring S is a finite-dimensional $\mathrm{Z}(S)$-algebra (Lemma II.12.5). In this chapter, we classify simple algebras with a given center. The set of Morita equivalence classes of these algebras receives a group structure through the tensor product, whose isomorphism type we calculate in examples. As before, we always consider finite-dimensional algebras over a field K.

Definition III.7.2. A K-algebra A is called *central*, if $\mathrm{Z}(A) = K1_A$ holds. If A is additionally simple as a ring (i.e., 0 and $A \neq 0$ are the only ideals in A), then A is called *central simple*.

Remark III.7.3. Let A be central simple.

(i) According to Artin-Wedderburn, there exists a division algebra D and $n \in \mathbb{N}$ with $A \cong D^{n\times n}$ (cf. Remark II.8.14 and Remark II.12.3). According to Example II.12.22, D is the basic algebra of A. According to Lemma II.12.5, $K \cong \mathrm{Z}(A) \cong \mathrm{Z}(D^{n\times n}) \cong \mathrm{Z}(D)$ holds. Therefore, D is also a central simple algebra.

(ii) If D is a division algebra, then $D^{n\times n}$ for $n \in \mathbb{N}$ is a central simple $\mathrm{Z}(D)$-algebra. In particular, every simple algebra B is a central simple $\mathrm{Z}(B)$-algebra.

(iii) If the K-algebra B is Morita equivalent to A, then B is also central simple according to Theorem III.6.9 and Theorem III.6.37.

Definition III.7.4. Let A and B be algebras with bases $a_1, \ldots, a_n$ and $b_1, \ldots, b_m$ over K, respectively. We already know the tensor product $A \otimes B = A \otimes_K B$ as a K-vector space with basis $\{a_i \otimes b_j : 1 \leq i \leq n, 1 \leq j \leq m\}$. By

$$(a_i \otimes b_j)(a_r \otimes b_s) := a_i a_r \otimes b_j b_s$$

(and linear extension), $A \otimes B$ becomes a K-algebra. $A \otimes B$ is called the *tensor product* of A and B.

Remark III.7.5.

(i) For $a = \sum_{i=1}^n \alpha_i a_i$, $b = \sum_{j=1}^m \beta_j b_j$, $c = \sum_{r=1}^n \gamma_r a_r$ and $d = \sum_{s=1}^m \delta_s b_s$, we have

$$\begin{aligned}(a \otimes b)(c \otimes d) &= \Big(\sum_{i,j} \alpha_i\beta_j(a_i \otimes b_j)\Big)\Big(\sum_{r,s} \gamma_r\delta_s(a_r \otimes b_s)\Big)\\ &= \sum_{i,j,r,s} \alpha_i\beta_j\gamma_r\delta_s(a_i a_r \otimes b_j b_s) = ac \otimes bd.\end{aligned}$$

(ii) The *universal property* for tensor products of algebras is: For every bilinear map $f\colon A \times B \to C$ with $f(1,1) = 1$ and $f(a,b)f(c,d) = f(ac,bd)$ for all $(a,b),(c,d) \in A \times B$, there exists exactly one homomorphism $\hat{f}\colon A \otimes B \to C$ of algebras with $\hat{f}(a \otimes b) = f(a,b)$ for $(a,b) \in A \times B$.

(iii) For K-algebras A, B, C, there are (as in Remark III.3.17) canonical isomorphisms of algebras:

$$K \otimes A \cong A, \qquad (A \otimes B) \otimes C \cong A \otimes (B \otimes C),$$
$$A \otimes B \cong B \otimes A, \qquad (A \times B) \otimes C \cong (A \otimes C) \times (B \otimes C).$$

(iv) If A and B are algebras such that $A \otimes B$ is semisimple, then A and B are also semisimple, because $\mathrm{J}(A) \otimes B$ and $A \otimes \mathrm{J}(B)$ are nilpotent ideals in $A \otimes B$. In general, however, $\mathrm{J}(A \otimes B)$ cannot be calculated from $\mathrm{J}(A)$ and $\mathrm{J}(B)$ (see Example III.7.7 and Theorem A.8.16).

(v) Every A-B-bimodule M becomes an $A \otimes B^o$-left module via $(a \otimes b)m := amb$ (one first defines $(a_i \otimes b_j)m$ and then extends linearly). In the same way, every $A \otimes B^o$-left module becomes an A-B-bimodule.

Lemma III.7.6. *Let $K \subseteq L$ be a finite field extension and $x \in \overline{K}$ with minimal polynomial $\mu \in K[X]$. Then $L \otimes K(x) \cong L[X]/(\mu)$.*

Proof. The evaluation homomorphism $\Gamma\colon L[X] \to L \otimes K(x)$, $\alpha \mapsto \alpha(1 \otimes x)$ is clearly surjective and $\mu \in \mathrm{Ker}(\Gamma)$. Due to $\dim_L(L \otimes K(x)) = \dim_K K(x) = \deg \mu \geq |L[X] : \mathrm{Ker}(\Gamma)|$, we have $\mathrm{Ker}(\Gamma) = (\mu)$. □

Example III.7.7.

(i) For finite groups G and H, it holds that $K[G \times H] \cong KG \otimes KH$. For every field extension $K \subseteq L$, $L \otimes KG \cong LG$.

(ii) According to Lemma III.7.6,

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[X]/(X^2 + 1) \cong \mathbb{C}[X]/(X - \mathrm{i}) \times \mathbb{C}[X]/(X + \mathrm{i}) \cong \mathbb{C} \times \mathbb{C}.$$

(iii) Let $K := \mathbb{F}_2(X^2)$ and $L := \mathbb{F}_2(X)$. Then $L \otimes L \cong L[Y]/(Y^2 - X^2) = L[Y]/(Y - X)^2$ possesses the nilpotent element $Y - X + (Y - X)^2$. In particular, $L \otimes L$ is not semisimple.

Theorem III.7.8. *For every finite field extension $K \subseteq L$, the following are equivalent:*

(1) $K \subseteq L$ is separable.

(2) For every finite field extension $K \subseteq M$, $M \otimes L$ is semisimple.

(3) $L \otimes L$ is semisimple.

Proof.

(1)⇒(2): Let $x \in L$ be a primitive element with minimal polynomial $\mu \in K[X]$. According to Lemma III.7.6, $M \otimes L \cong M[X]/(\mu)$. By assumption, $\mu = \mu_1 \dots \mu_k$ with pairwise coprime irreducible polynomials $\mu_1, \dots, \mu_k \in M[X]$. By the Chinese Remainder Theorem, $M[X]/(\mu)$ is a direct product of fields and thus semisimple.

(2)⇒(3): Trivial.

(3)⇒(1): Let $x \in L$ with minimal polynomial $\mu \in K[X]$. Since $L \otimes L$ is commutative, $K(x) \otimes K(x)$ is semisimple (Exercise II.43). We can therefore assume $L = K(x)$. Now $L[X]/(\mu)$ is semisimple. If μ possesses an irreducible divisor $\rho \in L[X]$ with multiplicity > 1, then $\frac{\mu}{\rho} + (\mu) \neq 0$ would be a nilpotent element in $L[X]/(\mu)$. This contradiction shows that x is separable. □

Lemma III.7.9. *For K-algebras A and B, it holds that* $\boxed{\mathrm{Z}(A \otimes B) = \mathrm{Z}(A) \otimes \mathrm{Z}(B).}$

Proof. Certainly $\mathrm{Z}(A) \otimes \mathrm{Z}(B) \subseteq \mathrm{Z}(A \otimes B)$. Let $A = \mathrm{Z}(A) \oplus A_1$ be a decomposition into subspaces and $z \in \mathrm{Z}(A \otimes B)$. We write $z = x + y$ with $x \in \mathrm{Z}(A) \otimes B$ and $y \in A_1 \otimes B$. For $a \in A$, $a \otimes 1$ is commutable with both z and x. Therefore, $a \otimes 1$ is also commutable with y. Let $b_1, \ldots, b_m$ be a basis of B and $y = \sum_{i=1}^{m} a_i \otimes b_i$ with $a_i \in A$. Because of

$$\sum_{i=1}^{m} a_i a \otimes b_i = y(a \otimes 1) = (a \otimes 1)y = \sum_{i=1}^{m} a_i a \otimes b_i$$

it holds that $a_i a = a a_i$ for $i = 1, \ldots, m$. Since $a \in A$ was arbitrary, $a_i \in \mathrm{Z}(A)$ for $i = 1, \ldots, m$. This shows $y \in (A_1 \otimes B) \cap (\mathrm{Z}(A) \otimes B) = 0$ and $\mathrm{Z}(A \otimes B) \subseteq \mathrm{Z}(A) \otimes B$. We can now analogously decompose $B = \mathrm{Z}(B) \oplus B_1$ and write $z = x + y$ with $x \in \mathrm{Z}(A) \otimes \mathrm{Z}(B)$ as well as $y \in \mathrm{Z}(A) \otimes B_1$. Then y is commutable with $1 \otimes b$ ($b \in B$) and one easily obtains $y = 0$. Overall, $\mathrm{Z}(A \otimes B) \subseteq \mathrm{Z}(A) \otimes \mathrm{Z}(B)$. □

Remark III.7.10. One should compare the next lemma with Lemma II.12.26.

Lemma III.7.11. *For K-algebras A, B and $n, m \in \mathbb{N}$ it holds that* $\boxed{A^{n \times n} \otimes B^{m \times m} \cong (A \otimes B)^{nm \times nm}.}$

Proof. For $a = (a_{ij})_{i,j} \in A^{n \times n}$ and $b = (b_{rs})_{r,s} \in B^{m \times m}$ we define $a_{ij} \otimes b := (a_{ij} \otimes b_{rs})_{r,s} \in (A \otimes B)^{m \times m}$ and $a \otimes b := (a_{ij} \otimes b)_{i,j} \in (A \otimes B)^{nm \times nm}$ similar to the Kronecker product. This yields a bilinear map

$$\begin{aligned} f \colon A^{n \times n} \times B^{m \times m} &\to (A \otimes B)^{nm \times nm}, \\ (a, b) &\mapsto a \otimes b \end{aligned}$$

with $f(1_n, 1_m) = 1_{nm}$ and

$$\begin{aligned} f(a,b)f(c,d) = (a \otimes b)(c \otimes d) &= \Big(\sum_{k=1}^{n} (a_{ik} \otimes b)(c_{kj} \otimes d) \Big)_{i,j} \\ &= \Big(\Big(\sum_{k=1}^{n} a_{ik} c_{kj} \Big) \otimes bd \Big)_{i,j} = ac \otimes bd = f(ac, bd). \end{aligned}$$

According to the universal property, one obtains a homomorphism of algebras $\hat{f} \colon A^{n \times n} \otimes B^{m \times m} \to (A \otimes B)^{nm \times nm}$. If one chooses bases $a_1, \ldots, a_r$ of A and $b_1, \ldots, b_s$ of B, then the matrices $a_i E_{kl}$ and $b_i E_{kl}$ respectively form bases of $A^{n \times n}$ and $B^{m \times m}$ respectively (as usual let $E_{kl} = (\delta_{ik}\delta_{jl})_{i,j}$). Furthermore,

$$\hat{f}(a_i E_{kl} \otimes b_j E_{pq}) = (a_i \otimes b_j) E_{(k-1)m+p,(l-1)m+p}$$

form a K-basis of $(A \otimes B)^{nm \times nm}$. Thus $\hat{f}$ is bijective. □

Lemma III.7.12. *Let A and B be division algebras and $0 \neq I \trianglelefteq A \otimes B$. Then $I \cap \mathrm{Z}(A \otimes B) \neq 0$.*

Proof. Let $a_1, \ldots, a_n$ be a K-basis of A. Choose $x \in I \setminus \{0\}$ such that in the unique representation $x = \sum_{i=1}^{n} a_i \otimes b_i$ as many as possible of the $b_i \in B$ vanish. Wlog. let $b_1 \neq 0$. After multiplication by $1 \otimes b_1^{-1}$ we can assume $b_1 = 1$. For all $b \in B$ it then holds that

$$I \ni (1 \otimes b)x - x(1 \otimes b) = \sum_{i=2}^{n} a_i \otimes (bb_i - b_i b).$$

The choice of x shows $bb_i = b_ib$, i. e. $b_i \in \mathrm{Z}(B)$ and $x \in A \otimes \mathrm{Z}(B)$. One can now replace B by $Z := \mathrm{Z}(B)$ and I by $J := I \cap (A \otimes Z) \neq 0$. As above, it follows that $J \cap (\mathrm{Z}(A) \otimes Z) \neq 0$. Because $\mathrm{Z}(A) \otimes \mathrm{Z}(B) = \mathrm{Z}(A \otimes B)$, the claim holds. □

Lemma III.7.13. *Let A be a simple algebra and B a central-simple algebra. Then $A \otimes B$ is simple.*

Proof. According to Remark III.7.3 there exist division algebras D_A and D_B and $n, m \in \mathbb{N}$ with $A \cong D_A^{n\times n}$ as well as $B \cong D_B^{m\times m}$. Here $\mathrm{Z}(D_B) \cong \mathrm{Z}(D_B^{m\times m}) \cong \mathrm{Z}(B) \cong K$. With Lemma III.7.11 it follows that

$$A \otimes B \cong (D_A \otimes D_B)^{nm\times nm}.$$

We will show that $D_A \otimes D_B$ is simple, because then there exists a division algebra D and $k \in \mathbb{N}$ with $D_A \otimes D_B \cong D^{k\times k}$ and

$$A \otimes B \cong D^{knm\times knm}$$

according to Lemma II.12.26. We can therefore assume $A = D_A$ and $B = D_B$. Let $0 \neq I \trianglelefteq A \otimes B$. According to Lemma III.7.12 it holds that

$$0 \neq I \cap (A \otimes \mathrm{Z}(B)) \trianglelefteq A \otimes \mathrm{Z}(B) = A \otimes K \cong A.$$

Since A is simple, it follows that $1 = 1 \otimes 1 \in I$ and $I = A \otimes B$. Therefore $A \otimes B$ is simple. □

Theorem III.7.14. *If A and B are central-simple algebras, then so is $A \otimes B$.*

Proof. Follows from Lemma III.7.9 and Lemma III.7.13. □

Theorem III.7.15. *An algebra A is central-simple if and only if the map $F\colon A \otimes A^o \to \mathrm{End}_K(A)$ with $F(a \otimes b)(x) := axb$ is an isomorphism of algebras.*

Proof. For $a, b \in A$, $f_{a,b}\colon A \to A$, $x \mapsto axb$ is a K-endomorphism with $f_{1,1} = \mathrm{id}_A$ and $f_{aa',b'b} = f_{a,b} \circ f_{a',b'}$. According to the axioms for algebras, the map $f\colon A \times A^o \to \mathrm{End}_K(A)$, $(a, b) \mapsto f_{a,b}$ is bilinear with $f((a, b)(a', b')) = f(aa', b'b) = f(a, b)f(a', b')$. By the universal property, F is a homomorphism of algebras.

Now let A be central-simple. According to Theorem III.7.14, $A \otimes A^o$ is simple and therefore $\mathrm{Ker}(F) = 0$. Because of $\dim A \otimes A^o = \dim(A)^2 = \dim \mathrm{End}_K(A)$, F is an isomorphism. Conversely, let F be an isomorphism. Then $A \otimes A^o \cong \mathrm{End}_K(A) \cong K^{n\times n}$ is central-simple. Because of $\mathrm{Z}(A) \otimes \mathrm{Z}(A) \cong \mathrm{Z}(A \otimes A^o) \cong \mathrm{Z}(K)$, it follows that $\mathrm{Z}(A) \cong K$. For $0 \neq I \trianglelefteq A$, we have $0 \neq I \otimes A^o \trianglelefteq A \otimes A^o$. Since $A \otimes A^o$ is simple, it follows that $\dim(I) \dim(A) = \dim(I \otimes A^o) = \dim(A \otimes A^o) = \dim^2(A)$ and $I = A$. Thus A is simple. □

Definition III.7.16. Let $[A]$ be the Morita equivalence class of a central-simple K-algebra A. Let $\mathrm{Br}(K) := \big\{[A] : A \text{ central-simple}\big\}$.

Remark III.7.17. According to Remark III.7.3, $[A]$ contains exactly one division algebra up to isomorphism.

Theorem III.7.18. *By*

$$[A] \cdot [B] := [A \otimes B]$$

$\mathrm{Br}(K)$ *becomes an abelian group.* $\mathrm{Br}(K)$ *is called the* Brauer group *of* K.

Proof. Let D, D_A, D_B be division algebras with $A \cong D_A^{n\times n}$, $B \cong D_B^{m\times m}$ and $D_A \times D_B \cong D^{k\times k}$. As in Lemma III.7.13, $A \otimes B \cong D^{nmk\times nmk}$. From this it follows easily that $[A] \cdot [B]$ does not depend on the choice of representatives A and B. According to Theorem III.7.14 and Remark III.7.5, $\cdot$ is well-defined, associative, commutative and $[K]$ is an identity element. According to Theorem III.7.15, $[A] \cdot [A^o] = [\mathrm{End}_K(A)] = [K^{n\times n}] = [K]$. Thus $[A^o]$ is the inverse of $[A]$. □

Example III.7.19.

(i) For every algebraically closed field K, $\mathrm{Br}(K) = 1$ according to Lemma II.12.6. In this situation, $\mathrm{Br}(K(X)) = 1$ also holds according to a theorem of Tsen.

(ii) If K is finite, then so is every (finite-dimensional) division algebra over K according to Wedderburn (Theorem II.8.7). Therefore, $\mathrm{Br}(K) = 1$ holds here as well.

Theorem III.7.20 (Skolem-Noether)**.** *Let A be central-simple and B simple. Then for all homomorphisms $f, g\colon B \to A$, there exists an $a \in A^\times$ with $f(x) = ag(x)a^{-1}$ for all $x \in B$.*

Proof. We consider $M_f := A$ as an $A \otimes B^o$-module (or A-B-bimodule) via

$$(a \otimes b)m := amf(b) \qquad (a \in A, b \in B, m \in M).$$

According to Lemma III.7.13, $A \otimes B^o$ is simple. In particular, $A \otimes B^o$ possesses only one simple module S up to isomorphism. Therefore, $M_f \simeq S^k$ for some $k \in \mathbb{N}$. Analogously, M_g is also an $A \otimes B^o$-module of the same dimension. Therefore, $M_f \simeq S^k \simeq M_g$. Let $\varphi\colon M_f \to M_g$ be an isomorphism. For $a := \varphi(1)$ and $x \in B$, it then holds that

$$ag(x) = (1 \otimes x)\varphi(1) = \varphi((1 \otimes x)1) = \varphi(f(x)) = \varphi((f(x) \otimes 1)1) = (f(x) \otimes 1)\varphi(1) = f(x)a.$$

For $y := \varphi^{-1}(1) \in A$, it holds that $ya = (y \otimes 1)\varphi(1) = \varphi((y \otimes 1)1) = \varphi(y) = 1 = \ldots = ay$. Therefore, $a \in A^\times$. □

Remark III.7.21. Since we only used the simplicity of $A \otimes B^o$ in the proof, the statement also holds if one swaps A and B. One can even dispense with the simplicity of B (Theorem A.8.18).

Example III.7.22. For $A = B = K^{n\times n}$ and $g = \mathrm{id}_A$, one obtains that $K^{n\times n}$ possesses only inner automorphisms (Exercise II.63).

Theorem III.7.23 (Double Centralizer Theorem)**.** *Let A be a central simple K-algebra and $B \subseteq A$ a simple subalgebra. Then:*

(i) The centralizer $C := \mathrm{C}_A(B) := \{a \in A : \forall b \in B : ab = ba\}$ is a simple algebra.

(ii) If D is a division algebra with $C \cong D^{k\times k}$, then $A \otimes B^o \cong D^{n\times n}$ with $k \mid n$.

(iii) $\dim A = \dim(B)\dim(C)$.

(iv) $\mathrm{C}_A(C) = B$.

Proof.

(i) Obviously C is an algebra. As in the proof of Skolem-Noether, we consider $M := A$ as a module of the simple algebra $A \otimes B^o$ via $(a \otimes b)m := amb$ for $m \in M$, $a \in A$ and $b \in B$. Let S be the simple $A \otimes B^o$-module and $A \otimes B^o \simeq S^n$ the regular module. For the division algebra $D := \mathrm{End}_{A\otimes B^o}(S)$ (Schur's Lemma), we have $(A \otimes B^o)^o \cong D^{n\times n}$. Let $M \simeq S^k$ and $E := \mathrm{End}_{A\otimes B^o}(M) \cong D^{k\times k}$. Let $\varphi \in E$ and $a := \varphi(1)$. For $b \in B$ it then holds that

$$ab = (1 \otimes b)\varphi(1) = \varphi((1 \otimes b)1) = \varphi((b \otimes 1)1) = (b \otimes 1)\varphi(1) = ba,$$

i. e. $a \in C$. This yields an algebra homomorphism $F\colon E \to C^o$, $\varphi \mapsto \varphi(1)$ (note $(\varphi\psi)(1) = \varphi(\psi(1)1) = \psi(1)\varphi(1)$). Since φ is uniquely determined by $\varphi(1)$, F is injective. Conversely, for every $c \in C$, the map $\varphi\colon M \to M$, $m \mapsto mc$ is an element of E, because

$$\varphi((a \otimes b)m) = \varphi(amb) = ambc = amcb = (a \otimes b)mc = (a \otimes b)\varphi(m).$$

Thus F is also surjective. Consequently $C \cong E^o$ is simple.

(ii) We have $C \cong E^o \cong (D^o)^{k\times k}$ and $A \otimes B^o \cong (D^o)^{n\times n}$. Because of $k \dim(A) \dim(B) = kn^2 \dim(D) = nk \dim(S) = n \dim(M_f) = n \dim(A)$, it follows that $k \mid n$.

(iii) Now it holds that

$$\begin{aligned}\dim(A)\dim(B)\dim(C) &= \dim(A \otimes B^o)\dim(E) = (nk\dim(D))^2 \\ &= (k\dim(S))^2 = \dim(M_f)^2 = \dim(A)^2.\end{aligned}$$

(iv) Since C is simple, we can replace B by C and obtain

$$\dim(C)\dim(\mathrm{C}_A(C)) = \dim(A) = \dim(C)\dim(B)$$

from (iii). Because of $B \subseteq \mathrm{C}_A(C)$, it follows that $\mathrm{C}_A(C) = B$. □

Lemma III.7.24. *A subfield L of a division algebra D is maximal if and only if $\mathrm{C}_D(L) = L$ holds.*

Proof. In the case $\mathrm{C}_D(L) = L$, L is certainly maximal. Conversely, let L be maximal and $c \in \mathrm{C}_D(L)$. Then $L(c)$ is also a subfield of D and it follows that $c \in L$. □

Theorem III.7.25. *Let L be a maximal subfield of a central division algebra D. Then $\dim D = \dim(L)^2$ and $L \otimes D \cong L^{n\times n}$ with $n := \dim L$.*

Proof. As a field, L is a simple subalgebra of D and simultaneously a division algebra. According to Lemma III.7.24 and the Double Centralizer Theorem, it holds that $\dim D = \dim(L)\dim(\mathrm{C}_D(L)) = \dim(L)^2$ and $D \otimes L \cong D \otimes L^o \cong L^{n\times n}$. Dimension comparison shows $n = \dim L$. □

Corollary III.7.26. *For every central simple algebra A, $\dim A$ is a square number.*

Proof. Let D be a central division algebra with $A \cong D^{n\times n}$. For dimension reasons, there always exists a maximal subfield of D. According to Theorem III.7.25, $\dim D$ is a square number and thus also $\dim A = n^2 \dim D$. □

Theorem III.7.27 (Frobenius)**.** *Every $\mathbb{R}$-division algebra is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. In particular,* $\mathrm{Br}(\mathbb{R}) = \langle[\mathbb{H}]\rangle \cong C_2$.

Proof. Let D be an $\mathbb{R}$-division algebra. We identify $\mathbb{R}$ with $\mathbb{R}1_D \subseteq D$ and assume $\mathbb{R} \neq D$. Let $L \subseteq D$ be a maximal subfield and $x \in L$ a primitive element of the separable field extension $\mathbb{R} \subseteq L$. For the irreducible minimal polynomial $\mu \in \mathbb{R}[X]$ of x, it is well known that $|L : \mathbb{R}| = |\mathbb{R}(x) : \mathbb{R}| = \deg \mu = 2$ by the Fundamental Theorem of Algebra. Let $\mu = X^2 + aX + b$ with $a, b \in \mathbb{R}$. Since μ is irreducible, $y := D_\mu = a^2 - 4b < 0$ holds and

$$L = \mathbb{R}(x) = \mathbb{R}(\sqrt{y}) = \mathbb{R}\Big(\frac{\sqrt{y}}{\sqrt{-y}}\Big) = \mathbb{R}(\sqrt{-1}) \cong \mathbb{C}.$$

We can therefore assume $x^2 = -1$. In the case $\mathrm{Z}(D) = L$, $D \cong \mathbb{C}$ by Lemma II.12.6. Otherwise, D is central with $\dim D = \dim(L)^2 = 4$ by Theorem III.7.25. As is well known, there exists $f \in \mathrm{Aut}(L)$ with $f(x) = -x$. We can extend f to $f\colon L \to D$. By Skolem-Noether, x and $-x$ are now conjugate in D. So let $y \in D$ with $yx = -xy$. Then

$$y^2 \in \mathrm{C}_D(L) \cap \mathbb{R}(y) = L \cap \mathbb{R}(y) = \mathbb{R}$$

by Lemma III.7.24. In the case $y^2 > 0$, $y \in \mathbb{R} \subseteq L$ would hold, because the polynomial $X^2 - y^2$ has at most two zeros in $\mathbb{R}(y)$. After normalization, we can thus assume $y^2 = -1$. Because $y \notin L$, $1, x, y, xy$ is an $\mathbb{R}$-basis of D and the multiplication table is uniquely determined. This shows $D \cong \mathbb{H}$. Since $\mathbb{C}$ is not central as an $\mathbb{R}$-algebra, $[\mathbb{H}]$ is the only non-trivial element in $\mathrm{Br}(\mathbb{R})$. It follows that $\mathrm{Br}(\mathbb{R}) = \langle[\mathbb{H}]\rangle \cong C_2$. □

Definition III.7.28. For a finite field extension $K \subseteq L$ and an algebra A, let $A_L := L \otimes A$. By

$$\lambda(x \otimes a) := (\lambda \otimes 1)(x \otimes a) = (\lambda x) \otimes a \qquad (\lambda, x \in L, a \in A)$$

A_L becomes an L-algebra. One says that A_L arises by *extension of scalars* from A. If there exists a ring isomorphism $A_L \cong L^{n\times n}$, then L is called a *splitting field* of A.

Remark III.7.29.

(i) Because of $A \cong A_K$, K is a splitting field of A if and only if $[A] = 1$ holds.

(ii) If $a_1, \ldots, a_n$ is a basis of A, then $1 \otimes a_1, \ldots, 1 \otimes a_n$ is an L-basis of A_L. In particular, $\dim A = \dim_L(A_L)$.

(iii) Let $f\colon A_L \to L^{n\times n}$ be a ring isomorphism. Restricting f yields a ring isomorphism

$$L \otimes \mathrm{Z}(A) \cong \mathrm{Z}(A_L) \to \mathrm{Z}(L^{n\times n}) \cong L.$$

In particular, A_L is central-simple. According to Skolem-Noether, there exists for the homomorphisms $f\colon \mathrm{Z}(A_L) \to L^{n\times n}$ and $g\colon \mathrm{Z}(A_L) \to L^{n\times n}$, $\lambda \otimes 1 \mapsto \lambda 1_n$ an $a \in \mathrm{GL}(n, L)$ with $f(x) = ag(x)a^{-1}$ for $x \in \mathrm{Z}(A_L)$. We can therefore assume $f(\lambda \otimes 1) = \lambda 1_n$ for $\lambda \in L$. Then f is also an isomorphism of L-algebras.

(iv) According to Theorem III.7.25, every central division algebra D has a splitting field L, say $D_L \cong L^{n\times n}$. Because of

$$L \otimes D^{k\times k} \overset{\text{III.7.11}}{\cong} D_L^{k\times k} \overset{\text{II.12.26}}{\cong} L^{nk\times nk}$$

L is also a splitting field of every central-simple algebra with basic algebra D.

(v) Along with L, every finite extension M of L is also a splitting field of A, because

$$A_M = M \otimes A \cong (M \otimes_L L) \otimes A \cong M \otimes_L A_L \cong M \otimes_L L^{n\times n} \cong (M \otimes_L L)^{n\times n} \cong M^{n\times n}.$$

(vi) As an application, we prove a theorem about symmetric algebras .

Lemma III.7.30. *For the commutator space of every K-algebra A, $\gamma(A) \neq A$ holds.*

Proof. Assume indirectly $\gamma(A) = A$. For $\overline{A} = A/\mathrm{J}(A)$, then $\gamma(\overline{A}) = \overline{A}$ holds. We can thus assume that A is semisimple. According to Artin-Wedderburn, A is a direct sum of matrix algebras over division algebras. According to Lemma II.12.34, we can assume $A = D^{n\times n}$ for a division algebra D. Because of $\lambda(ab - ba) = (\lambda a)b - b(\lambda a)$ for $a, b \in A$ and $\lambda \in K$, every element in A is a sum of commutators (one does not need linear combinations). Since this characterization is independent of K, we can assume $K = \mathrm{Z}(D)$, so that A becomes a central-simple algebra. Let $e_1, \ldots, e_n \in A$ be a K-basis. Then $\gamma(A)$ is generated by the elements of the form $e_ie_j - e_je_i$. Thus $\gamma(A)$ depends only on the structure constants of A. According to Remark III.7.29, A has a splitting field L with $A_L \cong L^{s\times s}$. Now $1 \otimes e_1, \ldots, 1 \otimes e_n$ is a basis of A_L with the same structure constants. We can therefore replace (K, A) by (L, A_L). Now, however, Lemma II.12.34 yields the contradiction $\gamma(A) = \gamma(L^{s\times s}) \neq A$. □

Theorem III.7.31 (Eilenberg-Nakayama)**.** *Every semisimple algebra is symmetric.*

Proof. According to Artin-Wedderburn and Example II.13.10, it suffices to show that every division algebra D is symmetric. According to Lemma III.7.30, there exists a non-trivial K-linear map $\lambda\colon D \to K$ with $\gamma(D) \subseteq \mathrm{Ker}(\lambda)$. It is easy to show that $\beta(x, y) := \lambda(xy)$ for $x, y \in D$ defines a symmetric, associative, non-degenerate bilinear form. □

Theorem III.7.32. *For every finite field extension $K \subseteq L$, the map*

$$\Gamma\colon \mathrm{Br}(K) \to \mathrm{Br}(L), \qquad [A] \mapsto [A_L]$$

is a homomorphism. One sets $\mathrm{Br}(L|K) := \mathrm{Ker}(\Gamma)$.

Proof. Let A be a central simple K-algebra. According to Lemma III.7.13, A_L is simple and according to Lemma III.7.9, $\mathrm{Z}(A_L) \cong L \otimes \mathrm{Z}(A) \cong L \otimes K \cong L$. Thus $[A_L] \in \mathrm{Br}(L)$. Let $[A] = [B]$ with $A \cong D^{n\times n}$ and $B \cong D^{m\times m}$ for a division algebra D. Then $A_L = L \otimes D^{n\times n} \cong D_L^{n\times n}$ according to Lemma III.7.11. As already shown, D_L is a simple L-algebra. Thus there exists a division algebra E with $D_L \cong E^{k\times k}$ and it follows that $A_L \cong E^{nk\times nk}$ as well as $B_L \cong E^{mk\times mk}$. Therefore $[A_L] = [B_L]$ and Γ is well-defined. For $[A], [B] \in \mathrm{Br}(K)$, it finally holds that

$$(A \otimes B)_L = L \otimes A \otimes B \cong A \otimes (L \otimes_L L) \otimes B \cong (A \otimes L) \otimes_L (L \otimes B) \cong A_L \otimes_L B_L.$$

This shows $\Gamma([A][B]) = \Gamma([A \otimes B]) = [(A \otimes B)_L] = [A_L][B_L] = \Gamma([A])\Gamma([B])$. □

Remark III.7.33. Obviously, $\mathrm{Br}(L|K)$ consists precisely of the central simple K-algebras with splitting field L. According to Remark III.7.29, it therefore holds that

$$\mathrm{Br}(K) = \bigcup_{\substack{L\supseteq K,\\ |L:K|<\infty}} \mathrm{Br}(L|K).$$

We show that it suffices to take the union over Galois extensions of K.

Example III.7.34. According to Theorem III.7.25, $\mathbb{C}$ is a splitting field of $\mathbb{H}$. Therefore $\mathrm{Br}(\mathbb{C}|\mathbb{R}) = \mathrm{Br}(\mathbb{R}) = \langle \mathbb{H} \rangle$ according to Theorem III.7.27.

Theorem III.7.35 (NOETHER-JACOBSON)**.** *Every central division algebra D possesses a maximal subfield L such that $K \subseteq L$ is separable.*

Proof (HERSTEIN). We argue by induction on $\dim(D)$. According to Example II.3.3, we can assume $\operatorname{char} K = p > 0$ and $D \neq K$. If for every $x \in D$ the field $K(x)$ is separable over K, then the assertion follows from Theorem III.7.25. Now let $x \in D \setminus K$ be inseparable with minimal polynomial μ. Because of $\mu' = 0$, there exists an irreducible polynomial $\nu \in K[X]$ with $\mu(X) = \nu(X^p)$. Then ν is the minimal polynomial of x^p. If x^p is also inseparable, we can consider x^{p^2} and so on. In the end, we obtain an inseparable element $x \in D$ such that x^p is separable. Let us assume $x^p \in K$ and consider the map

$$\delta \colon D \to D, \qquad d \mapsto dx - xd.$$

Because $x \notin K = \mathrm{Z}(D)$, there exists a $y \in D$ with $\delta(y) \neq 0$. Let $\delta_1, \delta_2 \in \mathrm{End}_K(D)$ with $\delta_1(x) := dx$ and $\delta_2(x) := xd$. Then $\delta = \delta_1 - \delta_2$ holds in $\mathrm{End}_K(D)$. Because of $\operatorname{char} K = p$, it follows that $\delta^p = (\delta_1 - \delta_2)^p = \delta_1^p - \delta_2^p$. In particular,

$$\delta^p(y) = yx^p - x^p y = 0$$

because of $x^p \in K$. Let $m \in \mathbb{N}$ be minimal with $\delta^m(y) = 0$ and let $z := \delta^{m-1}(y)$ as well as $w := \delta^{m-2}(y)$. Then $z = \delta(w) = wx - xw$. Set $u := x^{-1}z$. Because of $\delta(z) = 0$, we have $ux = xu$. It follows that

$$x = zu^{-1} = (wx - xw)u^{-1} = wxu^{-1} - xwu^{-1} = (wu^{-1})x - x(wu^{-1}).$$

For $a := wu^{-1}$, it thus holds that $x = ax - xa$ and $a = 1 + xax^{-1}$. As at the beginning of the proof, there exists a power $p^n = q$ such that a^q is separable. But now $a^q = 1 + xa^q x^{-1}$. In particular, x and a^q are not commutable and it follows that $a^q \notin K$. Thus we have found a separable extension $K \subsetneq K(a^q) =: M$ (Theorem II.3.8).

Clearly $C := \mathrm{C}_D(M)$ is a division algebra and by Theorem III.7.23 we have $M \subseteq \mathrm{Z}(C) \subseteq \mathrm{C}_D(C) = M$. Thus C is central over M with $\dim_M(C) < \dim_K(D)$. By induction, C possesses a maximal subfield L that is separable over M. By Lemma II.3.7, L is then also separable over K. Now it holds that

$$\dim D \overset{\text{III.7.23}}{=} \dim(M)\dim(C) \overset{\text{I.9.5}}{=} \dim_M(C)\dim(M)^2 \overset{\text{III.7.25}}{=} \dim_M(L)^2\dim(M)^2 \overset{\text{I.9.5}}{=} \dim(L)^2.$$

By Theorem III.7.25, L is therefore also a maximal subfield of D. □

Corollary III.7.36. *Every central simple algebra possesses a splitting field L such that $K \subseteq L$ is a Galois extension.*

Proof. According to Remark III.7.29, it suffices to prove the assertion for central division algebras D. By Theorem III.7.35, there exists a maximal subfield $L \subseteq D$ such that $K \subseteq L$ is separable. By Theorem II.3.4, $K \subseteq L$ is contained in a Galois extension $K \subseteq M$. Now M is also a splitting field of D. □

Definition III.7.37. In the situation of Corollary III.7.36, L is called a *Galois splitting field* of A.

Lemma III.7.38. *Let L be a splitting field of a central division algebra D. Then L is isomorphic to a subfield of $D^{n\times n}$, where $\dim(L)^2 = n^2 \dim D$ holds.*

Proof. Let $D_L \cong L^{k\times k}$ and let $S \simeq L^{k\times 1}$ be the simple D_L-module. By $ds := (1 \otimes d)s$ for $s \in S$ and $d \in D$, S becomes a D-module. For $\lambda \in L$, it holds that $\lambda ds = (\lambda \otimes d)s = d\lambda s$. Therefore, the scalar multiplication of L on S induces an algebra homomorphism $f\colon L \to \mathrm{End}_D(S)$, which is injective since L is simple. Since S has a basis over D (Theorem II.9.10), it holds that $\mathrm{End}_D(S) \cong D^{n\times n}$ with $n := \dim_D(S)$. Now $\dim(D)\dim(L) = \dim(D_L) = k^2 \dim L$ and

$$k \dim L = \dim S = \dim_D(S) \dim D = nk^2.$$

It follows that $\dim(L)^2 = n^2k^2 = n^2 \dim D$. □

Definition III.7.39. Let $K \subseteq L$ be a Galois extension and $G := \mathrm{Gal}(L|K)$. Let $C^n(G, L^\times)$ be the group of all mappings $G^n \to L^\times$ with respect to pointwise operation. A $\gamma \in C^2(G, L^\times)$ is called a *factor system* (or 2-*cocycle*), if

$$\boxed{\gamma(x,y)\gamma(xy,z) = x(\gamma(y,z))\gamma(x,yz)} \qquad \forall x,y,z \in G. \tag{III.7.1}$$

The factor systems form a subgroup $Z^2(G, L^\times) \leq C^2(G, L^\times)$.

Lemma III.7.40. *The mapping $\partial\colon C^1(G, L^\times) \to Z^2(G, L^\times)$ with $\partial\lambda(x,y) = \lambda(x)x(\lambda(y))\lambda(xy)^{-1}$ for $\lambda \in C^1(G, L^\times)$ and $x, y \in G$ is a homomorphism.*

Proof. For $x, y, z \in G$ it holds that

$$\begin{aligned}\partial\lambda(x,y)\partial\lambda(xy,z) &= \lambda(x)x(\lambda(y))\lambda(xy)^{-1}\lambda(xy)(xy)(\lambda(z))\lambda(xyz)^{-1}\\ &= x(\lambda(y))x(y(\lambda(z)))\lambda(x)\lambda(xyz)^{-1}\\ &= x(\lambda(y)y(\lambda(z))\lambda(yz)^{-1})\lambda(x)x(\lambda(yz))\lambda(xyz)^{-1} = x(\partial\lambda(y,z))\partial\lambda(x,yz).\end{aligned}$$

Therefore ∂ maps into $Z^2(G, L^\times)$. The homomorphism property is obvious. □

Definition III.7.41. One sets $B^2(G, L^\times) := \partial(C^1(G, L^\times))$ and calls

$$H^2(G, L^\times) := Z^2(G, L^\times)/B^2(G, L^\times)$$

the *second cohomology group* of G with values in $L^\times$.

Lemma III.7.42. *For $\gamma \in Z^2(G, L^\times)$ and $x \in G$ it holds that $\gamma(1,x) = \gamma(1,1)$ and $x(\gamma(1,1)) = \gamma(x,1)$. Every element of $H^2(G, L^\times)$ contains a* normalized *factor system γ with $\gamma(1,x) = \gamma(x,1) = 1$ for all $x \in G$.*

Proof. Setting $x = y = 1$ in (III.7.1), it follows that $\gamma(1,1)\gamma(1,z) = \gamma(1,z)\gamma(1,z)$. Setting $y = z = 1$, we obtain $\gamma(x,1)\gamma(x,1) = x(\gamma(1,1))\gamma(x,1)$. For the second assertion, one replaces γ by $\delta := \gamma\partial\lambda$ with $\lambda(1) := \gamma(1,1)^{-1}$. Then

$$\delta(1,x) = \delta(1,1) = \gamma(1,1)\lambda(1)\lambda(1)\lambda(1)^{-1} = 1$$

and $\delta(x,1) = x(\delta(1,1)) = 1$. □

Theorem III.7.43. *For $\overline{\gamma} \in H^2(G, L^\times)$, we have $\overline{\gamma}^{|G|} = 1$.*

Proof. Let $\delta(x) := \prod_{g\in G} \gamma(x,g)$ for $x \in G$. According to (III.7.1),

$$\gamma(x,y)^{|G|}\delta(xy) = \prod_{z\in G} \gamma(x,y)\gamma(xy,z) = \prod_{z\in G} x(\gamma(y,z))\gamma(x,yz) = x(\delta(y))\delta(x).$$

This shows $\gamma^{|G|} = \partial\delta \in B^2(G, L^\times)$. □

Example III.7.44. We consider the Galois extension $\mathbb{Q} \subseteq \mathbb{Q}(\mathrm{i})$ with $G := \mathrm{Gal}(\mathbb{Q}(\mathrm{i})|\mathbb{Q}) = \langle\sigma\rangle$, where σ is the complex conjugation. Let $\gamma \in Z^2(G, \mathbb{Q}(\mathrm{i})^\times)$ be normalized. Then γ is uniquely determined by $\zeta := \gamma(\sigma,\sigma)$. From (III.7.1) with $x = y = z = \sigma$, it follows that $\sigma(\zeta) = \zeta \in \mathbb{Q}^\times$. It is easy to check that the other assignments of x, y, z yield no further restrictions. Let $\gamma' := \gamma\partial\mu$ also be normalized with $\mu \in C^1(G, \mathbb{Q}(\mathrm{i})^\times)$. Then $1 = \gamma'(1,1) = \gamma(1,1)\mu(1)\mu(1)\mu(1)^{-1} = \mu(1)$. For $\mu(\sigma) = a + b\mathrm{i}$, we have

$$\zeta' = \gamma'(\sigma,\sigma) = \zeta\mu(\sigma)\sigma(\mu(\sigma))\mu(\sigma^2)^{-1} = \zeta(a^2+b^2).$$

With $a = \frac{a_1}{a_2}$ and $b = \frac{b_1}{b_2}$ (where $a_1, a_2, b_1, b_2 \in \mathbb{Z}$), it follows that

$$\zeta' = \zeta\frac{(a_1b_2)^2 + (b_1a_2)^2}{(a_2b_2)^2}.$$

According to Theorem II.5.34, the prime factors $p \equiv 3 \pmod 4$ occur with even multiplicity in $(a_1b_2)^2 + (b_1a_2)^2$. The multiplicities of p in ζ and ζ' thus have the same parity. For each such prime number, we now define $\gamma_p \in Z^2(G, \mathbb{Q}(\mathrm{i})^\times)$ by $\gamma_p(\sigma,\sigma) = p$. For distinct $p, q \in \mathbb{P}$ with $p \equiv 3 \equiv q \pmod 4$, we then have $\overline{\gamma_p} \neq \overline{\gamma_q}$ in $H^2(G, \mathbb{Q}(\mathrm{i})^\times)$. From Exercise I.5, it follows that $|H^2(G, \mathbb{Q}(\mathrm{i})^\times)| = \infty$. Since $H^2(G, \mathbb{Q}(\mathrm{i})^\times)$ is countable, more precisely

$$H^2(G, \mathbb{Q}(\mathrm{i})^\times) \cong \coprod_{k=1}^{\infty} C_2$$

holds according to Theorem III.7.43.

Definition III.7.45. Let D be a central division algebra with Galois splitting field L. According to Lemma III.7.38, L can be embedded into the central simple algebra $A := D^{n\times n}$. In this case, $\dim A = \dim(L)^2$ holds. According to the Double Centralizer Theorem, on the other hand, $\dim A = \dim(L)\dim(\mathrm{C}_A(L)) \geq \dim(L)^2$. This shows $\mathrm{C}_A(L) = L$. Let $G := \mathrm{Gal}(L|K)$ and $x \in G$. According to Skolem-Noether, x can be extended to an inner automorphism of A. So let $a_x \in A^\times$ with $x(\lambda) = a_x\lambda a_x^{-1}$ for all $\lambda \in L$. Because $\mathrm{C}_A(L) = L$, a_x is uniquely determined up to L-multiplication. If $y \in G$ is also given, then

$$a_{xy}\lambda a_{xy}^{-1} = (xy)(\lambda) = x(y(\lambda)) = a_xa_y\lambda a_y^{-1}a_x^{-1}.$$

Therefore $a_xa_y = \gamma(x,y)a_{xy}$ with $\gamma(x,y) \in L^\times$.

Lemma III.7.46. *With the notation from Definition III.7.45, $\gamma\colon G \times G \to L^\times$ is a factor system. The corresponding coset $\overline{\gamma} \in H^2(G, L^\times)$ does not depend on the choice of the a_x.*

Proof. For $x, y, z \in G$ we have

$$\begin{aligned}\gamma(x,y)\gamma(xy,z)a_{xyz} &= \gamma(x,y)a_{xy}a_z = (a_xa_y)a_z = a_x(a_ya_z) = a_x\gamma(y,z)a_{yz}\\ &= x(\gamma(y,z))a_xa_{yz} = x(\gamma(y,z))\gamma(x,yz)a_{xyz}.\end{aligned}$$

This shows $\gamma \in Z^2(G, L^\times)$. Now let $\lambda\colon G \to L^\times$ with $a'_x = \lambda(x)a_x$ and $a'_x a'_y = \gamma'(x,y)a'_{xy}$. Then it follows that

$$\gamma'(x,y)\lambda(xy)a_{xy} = \gamma'(x,y)a'_{xy} = a'_x a'_y = \lambda(x)a_x\lambda(y)a_y = \lambda(x)x(\lambda(y))\gamma(x,y)a_{xy}$$

and $\gamma'(x,y) = \gamma(x,y)\lambda(x)x(\lambda(y))\lambda(xy)^{-1}$. This shows $\gamma' = \gamma\partial_\lambda \in \overline{\gamma}$. □

Definition III.7.47. Let $K \subseteq L$ be a Galois extension, $G := \mathrm{Gal}(L|K)$ and $\gamma \in Z^2(G, L^\times)$. We define the *crossed group algebra* $L_\gamma G$ as the K-vector space LG with the multiplication

$$\lambda_x x \cdot \lambda_y y := \lambda_x x(\lambda_y)\gamma(x,y)xy \qquad (x, y \in G, \lambda_x, \lambda_y \in L).$$

Theorem III.7.48. *With the notation from Definition III.7.47, $L_\gamma G$ is a central simple K-algebra with splitting field L and $\dim_K(L_\gamma G) = |G|^2 = |L:K|^2$.*

Proof. For $x, y, z \in G$ we have

$$\begin{aligned}(\lambda_x x \cdot \lambda_y y) \cdot \lambda_z z &= \lambda_x x(\lambda_y)\gamma(x,y)xy \cdot \lambda_z z = \lambda_x x(\lambda_y)\gamma(x,y)(xy)(\lambda_z)\gamma(xy,z)xyz\\ &= \lambda_x x(\lambda_y y(\lambda_z))\gamma(x,y)\gamma(xy,z)xyz = \lambda_x x(\lambda_y y(\lambda_z))x(\gamma(y,z))\gamma(x,yz)xyz\\ &= \lambda_x x \cdot \lambda_y y(\lambda_z)\gamma(y,z)yz = \lambda_x x \cdot (\lambda_y y \cdot \lambda_z z).\end{aligned}$$

This shows the associativity of the multiplication in $A := L_\gamma G$. The identity element is $e := \gamma(1,1)^{-1}1$, because according to Lemma III.7.42 we have

$$\begin{aligned}e \cdot \lambda_x x &= \gamma(1,1)^{-1}\lambda_x\gamma(1,x)x = \lambda_x x,\\ \lambda_x x \cdot e &= \lambda_x x(\gamma(1,1))^{-1}\gamma(x,1)x = \lambda_x x\end{aligned}$$

for all $x \in G$. We can therefore identify L with $Le \subseteq A$. The distributive laws hold by linear extension of the multiplication rule. For $\mu \in K$ we have

$$\mu(\lambda_x x \cdot \lambda_y y) = \mu\lambda_x x(\lambda_y)\gamma(x,y)xy = (\mu\lambda_x x) \cdot \lambda_y y = \lambda_x x(\mu\lambda_y)\gamma(x,y)xy = \lambda_x x \cdot (\mu\lambda_y y).$$

Thus A is a K-algebra.

Let $a := \sum_{x\in G} \lambda_x x \in \mathrm{C}_A(L)$. For $\mu \in L$ we have

$$\sum_{x\in G} \mu\lambda_x x = \mu e \cdot a = a \cdot \mu e = \sum_{x\in G} \lambda_x x(\mu)x.$$

In the case $\lambda_x \neq 0$ it follows that $x(\mu) = \mu$ for all $\mu \in L$. This shows $a = \lambda_1 1$ and $\mathrm{C}_A(L) = L$. If additionally $a \in \mathrm{Z}(A)$, then

$$x(\lambda_1\gamma(1,1)) = x(\lambda_1)\gamma(x,1)x = x \cdot a = a \cdot x = \lambda_1\gamma(1,x)x = \lambda_1\gamma(1,1)x$$

for all $x \in G$. It follows that $\lambda_1\gamma(1,1) \in L^G = K$ and $\mathrm{Z}(A) = Ke$, i. e. A is central.

Now let $0 \neq I \trianglelefteq A$. We choose $a = \sum_{x\in G} \lambda_x x \in I \setminus \{0\}$ such that as many λ_x as possible vanish. After multiplication by an $x \in G$ we can assume $\lambda_1 \neq 0$. Let $\mu \in L$ be arbitrary. Then

$$I \ni a \cdot \mu e - \mu e \cdot a = \sum_{x\in G\setminus\{1\}} (\lambda_x x(\mu) - \mu\lambda_x)x$$

and it follows that $a \cdot \mu e = \mu e \cdot a$. Therefore $a \in \mathrm{C}_A(L) = L$. In particular, a is invertible and one obtains $I = A$. Thus A is simple. By the Double Centralizer Theorem, $L \otimes A \cong A \otimes L^o \cong L^{n\times n}$. Thus L is a splitting field of A. If $\mu_1, \ldots, \mu_n \in L$ is a K-basis of L, then $\{\mu_i g : i = 1, \ldots, n, g \in G\}$ is a K-basis of $L_\gamma G$. The last assertion therefore follows from $|G| = |L:K|$. □

Lemma III.7.49. *For $\gamma, \delta, \in Z^2(G, L^\times)$ we have $L_\gamma G \cong L_\delta G$ if and only if $\gamma \equiv \delta \pmod{B^2(G, L^\times)}$.*

Proof. Let $A := L_\gamma G$, $B := L_\delta G$ and $f\colon A \to B$ be an isomorphism of K-algebras. As in the proof of Theorem III.7.48, L can be viewed as a subfield of A and B (consider $L \to A$, $\lambda \mapsto \lambda\gamma(1,1)^{-1}1$). By Skolem-Noether, we can then assume $f(\lambda) = \lambda$ for all $\lambda \in L$. Let $x \in G$ and $f(x) = \sum_{g\in G} \mu_g g \in B$. For $\lambda \in L$, it holds that

$$\sum_{g\in G} \mu_g g(\lambda) g = f(x)\lambda = f(x)f(\lambda) = f(x\lambda) = f(x(\lambda)x) = x(\lambda)f(x) = \sum_{g\in G} x(\lambda)\mu_g g.$$

In the case $\mu_g \neq 0$, one obtains $g(\lambda) = x(\lambda)$ for all $\lambda \in L$. This shows $f(x) = \mu_x x =: \mu(x)x$. Now

$$\begin{aligned}\gamma(x,y)\mu(xy)xy &= \gamma(x,y)f(xy) = f(\gamma(x,y)xy) = f(x\cdot y) = f(x)\cdot f(y)\\ &= \mu(x)x\cdot\mu(y)y = \mu(x)x(\mu(y))\delta(x,y)xy,\end{aligned}$$

thus $\gamma = \delta\partial\mu \equiv \delta \pmod{B^2(G, L^\times)}$.

Conversely, let $\gamma = \delta\partial\mu$ with $\mu \in C^1(G, L^\times)$. We consider the K-linear map $f\colon A \to B$, $\lambda x \mapsto \lambda\mu(x)x$ for $x \in G$ and $\lambda \in L$. Because of $\gamma(1,1) = \delta(1,1)\mu(1)\mu(1)\mu(1)^{-1} = \delta(1,1)\mu(1)$, it holds that

$$f(1_A) = f(\gamma(1,1)^{-1}1) = \gamma(1,1)^{-1}\mu(1)1 = \delta(1,1)^{-1}1 = 1_B.$$

For $x, y \in G$ and $\lambda_x, \lambda_y \in L$, we have

$$\begin{aligned}f(\lambda_x x\cdot\lambda_y y) &= f(\lambda_x x(\lambda_y)\gamma(x,y)xy) = \lambda_x x(\lambda_y)\gamma(x,y)\mu(xy)xy\\ &= \lambda_x x(\lambda_y)\delta(x,y)\mu(x)x(\mu(y))xy = \lambda_x\mu(x)x\cdot\lambda_y\mu(y)y = f(\lambda_x x)\cdot f(\lambda_y y).\end{aligned}$$

Thus f is a homomorphism. Since A is simple, f is injective. Because of $\dim A = |G|^2 = \dim B$, f is also surjective. □

Remark III.7.50. For the construction of $L_\gamma G$, one can choose a normalized factor system $\gamma \in Z^2(G, L^\times)$ according to Lemma III.7.49. Then $1 \in G$ is the identity element in $L_\gamma G$ as in the usual group algebra LG. Since $L = L1$ is a subfield of $L_\gamma G$, one can also consider $L_\gamma G$ as an L-vector space with basis G. In contrast to LG, however, $L_\gamma G$ is not an L-algebra (even if γ is trivial), because for that one would need $L \subseteq \mathrm{Z}(L_\gamma G)$.

Theorem III.7.51. *For every Galois extension $K \subseteq L$ with $G := \mathrm{Gal}(L|K)$,*

$$\begin{aligned}\Gamma\colon H^2(G, L^\times) &\to \mathrm{Br}(L|K),\\ \gamma &\mapsto [L_\gamma G]\end{aligned}$$

is an isomorphism.

Proof (Chase).
Step 1: Γ is bijective.
According to Theorem III.7.48 and Lemma III.7.49, Γ is well-defined. Let D be a central division algebra with splitting field L. As in Definition III.7.45, L is isomorphic to a subalgebra of $A := D^{n\times n}$ and one obtains $a_x \in A^\times$ and $\gamma \in Z^2(G, L^\times)$ with $x(\lambda) = a_x\lambda a_x^{-1}$ and $a_x a_y = \gamma(x,y)a_{xy}$ for $x, y \in G$ and $\lambda \in L$. We define the K-linear map $f\colon L_\gamma G \to A$, $\lambda x \mapsto \lambda a_x$ with $\lambda \in L$ and $x \in G$. For $\lambda x, \mu y \in L_\gamma G$ it holds that

$$f(\lambda x\cdot\mu y) = f(\lambda x(\mu)\gamma(x,y)xy) = \lambda x(\mu)\gamma(x,y)a_{xy} = \lambda x(\mu)a_x a_y = \lambda a_x\cdot\mu a_y = f(\lambda x)f(\mu y),$$

i. e. f is a homomorphism of algebras. Since $L_\gamma G$ is simple, f is injective. According to Lemma III.7.38

$$\dim(L_\gamma G) = |L : K|^2 = \dim(L)^2 = n^2 \dim D = \dim A.$$

Thus f is an isomorphism and Γ is surjective.

Let $\gamma, \delta \in Z^2(G, L^\times)$ with $[L_\gamma G] = [L_\delta G]$. Then $L_\gamma G$ and $L_\delta G$ have a common base algebra D. Because of $\dim(L_\gamma G) = \dim(L)^2 = \dim(L_\delta G)$ it follows that $L_\gamma G \cong D^{n\times n} \cong L_\delta G$. From Lemma III.7.49 it follows that $\overline{\gamma} = \overline{\delta}$ in $H^2(G, L^\times)$. Therefore Γ is bijective.

Step 2: Γ is a homomorphism.
Let $\gamma, \delta \in Z^2(G, L^\times)$ be normalized, $A := L_\gamma G$, $B := L_\delta G$ and $C := L_{\gamma\delta} G$. According to Remark III.7.50, A is an L-A-bimodule and B is an L-B-bimodule. Thus $V := A^o \otimes_L B$ is an A^o-B-bimodule, which we can view as an $A \otimes_K B$-right module. For $a \otimes b \in V$ and $x \otimes y \in A \otimes_K B$ it holds that

$$(a \otimes b)(x \otimes y) = (x * a) \otimes by = ax \otimes by,$$

where $*$ denotes the multiplication in A^o. Especially for $\lambda \in L$ it holds that

$$\lambda a \otimes b = (a * \lambda) \otimes b = a \otimes \lambda b.$$

We now define a scalar multiplication on V with C from the left. For $\lambda x \in C$ the map $A^o \times B \to V$, $(a, b) \mapsto \lambda xa \otimes xb$ is balanced. Therefore

$$(\lambda x)(a \otimes b) := \lambda xa \otimes xb$$

is well-defined. By linear extension one obtains the distributive laws. For $\lambda_x x, \lambda_y y \in C$ it holds that

$$\begin{aligned}(\lambda_x x \cdot \lambda_y y)(a \otimes b) &= (\lambda_x x(\lambda_y)\gamma(x,y)\delta(x,y)xy)(a \otimes b) = \lambda_x x(\lambda_y)\gamma(x,y)\delta(x,y)xya \otimes xyb \\ &= \lambda_x x(\lambda_y)\gamma(x,y)xya \otimes \delta(x,y)xyb = (\lambda_x x)(\lambda_y ya \otimes yb) \\ &= (\lambda_x x)((\lambda_y y)(a \otimes b))\end{aligned}$$

Thus V is a C-left module. For $a' \otimes b' \in A \otimes_K B$ it holds that

$$(\lambda x(a \otimes b))(a' \otimes b') = (\lambda xa \otimes xb)(a' \otimes b') = \lambda xaa' \otimes xbb' = \lambda x(aa' \otimes bb') = \lambda x((a \otimes b)(a' \otimes b')).$$

The scalar multiplication from the right thus yields a homomorphism $f\colon (A \otimes_K B)^o \to \mathrm{End}_C(V)$. Since $A \otimes_K B$ is simple, f is injective.

With $n := |G| = \dim L$ it holds that $\dim_K(V) = |L : K| \dim_L(A) \dim_L(B) = n^3$. Let $C \simeq S^r$ be the decomposition of the regular C-module with the simple module S of the simple algebra C. Because of $n^2 = \dim C = r \dim S$ it follows that $V \simeq S^{nr}$, since with C also V is semisimple. According to Lemma II.7.20 it holds that $\mathrm{End}_C(V) \cong D^{nr\times nr}$ with the division algebra $D := \mathrm{End}_C(S)$. Furthermore

$$n^2 = \dim(C^o) = \dim \mathrm{End}_C(C) = \dim(D^{r\times r}) = r^2 \dim D.$$

This shows

$$\dim(A \otimes_K B)^o = n^4 = n^2 r^2 \dim D = \dim \mathrm{End}_C(V).$$

Therefore f is an isomorphism. In particular $(A \otimes_K B)^o \cong D^{nr\times nr}$ as well as $C^o \cong D^{r\times r}$. This yields $[A] \cdot [B] = [C]$, i. e. Γ is a homomorphism. □

Corollary III.7.52. *For every field K, $\mathrm{Br}(K)$ is a torsion group, i. e. every element has finite order.*

Proof. This follows from Remark III.7.33, Corollary III.7.36, Theorem III.7.51 and Theorem III.7.43. □

Example III.7.53. According to Theorem III.7.51 and Example III.7.44, it holds that

$$\mathrm{Br}(\mathbb{Q}(\mathrm{i})|\mathbb{Q}) \cong H^2(G, \mathbb{Q}(\mathrm{i})^\times) \cong \coprod_{i=1}^{\infty} C_2.$$

With the Albert-Brauer-Hasse-Noether theorem from class field theory, one shows

$$\mathrm{Br}(\mathbb{Q}) \cong C_2 \times \bigtimes_{k=1}^{\infty} \mathbb{Q}/\mathbb{Z}.$$

Definition III.7.54. According to Corollary III.7.26, the dimension of a central simple algebra A is a square number. One calls $\deg A := \sqrt{\dim A}$ the *degree* and $e(A) := \deg(A^b)$ the *index* of A, where A^b is the basic algebra of A.

Remark III.7.55. For a central division algebra D with splitting field L, it holds that $\deg D \mid \dim L$ according to Lemma III.7.38. The following theorem therefore improves Theorem III.7.43.

Theorem III.7.56. *For $[A] \in \mathrm{Br}(K)$, it holds that $[A]^{e(A)} = 1$.*

Proof. We can assume that $D := A$ is a division algebra with $e := e(A) = \deg(D)$. Let L be a Galois splitting field of D. As in Definition III.7.45, we can embed L into $A := D^{n\times n}$ (a "new" algebra A). In this case, $(ne)^2 = n^2 \dim D = \dim A = \dim(L)^2$ and $\dim L = ne$. Let $G := \mathrm{Gal}(L|K)$. Then there exist $a_x \in A^\times$ with $x(\lambda) = a_x \lambda a_x^{-1}$ and $a_x a_y = \gamma(x,y) a_{xy}$ for $x, y \in G$, $\lambda \in L$ and $\gamma \in C^2(G, L^\times)$. Let $S = D^{n\times 1}$ be the simple A-module. By restriction, S becomes an L-vector space. In this case,

$$\dim_L(S) = \frac{\dim S}{\dim L} = \frac{n \dim D}{ne} = e.$$

Let $v_1, \ldots, v_e$ be an L-basis of S. For $x \in G$, let $\alpha(x) = (\alpha_{ij}(x)) \in L^{e\times e}$ with

$$a_x v_i = \sum_{j=1}^{e} \alpha_{ij}(x) v_j.$$

For $x, y \in G$, it then holds that

$$\begin{aligned}\gamma(x,y) \sum_{j=1}^{e} \alpha_{ij}(xy) v_j = \gamma(x,y) a_{xy} v_i = a_x a_y v_i = a_x \Big(\sum_{k=1}^{e} \alpha_{ik}(y) v_k \Big) \\ = \sum_{k=1}^{e} x(\alpha_{ik}(y)) a_x v_k = \sum_{k,j=1}^{e} x(\alpha_{ik}(y)) \alpha_{kj}(x) v_j.\end{aligned}$$

This shows $\gamma(x,y)\alpha(xy) = x(\alpha(y))\alpha(x)$ for all $x, y \in G$. Finally, let $\lambda(x) := \det(\alpha(x))$. Then it follows

$$\gamma(x,y)^e \lambda(xy) = \det(\gamma(x,y)\alpha(xy)) = \det(x(\alpha(y))) \det(\alpha(x)) = x(\lambda(y))\lambda(x).$$

Thus $\gamma^e = \partial\lambda \in B^2(G, L^\times)$ and the claim follows from Theorem III.7.51. □

Lemma III.7.57. *For every central simple algebra A, $e(A)$ and $|\langle [A] \rangle|$ have the same prime divisors.*

Proof. According to Theorem III.7.56, $|\langle [A]\rangle|$ is a divisor of $e(A)$. We therefore only need to show that a prime divisor $p \mid e(A)$ also divides $|\langle [A]\rangle|$. Let $A \cong D^{n\times n}$ for a division algebra D. Let L be a Galois splitting field of D with $G := \mathrm{Gal}(L|K)$. Then $|G|^2 = \dim(L)^2 = n^2 \dim D = (ne(A))^2$ (Lemma III.7.38) and p divides $|G|$. Let $P \in \mathrm{Syl}_p(G)$ and $L_p := \mathrm{Fix}(P) \leq L$. According to the fundamental theorem of Galois theory, p is not a divisor of $|G : P| = |L_p : K| = \dim(L_p)$. According to Lemma III.7.38, L_p is not a splitting field of D. In particular, $[A_{L_p}] \neq 1$. On the other hand,

$$L \otimes_{L_p} A_{L_p} = L \otimes_{L_p} L_p \otimes_K A \cong L \otimes_K A \cong A_L,$$

i. e. $A_{L_p} \in \mathrm{Br}(L|L_p) \cong H^2(P, L^\times)$, because $\mathrm{Gal}(L|L_p) = P$. According to Theorem III.7.43, $|\langle [A_{L_p}]\rangle|$ is a divisor of $|P|$ and thus a non-trivial p-power. According to Theorem III.7.32, p must also divide $|\langle [A]\rangle|$. □

Remark III.7.58.

(i) For every central simple algebra A over a number field, $e(A) = |\langle A\rangle|$ holds (without proof).

(ii) Our next goal is a connection to the Schur indices defined in Definition II.14.61.

Lemma III.7.59. *Let $K \subseteq L$ be a field extension. Let V be a finite-dimensional KG-module and V_L the corresponding LG-module. Then*

$$\dim_K \mathrm{End}_{KG}(V) = \dim_L \mathrm{End}_{LG}(V_L).$$

Proof. Let $\Delta\colon G \to \mathrm{GL}(n, K) \subseteq \mathrm{GL}(n, L)$ be the representation belonging to V or V_L, respectively. According to the proof of Theorem II.14.47, $\mathrm{End}_{KG}(V) \cong \mathrm{C}_{K^{n\times n}}(\Delta(G))$ holds. Let $\Delta(g) = (\gamma_{ij}(g))_{i,j}$ for $g \in G$. Then

$$\begin{aligned} A = (a_{ij}) \in \mathrm{C}_{K^{n\times n}}(\Delta(G)) &\iff \forall g \in G : A\Delta(g) = \Delta(g)A \\ &\iff \forall g \in G\, \forall 1 \leq i, j \leq n : \sum_{k=1}^{n} a_{ik}\gamma_{kj}(g) = \sum_{k=1}^{n} \gamma_{ik}(g)a_{kj}. \end{aligned}$$

Consequently, $\mathrm{C}_{K^{n\times n}}(\Delta(G))$ is the solution space of a homogeneous system of equations in n^2 variables, whose coefficient matrix $M \in K^{n^2|G|\times n^2}$ is formed from the $\gamma_{ij}(g)$. As is well known, the dimension of this space depends only on the rank of M. The rank of M, in turn, does not change if one considers M as a matrix over L. The assertion follows from this. □

Theorem III.7.60. *Let $\chi \in \mathrm{Irr}(G)$ with values in a number field K. Let Δ be an irreducible K-representation with character $m_K(\chi)\chi$. Then $A := \Delta(KG)$ is a central simple K-algebra with $e(A) = m_K(\chi)$.*

Proof. According to Artin-Wedderburn, A is a simple K-algebra. According to Theorem II.14.44 there exists a splitting field $L \supseteq K$ of G with $|L : K| < \infty$. Let $\Delta_L\colon G \to \mathrm{GL}(d, L)$ with $\Delta_L(g) = \Delta(g)$ for $g \in G$. Let $\Gamma\colon G \to \mathrm{GL}(e, L)$ be an L-representation with character χ. By assumption $d = em$ with $m := m_K(\chi)$. With a suitable choice of basis, $\Delta(g) = \mathrm{diag}(\Gamma(g), \ldots, \Gamma(g))$ holds for all $g \in G$. Let $z \in KG$ with $\Delta(z) \in \mathrm{Z}(A)$. According to Theorem II.14.47, $\Gamma(z) \in \mathrm{C}_{L^{e\times e}}(\Gamma(G)) = L1_e$ holds. Therefore there exists an $\alpha \in L$ with $\Delta(z) = \alpha 1_d$. Because of $\alpha d = \mathrm{tr}\,\Delta(z) = m\chi(z) \in K$, it follows that $\alpha \in K$ and $\mathrm{Z}(A) \cong K$. This shows that A is a central-simple K-algebra.

Let V, V_L and W be the simple modules corresponding to Δ, Δ_L and Γ. Then A is a matrix algebra over the division algebra $E := \mathrm{End}_{KG}(V)^o$. Furthermore, $\mathrm{End}_{LG}(W) \cong \mathrm{C}_{L^{e\times e}}(\Gamma(G)) \cong L$ according to

Theorem II.14.47. According to Lemma II.7.20, $\operatorname{End}_{LG}(V_L) = \operatorname{End}_{LG}(W^m) \cong \operatorname{End}_{LG}(W)^{m\times m} \cong L^{m\times m}$ holds. With Lemma III.7.59 it follows that

$$e(A) = e(E) = \sqrt{\dim_K E} = \sqrt{\dim_L \operatorname{End}_{LG}(V_L)} = m. \qquad \square$$

Lemma III.7.61. *Let D_1 and D_2 be central division algebras with coprime degrees (or dimensions). Then $D_1 \otimes D_2$ is a division algebra.*

Proof. Let $D_1 \otimes D_2 \cong D^{n\times n}$ for a division algebra D. Let $D_1^o \otimes D_1 \cong K^{k\times k}$ (note $[D_1]^{-1} = [D_1^o]$). Then $k^2 = \dim(D_1^o \otimes D_1) = \dim(D_1)^2$ and $k = \dim(D_1)$ holds. On the other hand,

$$\begin{aligned} D_2^{k\times k} &\cong (K \otimes D_2)^{k\times k} \overset{\text{III.7.11}}{\cong} K^{k\times k} \otimes D_2 \cong D_1^o \otimes D_1 \otimes D_2 \\ &\cong D_1^o \otimes D^{n\times n} \cong (D_1^o \otimes D)^{n\times n} \cong (E^{l\times l})^{n\times n} \cong E^{nl\times nl} \end{aligned}$$

for another division algebra E. According to Artin-Wedderburn, $D_2 \cong E$ and $k = nl$. In particular, $n \mid k = \dim(D_1) = \deg(D_1)^2$. For reasons of symmetry, $n \mid \deg(D_2)^2$ also holds and the assumption yields $n = 1$, i. e. $D_1 \otimes D_2 \cong D$. $\square$

Theorem III.7.62. *Let D be a central division algebra with $\deg(D) = p_1^{a_1} \dots p_k^{a_k}$ (prime factorization). Then there exist, up to isomorphism, uniquely determined division algebras $D_1, \dots, D_k$ with $D \cong D_1 \otimes \dots \otimes D_k$ and $\deg(D_i) = p_i^{a_i}$ for $i = 1, \dots, k$.*

Proof. Let $\deg(D) = n_1 n_2$ with coprime $n_1, n_2 > 1$. We show that there exist uniquely determined division algebras D_1 and D_2 up to isomorphism with $D \cong D_1 \otimes D_2$ and $\deg(D_i) = n_i$ for $i = 1, 2$. The claim then follows by induction on k. Let $a, b \in \mathbb{Z}$ with $an_1 + bn_2 = \gcd(n_1, n_2) = 1$. Let D_1 and D_2 be the uniquely determined division algebras with $[D]^{bn_2} = [D_1]$ and $[D]^{an_1} = [D_2]$. Then $[D_1 \otimes D_2] = [D]^{an_1 + bn_2} = [D]$ and

$$[D_1]^{n_1} = [D]^{b \deg(D)} = [D]^{be(D)} = 1$$

according to Theorem III.7.56. According to Lemma III.7.57, every prime divisor of $\deg(D_1)$ is a divisor of n_1. The same applies analogously to D_2. From the assumption, it follows that $\gcd(\deg(D_1), \deg(D_2)) = 1$. Now $D_1 \otimes D_2$ is a division algebra according to Lemma III.7.61. This shows $D \cong D_1 \otimes D_2$. Because of $n_1 n_2 = \deg(D) = \deg(D_1 \otimes D_2) = \deg(D_1)\deg(D_2)$, it holds that $\deg(D_i) = n_i$ for $i = 1, 2$. $\square$

Remark III.7.63. With the help of Theorem III.7.62, one can refine the Artin-Wedderburn decomposition.

III.8 Path algebras

Remark III.8.1. Using graph-theoretic methods, we construct so-called path algebras, which are generally infinite-dimensional. We show that every finite-dimensional algebra is Morita equivalent to a factor algebra of a path algebra. Let K always be a field.

Definition III.8.2.

(i) A *quiver* Q is a directed multigraph, i. e. there exist

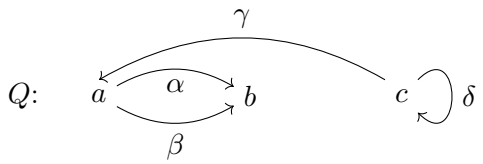
- a finite non-empty set Q_0 of *vertices*,
- a finite set Q_1 of *arrows*,
- maps $s, t\colon Q_1 \to Q_0$, which assign to each arrow $\alpha \in Q_1$ a *source* $s(\alpha)$ and a *target* $t(\alpha)$. We then also write $\alpha\colon s(\alpha) \to t(\alpha)$.

In the case $s(\alpha) = t(\alpha)$, α is called a *loop*.

(ii) A *subquiver* of Q is a quadruple $Q' = (Q'_0, Q'_1, s', t')$ with $Q'_0 \subseteq Q_0$, $Q'_1 \subseteq Q_1$, $s' = s_{|Q'_1}$ and $t' = t_{|Q'_1}$. Q' is called *full* if Q'_1 contains all arrows from Q_1 with source and target in Q'_0. In this case, Q' is uniquely determined by Q'_0.

(iii) A *path* from $a \in Q_0$ to $b \in Q_0$ of *length* n is a sequence of arrows $\rho = (\alpha_1, \ldots, \alpha_n) \in Q_1^n$ with $s(\alpha_1) = a$, $t(\alpha_n) = b$ and $s(\alpha_i) = t(\alpha_{i-1})$ for $i = 2, \ldots, n$. In the case $a = b$ and $n \geq 1$, ρ is called a *cycle*. For each $q \in Q_0$, we additionally define the path ϵ_q of length 0 from q to q.

Example III.8.3. We will represent quivers by graphs. For example



$$Q_0 = \{a, b, c\}, \qquad Q_1 = \{\alpha, \beta, \gamma, \delta\},$$
$$s(\alpha) = s(\beta) = t(\gamma) = a, \qquad t(\alpha) = t(\beta) = b, \qquad t(\gamma) = s(\delta) = t(\delta) = c.$$

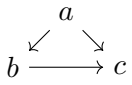
Definition III.8.4. Let K be a field, Q a quiver and P the set of all paths of Q of length ≥ 0. Let KQ be the K-vector space with basis P. For paths $(\alpha_1, \ldots, \alpha_m)$, $(\beta_1, \ldots, \beta_n)$ we define

$$(\alpha_1, \ldots, \alpha_m) \cdot (\beta_1, \ldots, \beta_n) = \begin{cases} (\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n) & \text{if } t(\alpha_m) = s(\beta_1), \\ 0 & \text{otherwise.} \end{cases}$$

We extend this multiplication linearly to KQ. It is easy to show that KQ in this way is a K-algebra with identity element $\sum_{q \in Q_0} \epsilon_q$. KQ is called the *path algebra* of Q over K.

Remark III.8.5.

(i) KQ is finite-dimensional if and only if Q has no cycles (in particular no loops). The corresponding undirected graph can nevertheless have cycles. For example, the path algebra of



has dimension 7.

(ii) We will often identify Q_0 with $\{\epsilon_q : q \in Q_0\} \subseteq KQ$. For $k \geq 2$ let Q_k be the set of paths of length k in Q. Then $KQ = \bigoplus_{k=0}^{\infty} KQ_k$ and $KQ_k \cdot KQ_l \subseteq KQ_{k+l}$ holds. Such a decomposition is called a *grading* of KQ. Furthermore, one calls

$$R(KQ) := \bigoplus_{k=1}^{n} KQ_k \trianglelefteq KQ$$

the *arrow ideal* of KQ.

Example III.8.6.

(i) For a quiver Q without arrows, $KQ = \bigoplus_{q \in Q_0} K\epsilon_q \cong K^{|Q_0|}$ holds.

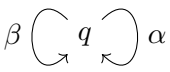
(ii) For $Q = (\{q\}, \{\alpha\}, s, t)$ with $\alpha \colon q \to q$, $KQ \cong K[X]$ by identifying α with X.

(iii) The quiver $Q = (\{a, b\}, \{\alpha\}, s, t)$ with $\alpha \colon a \to b$ possesses exactly three paths: ϵ_a, ϵ_b and α. Therefore, $\dim KQ = 3$. Because of $\epsilon_a \alpha = \alpha \neq 0 = \alpha \epsilon_a$, KQ is not commutative. It is easy to show that the map

$$\Gamma \colon KQ \to \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} : x, y, z \in K \right\} \subseteq K^{2\times 2}$$

with $\Gamma(\epsilon_a) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\Gamma(\epsilon_b) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\Gamma(\alpha) = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ is an isomorphism of algebras.

(iv) For



KQ is the *free* algebra of rank 2, i. e. no cancellation rules hold for the two generators α and β. The paths of Q are the *words* of the form $\alpha^{a_1}\beta^{a_2}\alpha^{a_3}\ldots$ or $\beta^{a_1}\alpha^{a_2}\beta^{a_3}\ldots$ with $a_1, a_2, \ldots \in \mathbb{N}$.

Theorem III.8.7. *Let K be a field and Q a quiver with vertices $q_1, \ldots, q_n$. Then $1 = \epsilon_{q_1} + \ldots + \epsilon_{q_n}$ is a decomposition into pairwise orthogonal primitive idempotents.*

Proof. It is clear that $\epsilon_{q_1}, \ldots, \epsilon_{q_n}$ are pairwise orthogonal idempotents. To show that they are primitive, we examine whether $P_i := KQ\epsilon_{q_i}$ is indecomposable (Lemma II.8.21). According to Remark II.12.12, it suffices to show that $E := \epsilon_{q_i} KQ \epsilon_{q_i} \cong \mathrm{End}_{KQ}(P_i)$ is local. For this, let $\epsilon \in E$ be an idempotent. Then $\epsilon = \lambda\epsilon_{q_i} + \alpha$ holds, where α is a linear combination of cycles of length ≥ 1 through q_i. Now

$$0 = \epsilon^2 - \epsilon = (\lambda^2 - \lambda)\epsilon_{q_i} + (2\lambda - 1)\alpha + \alpha^2$$

holds. Since the summands (cycles) of α^2 are longer than the summands of α, it follows that $\alpha = 0$ and $\lambda \in \{0, 1\}$. Thus E is local according to Theorem II.12.11. □

Remark III.8.8. Let Q be a quiver without cycles. According to Remark III.8.5 and Theorem II.12.16, KQ possesses at most $|Q_0|$ simple modules up to isomorphism. For the arrow ideal, $R(KQ)^k \subseteq \bigoplus_{l\geq 0} KQ_{k+l}$ holds. Therefore, $R(KQ)$ is nilpotent and $KQ/R(KQ) \cong K^{|Q_0|}$ is semisimple with exactly $|Q_0|$ non-isomorphic simple modules. This shows $\mathrm{J}(KQ) = R(KQ)$ and KQ is a basic algebra.

Definition III.8.9.

(i) Let α be an arrow of a quiver Q. We define the *inverse* arrow α^{-1} by $s(\alpha^{-1}) = t(\alpha)$ and $t(\alpha^{-1}) = s(\alpha)$ (we do not require that α^{-1} lies in Q_1). A *path* from $a \in Q_0$ to $b \in Q_0$ of *length* $l \geq 0$ is a sequence $(\alpha_1^{e_1}, \ldots, \alpha_l^{e_l})$ with $\alpha_1, \ldots, \alpha_l \in Q_1$, $e_1, \ldots, e_l \in \{\pm 1\}$, $s(\alpha_1^{e_1}) = a$, $t(\alpha_l^{e_l}) = b$ and $s(\alpha_i^{e_i}) = t(\alpha_{i-1}^{e_{i-1}})$ for $i = 2, \ldots, l$.

(ii) Vertices a and b are called *adjacent*, if a path of length 1 ((inverse) arrow) from a to b exists. Vertices $a, b \in Q_0$ are called *connected*, if an arbitrary path from a to b exists. This defines an equivalence relation on Q_0. The equivalence classes are called *components* of Q. Each component of Q induces a full subquiver. If Q has only one component, then Q is called *connected*.

Theorem III.8.10. *Let $A_1, \ldots, A_k$ be the components of a quiver Q. Let $\epsilon_i := \sum_{q\in A_i} \epsilon_q$ for $i = 1, \ldots, k$. Then $\epsilon_1, \ldots, \epsilon_k$ are the central-primitive idempotents of KQ. Furthermore, the block $KQ\epsilon_i$ is isomorphic to the path algebra over the full subquiver generated by A_i.*

Proof. Let $\alpha \in Q_1$. Then $s(\alpha)$ and $t(\alpha)$ lie in the same component of Q. Therefore, it holds that

$$\alpha\epsilon_i = \epsilon_i\alpha = \begin{cases} \alpha & \text{if } s(\alpha), t(\alpha) \in A_i, \\ 0 & \text{otherwise} \end{cases}$$

for $1 \leq i \leq k$. Thus $\epsilon_1, \ldots, \epsilon_k$ are central idempotents.

Conversely, let $z = z_0 + \ldots + z_n \in \mathrm{Z}(KQ)$ be an idempotent, where z_i is a linear combination of paths of length i (Remark III.8.5). Assume $n \geq 1$ and $z_n \neq 0$. Let $m \geq 1$ be minimal with $z_m \neq 0$. Then

$$z_0 + \ldots + z_n = z = z^2 = z_0^2 + z_0z_m + z_mz_0 + z_m^2 + \ldots + z_n^2$$

and it follows that $z_0^2 = z_0$ and $z_m = z_0z_m + z_mz_0$. Since z is central, it also holds that

$$z_0^2 + z_0z_m + \ldots + z_0z_n = z_0z = zz_0 = z_0^2 + z_mz_0 + \ldots + z_nz_0.$$

This shows $z_0z_m = z_mz_0$ and $z_m = 2z_0z_m$. Multiplication by z_0 yields $z_0z_m = 2z_0^2z_m = 2z_0z_m = 0$ and $z_m = 0$. Contradiction. Therefore $z = z_0 = \sum_{q\in Q_0} \lambda_q\epsilon_q$ with $\lambda_q \in K$. From $z^2 = z$ it follows easily that $\lambda_q \in \{0, 1\}$ for all $q \in Q_0$. Wlog. let $\lambda_q = 1$ for some $q \in A_1$. Suppose there is an arrow $\alpha \in Q_1$ from q to $q' \in A_1$. From $\alpha z = z\alpha = \alpha$ it follows that $\lambda_{q'} = 1$. If, on the other hand, there exists an arrow $\alpha' \in Q_1$ from q' to q, then $\lambda_{q'} = 1$ follows from $z\alpha = \alpha z = \alpha$. Therefore $\lambda_{q'} = 1$ for all neighbors q' of q. By induction, it follows that $\lambda_q = 1$ for all $q \in A_1$. Thus z is a sum of certain ϵ_i and $\epsilon_1, \ldots, \epsilon_k$ are the central-primitive idempotents of KQ. It is clear that $KQ\epsilon_i$ is generated by the paths between vertices in A_i. From this, the last statement follows. □

Theorem III.8.11 (Universal property)**.** *Let $Q = (Q_0, Q_1, s, t)$ be a quiver and A a K-algebra. Let $\varphi_0 \colon Q_0 \to A$ and $\varphi_1 \colon Q_1 \to A$ be maps with the following properties:*

(i) $\sum_{q\in Q_0} \varphi_0(q) = 1$, $\varphi_0(a)^2 = \varphi_0(a)$ and $\varphi_0(a)\varphi_0(b) = 0$ for all $a, b \in Q_0$ with $a \neq b$.

(ii) For all $\alpha \in Q_1$ it holds that $\varphi_1(\alpha) = \varphi_0(s(\alpha))\varphi_1(\alpha)\varphi_0(t(\alpha))$.

Then there exists exactly one algebra homomorphism $\Phi\colon KQ \to A$ *with* $\Phi(\epsilon_q) = \varphi_0(q)$ *for* $q \in Q_0$ *and* $\Phi(\alpha) = \varphi_1(\alpha)$ *for* $\alpha \in Q_1$.

Proof. For every path $\alpha = (\alpha_1, \ldots, \alpha_n)$ in Q we define

$$\Phi(\alpha) := \varphi_1(\alpha_1) \ldots \varphi_1(\alpha_n)$$

(for $n = 0$, $\Phi(\epsilon_q) = \varphi_0(q)$ is already given). Then Φ extends to a K-linear map $KQ \to A$. In this case, it holds that

$$\begin{aligned}
\Phi(1) &= \sum_{q \in Q_0} \Phi(\epsilon_q) = \sum_{q \in Q_0} \varphi_0(q) = 1, \\
\Phi(\alpha)\Phi(\epsilon_q) &= \varphi_1(\alpha_1) \ldots \varphi_0(s(\alpha_n))\varphi_1(\alpha_n)\varphi_0(t(\alpha_n))\varphi_0(q) \\
&= \begin{cases} \varphi_1(\alpha_1) \ldots \varphi_0(s(\alpha_n))\varphi_1(\alpha_n)\varphi_0(t(\alpha_n)) = \Phi(\alpha) = \Phi(\alpha\epsilon_q) & \text{if } q = t(\alpha_n) \\ 0 & \text{if } q \neq t(\alpha_n), \end{cases} \\
\Phi(\epsilon_q)\Phi(\alpha) &= \ldots = \begin{cases} \Phi(\epsilon_q\alpha) & \text{if } q = s(\alpha_1), \\ 0 & \text{if } q \neq s(\alpha_1). \end{cases}
\end{aligned}$$

Let $\beta = (\beta_1, \ldots, \beta_m)$ be another path. In the case $t(\alpha_n) = s(\beta_1)$, it holds that

$$\Phi(\alpha)\Phi(\beta) = \varphi_1(\alpha_1) \ldots \varphi_1(\alpha_n)\varphi_1(\beta_1) \ldots \varphi_1(\beta_m) = \Phi(\alpha\beta).$$

In the case $t(\alpha_n) \neq s(\beta_1)$, it holds that

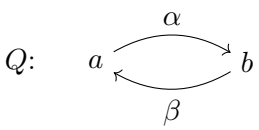
$$\varphi_1(\alpha_n)\varphi_1(\beta_1) = \varphi_0(s(\alpha_n))\varphi_1(\alpha_n) \underbrace{\varphi_0(t(\alpha_n))\varphi_0(s(\beta_1))}_{=0} \varphi_1(\beta_1)\varphi_0(t(\beta_1)) = 0$$

and $\Phi(\alpha)\Phi(\beta) = 0 = \Phi(0) = \Phi(\alpha\beta)$. This shows that Φ is a homomorphism of algebras. Let $\Phi'\colon KQ \to A$ be another homomorphism with the same properties. Then it holds that

$$\Phi'(\alpha) = \Phi'(\alpha_1) \ldots \Phi'(\alpha_n) = \varphi_1(\alpha_1) \ldots \varphi_1(\alpha_n) = \Phi(\alpha).$$

Thus $\Phi' = \Phi$. □

Example III.8.12. Let $A = K^{2\times 2}$ and

Q: 

Let, as usual, $E_{st} = (\delta_{is}\delta_{jt})_{i,j} \in A$. Let $\varphi_0(a) = E_{11}$, $\varphi_0(b) = E_{22}$, $\varphi_1(\alpha) = E_{12}$ and $\varphi_1(\beta) = E_{21}$. It is easy to check that the assumptions of Theorem III.8.11 are satisfied. Therefore, there exists an epimorphism $\Phi\colon KQ \to A$ with kernel $(\alpha\beta - \epsilon_a, \beta\alpha - \epsilon_b) \trianglelefteq KQ$.

Definition III.8.13. Let KQ be a path algebra. An ideal $I \trianglelefteq KQ$ is called *admissible*, if there exists an $m \geq 2$ with $R(KQ)^m \subseteq I \subseteq R(KQ)^2$.

Remark III.8.14. Let $I \trianglelefteq KQ$ be admissible with $R(KQ)^m \subseteq I$. Then all paths of length $\geq m$ vanish in KQ/I. Therefore KQ/I is finite-dimensional. If Q has no cycles, then $R(KQ)^m = 0$ for some m and every ideal in $R(KQ)^2$ is admissible. In particular, 0 is then also admissible. Arbitrary quotient algebras of path algebras can have worse properties as the following example illustrates.

Example III.8.15 (Dieudonné)**.** Let

$$Q: \qquad \alpha \circlearrowleft q \circlearrowright \beta$$

be as in Example III.8.6 and $I := (\alpha^2, \beta\alpha) \trianglelefteq KQ$. Because of $\beta^m \notin I$ for all $m \geq 1$, I is *not* admissible. Let $A := KQ/I$ and

$$J := K\{\alpha\beta^m + I : m \in \mathbb{N}\} \subseteq A.$$

Because of $\alpha(\alpha\beta^m) \in I$ and $\beta(\alpha\beta^m) \in I$, $J \trianglelefteq A$. Every generating system of J as an A-module also spans J as a K-vector space. Because of $\dim J = \infty$, J is not finitely generated. Therefore, A is not Noetherian.

Lemma III.8.16. *Let Q be a quiver and $I \trianglelefteq KQ$ be admissible. Then $\{\epsilon_q + I : q \in Q_0\}$ are pairwise orthogonal primitive idempotents in $A := KQ/I$.*

Proof. Let $R(KQ)^m \subseteq I$. Because of $I \subseteq R(KQ)^2$, $\overline{\epsilon_q} := \epsilon_q + I$ are non-zero pairwise orthogonal idempotents in KQ/I. As in the proof of Theorem III.8.7, it suffices to show that $E := \overline{\epsilon_q} A \overline{\epsilon_q}$ is local. Let $\bar{\epsilon} = \lambda\epsilon_q + \alpha + I \in E$ be an idempotent, where α is a linear combination of cycles of length ≥ 1 through q. From $\bar{\epsilon}^2 = \bar{\epsilon}$ it follows that

$$(\lambda^2 - \lambda)\epsilon_q + (2\lambda - 1)\alpha + \alpha^2 \in I \subseteq R(KQ)^2.$$

This shows $\lambda^2 = \lambda \in \{0, 1\}$. In the case $\lambda = 0$, $\alpha^2 \equiv \alpha \pmod{I}$. On the other hand, $\alpha^m \in R(KQ)^m \subseteq I$. This shows $\bar{\epsilon} = 0$. Now let $\lambda = 1$. Then $\alpha^2 \equiv -\alpha \pmod{I}$. As before, it follows that $\alpha \in I$ and $\bar{\epsilon} = \overline{\epsilon_q}$. Thus $\overline{\epsilon_q}$ is primitive. □

Theorem III.8.17. *Let Q be a quiver and $I \subseteq KQ$ be admissible. KQ/I is a block algebra if and only if Q is connected.*

Proof. Assume that Q has a component $A \neq Q_0$. According to Theorem III.8.10, $\bar{\epsilon} := \sum_{q \in A} \epsilon_q + I$ is a central idempotent in KQ/I. According to Lemma III.8.16, $0 \neq \bar{\epsilon} \neq 1$. Therefore, KQ/I is not a block algebra.

Conversely, let $\bar{z} \in \mathrm{Z}(KQ/I)$ be an idempotent. Then $\bar{z}$ can be decomposed into primitive idempotents. According to Theorem II.8.22 and Lemma III.8.16, we can assume $\bar{z} = \sum_{q \in A} \epsilon_q + I$ for a subset $A \subseteq Q_0$. As in the proof of Theorem III.8.10, one shows that A is a union of components of Q. Thus KQ/I is a block algebra if Q is connected. □

Remark III.8.18. In the following, we construct special generators for admissible ideals.

Definition III.8.19. Let Q be a quiver. A *relation* in KQ is a linear combination of paths $r = \sum_{i=1}^{n} \lambda_i \alpha_i$ with $\lambda_i \in K$, $\alpha_i \in R(KQ)^2$, $s(\alpha_i) = s(\alpha_j)$ and $t(\alpha_i) = t(\alpha_j)$ for all i, j.

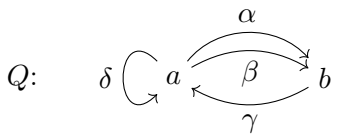
Theorem III.8.20. *Let Q be a quiver. Every admissible ideal of KQ can be generated as a KQ-module by finitely many relations.*

Proof. Let $I \trianglelefteq KQ$ be admissible, $R := R(KQ)$ and $R^m \subseteq I$. Since R^m is generated by all paths of length m and $I/R^m \subseteq KQ/R^m$ is finite-dimensional, I is finitely generated, say $I = (x_1, \ldots, x_n) \subseteq R^2$. For $a, b \in Q_0$ and $1 \leq i \leq n$ we have $\epsilon_a x_i \epsilon_b \in I$, since I is an ideal. Because of

$$x_i = 1x_i1 = \sum_{a,b \in Q_0} \epsilon_a x_i \epsilon_b$$

I is also generated by $\{\epsilon_a x_i \epsilon_b : a, b \in Q_0, 1 \leq i \leq n\}$. These are clearly (finitely many) relations. □

Example III.8.21. Let

Q: 

and $I \trianglelefteq KQ$ be the ideal generated by the relations $\delta^2 - \alpha\gamma$, $\alpha\gamma + \beta\gamma$, δ^3. Let $\rho \in Q_5$. If ρ contains the subpath $\beta\gamma$, we can replace it by $-\alpha\gamma$ without changing the coset $\rho + I$. In the same way, we can replace $\alpha\gamma$ by δ^2. Now α or β can only appear at the end of ρ. Thus ρ must contain the subpath δ^3 ($\gamma\delta^2\alpha$ is too short). This shows $\rho \in I$ and $R(KQ)^5 \subseteq I \subseteq R(KQ)^2$. Thus I is admissible.

Lemma III.8.22. *Let Q be a quiver, $I \trianglelefteq KQ$ admissible and $A := KQ/I$. Then $\mathrm{J}(A) = R(KQ)/I$ and A is a basic algebra.*

Proof. Because of $R(KQ)^m \subseteq I$ for some $m \in \mathbb{N}$, $R(KQ)/I \trianglelefteq A$ is nilpotent and $R(KQ)/I \subseteq \mathrm{J}(A)$ by Lemma II.8.15. Since the semisimple algebra $A/(R(KQ)/I) \cong KQ/R(KQ) \cong K^{|Q_0|}$ has no non-trivial nilpotent ideals, $\mathrm{J}(A) \subseteq R(KQ)/I$ holds. This shows $\mathrm{J}(A) = R(KQ)/I$. The second assertion follows from Example II.12.22. □

Definition III.8.23. Let A be a finite-dimensional K-algebra and $1 = e_1 + \ldots + e_n$ a decomposition into pairwise orthogonal primitive idempotents. We define a quiver $Q(A) = (Q_0, Q_1, s, t)$ as follows:

- $Q_0 = \{q_1, \ldots, q_n\}$.
- For $1 \leq i, j \leq n$, Q_1 contains exactly $\dim_K(e_i \mathrm{J}(A) e_j / e_i \mathrm{J}(A)^2 e_j)$ arrows $q_i \to q_j$.

Remark III.8.24. If $1 = e_1 + \ldots + e_n = f_1 + \ldots + f_n$ are decompositions into pairwise orthogonal idempotents, then by Theorem II.8.22 there exists an $x \in A^\times$ with $f_i = x e_i x^{-1}$. Since the map $A \to A$, $a \mapsto xax^{-1}$ is an (inner) automorphism, $Q(A)$ does not depend on the choice of the decomposition $1 = e_1 + \ldots + e_n$.

Example III.8.25.

(i) A is semisimple if and only if $Q(A)$ has no arrows.

(ii) Let $A \subseteq K^{n\times n}$ be the algebra of upper triangular matrices from Example II.12.22. For the primitive idempotents $e_i := E_{ii}$, it holds that $e_i\mathrm{J}(A)^k e_j = KE_{ij}$ if $i+k \leq j$ and 0 otherwise. This shows:

$$Q(A)\colon \quad q_1 \longrightarrow q_2 \longrightarrow \cdots \longrightarrow q_n$$

Theorem III.8.26. *Let Q be a quiver and $I \trianglelefteq KQ$ be admissible. Then $Q(KQ/I) = Q$.*

Proof. Let $A := KQ/I$. By Lemma III.8.16, $1 = \sum_{q\in Q_0} \overline{\epsilon_q}$ is a decomposition into pairwise orthogonal primitive idempotents. We can therefore assume $Q(A)_0 := Q_0$. By Lemma III.8.22, it holds that $\mathrm{J}(A)/\mathrm{J}(A)^2 \cong R(KQ)/R(KQ)^2 \cong KQ_1$. For $a, b \in Q_0$, $\dim_K \overline{\epsilon_a}\mathrm{J}(A)\overline{\epsilon_b}/\overline{\epsilon_a}\mathrm{J}(A)^2)\overline{\epsilon_b}$ is therefore the number of arrows from a to b. This yields a bijection $Q_1 \to Q(A)_1$. □

Lemma III.8.27. *Let $Q(A)$ be the quiver of a finite-dimensional K-algebra A. For each arrow $\alpha\colon q_i \to q_j$ in $Q(A)_1$, let $x_\alpha \in e_i\mathrm{J}(A)e_j$ such that the elements $x_\alpha + e_i\mathrm{J}(A)^2e_j$ form a K-basis of $e_i\mathrm{J}(A)e_j/e_i\mathrm{J}(A)^2e_j$. Then every element in $e_i\mathrm{J}(A)e_j$ is a K-linear combination of elements of the form $x_{\alpha_1}\dots x_{\alpha_k}$, where $k \in \mathbb{N}$ and $(\alpha_1, \dots, \alpha_k)$ is a path from q_i to q_j.*

Proof. By definition, it holds that

$$\begin{aligned} e_i\mathrm{J}(A)e_j &= \sum_{\substack{\alpha\in Q(A)_1\\ q_i\to q_j}} Kx_\alpha + e_i\mathrm{J}(A)^2e_j, \\ e_i\mathrm{J}(A)^2e_j &= \sum_{k=1}^{n} e_i\mathrm{J}(A)e_k\mathrm{J}(A)e_j = \sum_{k=1}^{n}\Big(\sum_{\substack{\alpha\in Q(A)_1\\ q_i\to q_k}} Kx_\alpha + e_i\mathrm{J}(A)^2e_k\Big)\Big(\sum_{\substack{\alpha\in Q(A)_1\\ q_k\to q_j}} Kx_\alpha + e_k\mathrm{J}(A)^2e_j\Big) \\ &= \sum_{\substack{(\alpha_1,\alpha_2)\in Q(A)_2\\ q_i\to q_j}} Kx_{\alpha_1}x_{\alpha_2} + e_i\mathrm{J}(A)^3e_j. \end{aligned}$$

Inductively, one obtains corresponding linear combinations for $e_i\mathrm{J}(A)^k e_j$ with $k \in \mathbb{N}$. Since $\mathrm{J}(A)$ is nilpotent, there exists an $l \in \mathbb{N}$ with $e_i\mathrm{J}(A)e_j = \sum_{k=1}^{l} e_i\mathrm{J}(A)^k e_j$. □

Theorem III.8.28. *Let K be algebraically closed and A a finite-dimensional basic algebra over K. Then there exists a admissible ideal $I \trianglelefteq KQ(A)$ with $A \cong KQ(A)/I$.*

Proof. Let $Q := Q(A)$. For $\alpha \in Q_1$ we choose x_α as in Lemma III.8.27. Let $\varphi_0\colon Q_0 \to A$, $q_i \mapsto e_i$ and $\varphi_1\colon Q_1 \mapsto A$, $\alpha \mapsto x_\alpha$. By the universal property, there exists a homomorphism $\Phi\colon KQ \to A$ with $\Phi(\epsilon_{q_i}) = e_i$ for $i = 1, \dots, n$ and $\Phi(\alpha) = x_\alpha$ for $\alpha \in Q_1$. Since A is a basic algebra and K is algebraically closed, $A = \sum_{i=1}^{n} Ke_i + \mathrm{J}(A)$ holds. Because of $\mathrm{J}(A) = \sum_{i,j=1}^{n} e_i\mathrm{J}(A)e_j$, Φ is surjective according to Lemma III.8.27. Let $I := \mathrm{Ker}(\Phi) \trianglelefteq KQ$ and $R := R(KQ)$. Then $\Phi(R) \subseteq \mathrm{J}(A)$ holds. Since $\mathrm{J}(A)$ is nilpotent, $\Phi(R^l) \subseteq \mathrm{J}(A)^l = 0$ holds for some $l \geq 1$. This shows $R^l \subseteq I$. Every $x \in I$ has the form

$$x = \sum_{i=1}^{n} \lambda_i\epsilon_{q_i} + \sum_{\alpha\in Q_1} \mu_\alpha\alpha + y$$

with $\lambda_i, \mu_\alpha \in K$ and $y \in R^2$. From $\Phi(x) = 0$ it follows that

$$\sum_{i=1}^{n} \lambda_i e_i + \sum_{\alpha \in Q_1} \mu_\alpha x_\alpha + \Phi(y) = 0.$$

In particular, $\sum_{i=1}^{n} \lambda_i e_i \in \mathrm{J}(A)$. Since $e_1, \ldots, e_n$ form a basis of $A/\mathrm{J}(A)$, it follows that $\lambda_1 = \ldots = \lambda_n = 0$. Since the cosets of x_α form a basis of $\mathrm{J}(A)/\mathrm{J}(A)^2$, it must now also hold that $\mu_\alpha = 0$ for all $\alpha \in Q_1$. This shows $I \subseteq R^2$, i. e. I is admissible with $KQ/I \cong \Phi(KQ) = A$. □

Remark III.8.29. The admissible ideal I in Theorem III.8.28 is generally not uniquely determined.

Example III.8.30.

(i) For every semisimple basic algebra A, $KQ(A) \cong K^{\dim A} \cong A$ holds according to Example III.8.25 and Example II.12.22.

(ii) Let $A \subseteq K^{n \times n}$ be the algebra of upper triangular matrices as in Example III.8.25. Every path in $Q(A)$ is uniquely determined by its start and end. Therefore, $\dim KQ(A) = \binom{n+1}{2} = \dim A$ and $A \cong KQ(A)$.

(iii) Let

$$A := \left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} : a, b, c \in K \right\}.$$

Obviously $\mathrm{J}(A) = (E_{12}, E_{23})$, $\mathrm{J}(A) = (E_{13})$ and $A/\mathrm{J}(A) \cong K$. It follows:

$Q(A)$: $\alpha \circlearrowright q \circlearrowright \beta$

The epimorphism $\Phi\colon KQ(A) \to A$ maps wlog. α to E_{12} and β to E_{23}. Because of $E_{23}E_{12} = 0$, $I := \mathrm{Ker}(\Phi) = (\alpha^2, \beta^2, \beta\alpha)$ and $A \cong KQ(A)/I$ (dimension comparison).

(iv) Let A be a 3-dimensional basic algebra over an algebraically closed field K. Let $Q := Q(A)$. If Q has three vertices, then $A \cong KQ \cong K^3$. Now assume $Q_0 = \{a, b\}$. If there exists an arrow $\alpha\colon a \to b$ in Q_1, then $A \cong KQ$ is isomorphic to the algebra of upper 2×2 triangular matrices from (ii). Now assume that a loop $\alpha\colon a \to a$ exists in Q_1. Then Q is disconnected and A is not a block algebra. One easily sees $A \cong KQ/(\alpha^2) \cong K \times K[X]/(X^2)$. Finally, let $Q_0 = \{a\}$. If Q_1 has only one loop $\alpha\colon a \to a$, then $A \cong KQ/(\alpha^3) \cong K[X]/(X^3)$. If Q_1 has two loops $\alpha, \beta\colon a \to a$, then one obtains

$$A \cong KQ/(\alpha^2, \beta^2, \alpha\beta, \beta\alpha) \cong K[X, Y]/(X^2, Y^2, XY).$$

One easily shows that the five mentioned algebras are pairwise non-isomorphic.

Definition III.8.31.

- A *representation* Δ of a quiver Q assigns to each vertex $q \in Q_0$ a K-vector space $\Delta(q)$ and to each arrow $\alpha\colon a \to b$ a K-linear map $\Delta(\alpha)\colon \Delta(a) \to \Delta(b)$. If all $\Delta(q)$ are finite-dimensional, then Δ is called *finite-dimensional*.

- If $\alpha = (\alpha_1, \ldots, \alpha_n) \in Q_1^n$ is a path and Δ is a representation of Q, then one defines

$$\Delta(\alpha) := \Delta(\alpha_1) \circ \ldots \circ \Delta(\alpha_n) \colon \Delta(s(\alpha_1)) \to \Delta(t(\alpha_n)).$$

  For the path ϵ_q of length 0, let $\Delta(\epsilon_q) := \mathrm{id}_{\Delta(q)}$. This definition can be linearly extended to sums of paths with common start/end. Let $I = (\rho_1, \ldots, \rho_k) \trianglelefteq KQ$ be admissible with relations $\rho_1, \ldots, \rho_k$. One calls Δ *admissible* with respect to I if $\Delta(\rho_i) = 0$ holds for all $i = 1, \ldots, k$.

- A *morphism* between representations Δ and Γ of Q is a family of linear maps $F := \{f_q \colon \Delta(q) \to \Gamma(q) : q \in Q_0\}$ with $f_b \circ \Delta(\alpha) = \Gamma(\alpha) \circ f_a$ for all arrows $\alpha \colon a \to b$. We write $F \colon \Delta \to \Gamma$. It is easy to see that the class of all representations of Q with the corresponding morphisms forms a category, which we denote by $\mathbf{Rep}(Q)$. Restricting to admissible representations with respect to $I \trianglelefteq KQ$, one obtains the category $\mathbf{Rep}(Q, I)$. Restricting to finite-dimensional representations, one obtains the categories $\mathbf{rep}(Q)$ and $\mathbf{rep}(Q, I)$.

Theorem III.8.32. *Let Q be a quiver, $I \trianglelefteq KQ$ admissible and $A := KQ/I$. Then $\mathbf{Mod}_A \approx \mathbf{Rep}(Q, I)$ and $\mathbf{mod}_A \approx \mathbf{rep}(Q, I)$ hold.*

Proof. Let M be an A-right module. For $q \in Q_0$ let $\bar{\epsilon}_q := \epsilon_q + I \in A$ be the corresponding idempotent. We define the representation Δ of Q by $\Delta(q) := M\bar{\epsilon}_q$. If M is finitely generated, then Δ is finite-dimensional. For an arrow $\alpha \colon a \to b$ in Q_1 let $\Delta(\alpha)(x) := x(\alpha + I) = x\overline{\alpha}\bar{\epsilon}_b \in \Delta(b)$ for $x \in \Delta(a)$. Obviously $\Delta(\alpha)$ is K-linear. Let $\rho = \alpha_1 + \ldots + \alpha_n \in I$ be a relation with paths $\alpha_1, \ldots, \alpha_n \colon a \to b$. For $x \in \Delta(a)$ it holds that

$$\Delta(\rho)(x) = \Delta(\alpha_1)(x) + \ldots \Delta(\alpha_n)(x) = x\overline{\alpha_1} + \ldots + x\overline{\alpha_n} = \bar{\rho}x = 0.$$

This shows $\Phi(M) := \Delta \in \mathbf{Rep}(Q, I)$. Let $f \colon M \to N$ be a homomorphism of A-right modules. For $x \in M\bar{\epsilon}_q$ it holds that $f(x) = f(x\bar{\epsilon}_q) = f(x)\bar{\epsilon}_q \in N\bar{\epsilon}_q$. The restriction f_q of f to $M\bar{\epsilon}_q$ thus maps to $N\bar{\epsilon}_q$. We define $\Phi(f) \colon \Phi(M) \to \Phi(N)$ by $\Phi(f)_q := f_q$ for $q \in Q_0$. For every arrow $\alpha \colon a \to b$ and $x \in \Phi(M)(a)$ it holds that

$$\big(f_b \circ \Phi(M)(\alpha)\big)(x) = f_b(x\overline{\alpha}) = f(x)\overline{\alpha} = \Phi(N)(\alpha)(f(x)) = \big(\Phi(N)(\alpha) \circ f_a\big)(x).$$

Therefore $\Phi(f)$ is a morphism and $\Phi \colon \mathbf{Mod}_A \to \mathbf{Rep}(Q, I)$ is a functor.

Conversely, we now start with $\Delta \in \mathbf{Rep}(Q, I)$ and define the K-vector space $\Psi(\Delta) = \bigtimes_{q \in Q_0} \Delta(q)$. If Δ is finite-dimensional, then so is $\Psi(\Delta)$. For $x = (x_q)_{q \in Q_0} \in \Psi(\Delta)$ and a path $\alpha \colon a \to b$ let

$$x\alpha := \big(\delta_{q,b}\Delta(\alpha)(x_a)\big)_{q \in Q_0} \in \Psi(\Delta)$$

with the Kronecker delta $\delta_{q,b}$. One easily verifies that $\Psi(\Delta)$ becomes a KQ-right module. For a relation $\rho \in I$ we have $x\rho = 0$ because of $\Delta(\rho) = 0$. Thus $\Psi(\Delta)$ is an A-module. Let $F = (f_q) \colon \Delta \to \Gamma$ be a morphism between representations Δ and Γ. We define $\Psi(F) \colon \Psi(\Delta) \to \Psi(\Gamma)$ by $\Psi(F)(x) = (f_q(x_q))_{q \in Q_0}$ for $x = (x_q) \in \Psi(\Delta)$. Obviously $\Psi(F)$ is K-linear. For a path $\alpha \colon a \to b$ it holds that

$$\Psi(F)(x\alpha) = \big(\delta_{b,q} f_b(\Delta(\alpha)(x_a))\big)_q = \big(\delta_{b,q}\Gamma(\alpha) f_a(x_a)\big)_q = \Psi(F)(x)\alpha,$$

i. e. $\Psi(F)$ is A-linear. Overall $\Psi \colon \mathbf{Rep}(Q, I) \to \mathbf{Mod}_A$ is a functor.

For every A-module M there exists a canonical isomorphism

$$\Psi(\Phi(M)) = \bigtimes_{q \in Q_0} M\bar{\epsilon}_q \xrightarrow{\sigma} \bigoplus_{q \in Q} M\overline{\epsilon_q} = M1_A = M.$$

For every homomorphism $f\colon M \to N$ and $x \in M$ it then holds that

$$\Psi(\Phi(f))(x) = \Psi\big((f_q)_{q\in Q_0}\big)(x) = (f_q(x\bar{\epsilon}_q))_q \xrightarrow{\sigma} \sum_{q\in Q_0} f_q(x\bar{\epsilon}_q) = f(x).$$

This shows $\Psi \circ \Phi = \mathrm{id}$. For a representation Δ of Q let

$$\tilde{\Delta} := \Phi(\Psi(\Delta)) = \Phi\Big(\bigtimes_{q\in Q_0} \Delta(q)\Big).$$

For $a \in Q_0$ there exists a canonical isomorphism

$$\tilde{\Delta}(a) = \bigtimes_{q\in Q_0} \Delta(q)\bar{\epsilon}_a = \Big\{\big(\delta_{q,a}\Delta(\epsilon_a)(x_a)\big)_q : x_q \in \Delta(q)\Big\} = \big\{(\delta_{q,a}x_a)_q : x_a \in \Delta(a))\big\} \xrightarrow{\sigma_a} \Delta(a).$$

Let $F := (f_q)\colon \Delta \to \Gamma$ be a morphism, $f := \Psi(F)\colon \Psi(\Delta) \to \Psi(\Gamma)$ and $\tilde{F} := (\tilde{f}_q) = \Phi(f)\colon \tilde{\Delta} \to \tilde{\Gamma}$. Then $\tilde{f}_a$ is the "restriction" of f to $\tilde{\Delta}(a)$. For $x \in \Delta(a)$ it therefore holds that

$$\tilde{f}_a\big((\delta_{q,a}x)_q\big) = f((\delta_{q,a}x)_q) = \big(f_q(\delta_{q,a}x)\big)_q \xrightarrow{\sigma_a} f_a(x),$$

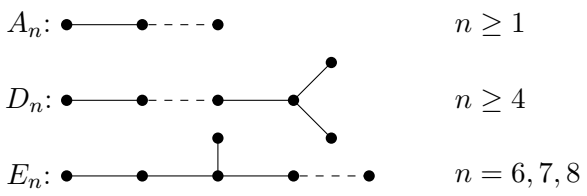
i. e. $\tilde{F}$ coincides with F modulo σ and $\Phi \circ \Psi = \mathrm{id}$. It follows that $\mathbf{Mod}_A \approx \mathbf{Rep}(Q, I)$. As already noted, finite-dimensional objects are preserved in both directions. This shows $\mathbf{mod}_A \approx \mathbf{rep}(Q, I)$. □

Corollary III.8.33. *For every quiver Q without cycles, $\mathbf{Rep}(Q) \approx \mathbf{Mod}_{KQ}$ and $\mathbf{rep}(Q) \approx \mathbf{mod}_{KQ}$ hold.*

Proof. Choose $I = 0$ in Theorem III.8.32. □

Example III.8.34. Let Q be a quiver and $q \in Q_0$. We define the representation Δ_q of Q by $\Delta_q(a) := \delta_{q,a}K$ and $\Delta_q(\alpha) = 0$ for $a \in Q_0$ and $\alpha \in Q_1$. Obviously, Δ_q is admissible with respect to every admissible ideal $I \subseteq R(KQ)^2$. Let $A := KQ/I$ be the corresponding basic algebra. Then Δ_q corresponds to a 1-dimensional A-module M_q. For $a \neq b$ in Q_0, there is obviously only the trivial morphism $\Delta_a \to \Delta_b$. Therefore, there is also only the trivial homomorphism between M_a and M_b. According to Lemma III.8.16, $\{M_q : q \in Q_0\}$ is a system of representatives for the simple A-modules.

Remark III.8.35. In Remark III.3.15, we introduced algebras of finite representation type. Let Q be a connected quiver without cycles. Gabriel has shown that KQ has finite representation type if and only if the graph of Q is one of the following *Dynkin diagrams* (n is the number of vertices):



The number of isomorphism classes of indecomposable KQ-modules in the five cases is $\frac{n^2+n}{2}$, $n^2 - n$, 36, 63, and 120 (without proof).

III.9 Lie Algebras

Remark III.9.1. Lie algebras are ring-like structures with non-associative multiplication (thus they are not algebras in the conventional sense). They appear in many areas of mathematics and physics. Their study could be described as "higher" linear algebra. We will transfer earlier theorems (such as Artin-Wedderburn or Wedderburn-Malcev) to Lie algebras and identify some differences. Let K always be a field.

Definition III.9.2. A *Lie algebra* is a K-vector space V with a bilinear map $L \times L \to L$, $(x, y) \mapsto [x, y]$ (*Lie bracket*), such that for all $x, y, z \in L$ the following hold:

- $[x, x] = 0$ (*alternating*),
- $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ (*Jacobi identity*).

Remark III.9.3.

(i) Lie algebras are *not* algebras in the sense of Definition II.12.2, because the Lie bracket is generally not associative and there is no identity element.

(ii) In the following, we always consider finite-dimensional Lie algebras, unless stated otherwise.

(iii) Let L be a Lie algebra and $x, y \in L$. From

$$0 = [x + y, x + y] = [x, x] + [x, y] + [y, x] + [y, y] = [x, y] + [y, x]$$

follows the antisymmetry $[x, y] = -[y, x]$. If $\operatorname{char} K \neq 2$, then antisymmetric is equivalent to alternating (set $y = x$).

(iv) The Jacobi identity can also be written in the form

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$$

according to (iii).

(v) For $k \geq 2$ we define inductively $[x_1, \ldots, x_{k+1}] := [x_1, [x_2, \ldots, x_k]]$.[1]

Example III.9.4.

(i) Every K-vector space V becomes a Lie algebra by setting $[v, w] := 0$ for $v, w \in V$. Such Lie algebras are called *abelian*.

(ii) If $(L_i)_{i \in I}$ is a family of Lie algebras, then the direct product $L := \bigtimes_{i \in I} L_i$ is also a Lie algebra by defining $[(x_i)_i, (y_i)_i] := ([x_i, y_i])_i$ for $(x_i)_i, (y_i)_i \in L$.

[1] Many books define *left-normed* commutators $[x_1, \ldots, x_k] = [[x_1, \ldots, x_{k-1}], x_k]$.

(iii) Let A be a K-algebra. For $x, y \in A$ let $[x, y] := xy - yx$. Then

$$\begin{aligned}
[\lambda x + y, z] &= (\lambda x + y)z - z(\lambda x + y) \qquad (\lambda \in K) \\
&= \lambda(xz - zx) + yz - zy = \lambda[x, z] + [y, z], \\
[x, x] &= 0, \\
[x, y + z] &= -[y + z, x] = \ldots = [x, y] + [x, z], \\
[x, y, z] + [y, z, x] + [z, x, y] &= x(yz - zy) - (yz - zy)x + y(zx - xz) \\
&\quad - (zx - xz)y + z(xy - yx) - (xy - yx)z = 0.
\end{aligned}$$

In this way, A becomes a Lie algebra.

(iv) As a special case of (iii), one obtains the *general linear* Lie algebra $\mathfrak{gl}(n, K) := K^{n \times n}$ of degree n (Note: $\mathfrak{gl}(n, K)$ does not only consist of the matrices in $\mathrm{GL}(n, K)$). As usual, let $\mathfrak{gl}(n, q) := \mathfrak{gl}(n, \mathbb{F}_q)$ for prime powers $q \neq 1$. As is well known, the matrices $\{E_{ij} : 1 \leq i, j \leq n\}$ form a K-basis of $\mathfrak{gl}(n, K)$. It holds that

$$[E_{ij}, E_{kl}] = E_{ij}E_{kl} - E_{kl}E_{ij} = \delta_{jk}E_{il} - \delta_{il}E_{kj}.$$

For every vector space V, one defines more generally the Lie algebra $\mathfrak{gl}(V) = \mathrm{End}_K(V)$.

(v) Let $L = K^3$ and

$$[x, y] := \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \times \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_2y_3 - x_3y_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{pmatrix} \qquad (\textit{cross product})$$

for $x, y \in L$. Obviously, the cross product is bilinear and alternating. Furthermore, it holds that

$$\begin{aligned}
x \times (y \times z) &= \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \times \begin{pmatrix} y_2z_3 - y_3z_2 \\ y_3z_1 - y_1z_3 \\ y_1z_2 - y_2z_1 \end{pmatrix} = \begin{pmatrix} x_2(y_1z_2 - y_2z_1) - x_3(y_3z_1 - y_1z_3) \\ * \\ * \end{pmatrix} \\
&= \begin{pmatrix} (x_1z_1 + x_2z_2 + x_3z_3)y_1 - (x_1y_1 + x_2y_2 + x_3y_3)z_1 \\ * \\ * \end{pmatrix} = \langle x, z\rangle y - \langle x, y\rangle z,
\end{aligned}$$

where $\langle x, y\rangle$ denotes the standard inner product. From this follows the Jacobi identity

$$[x, y, z] + [y, z, x] + [z, x, y] = \langle x, z\rangle y - \langle x, y\rangle z + \langle y, x\rangle z - \langle y, z\rangle x + \langle z, y\rangle x - \langle z, x\rangle y = 0.$$

Thus L is a Lie algebra.

Definition III.9.5. Let L be a Lie algebra. A subspace $U \leq L$ is called

- (*Lie*) *subalgebra*, if $[x, y] \in U$ holds for all $x, y \in U$. Certainly U is then itself a Lie algebra.
- *ideal*, if $[x, u] \in U$ holds for all $x \in L$ and $u \in U$. We then write $U \trianglelefteq L$ as with rings.

Remark III.9.6.

(i) Because of $[x, y] = -[y, x]$, ideals I can also be characterized by the equivalent condition $[u, x] \in I$ for $u \in I$ and $x \in L$.

(ii) In contrast to the situation with rings, ideals of Lie algebras are also subalgebras.

(iii) If $I \trianglelefteq L$, then the vector space L/I becomes a Lie algebra via

$$[x+I, y+I] := [x,y] + I \qquad (x, y \in L)$$

since $[x+u, y] + I = [x,y] + [u,y] + I = [v,w] + I$ for $x, y \in L$ and $u \in I$ (well-definedness). L/I is called a *Lie quotient algebra*.

Example III.9.7. Let L be a Lie algebra.

(i) As usual, 0 and L are ideals (and thus Lie subalgebras) of L. If L possesses no further ideals and L is not abelian, then L is called *simple* (possibly $\dim L \geq 2$).

(ii) The *center* $\mathrm{Z}(L) := \{x \in L : \forall v \in L : [x,v] = 0\}$ is obviously an ideal and at the same time an abelian subalgebra. Every subspace of $\mathrm{Z}(L)$ is an ideal in L.

(iii) For $X \subseteq L$, let $\langle X \rangle$ be the intersection of all subalgebras of L that contain X. Then $\langle X \rangle$ is the Lie algebra *generated* by X. As a vector space, $\langle X \rangle$ is spanned by all iterated Lie brackets $[x_1, \ldots, x_n]$ with $x_1, \ldots, x_n \in X$. In the case $L = \langle X \rangle$, X is called a *generating set* of L.

(iv) For $I, J \trianglelefteq L$, $I+J$ and $I \cap J$ are also ideals. Furthermore, $[I,J] := \mathrm{Span}_K\{[x,y] : x \in I, y \in J\} \trianglelefteq L$, because for $x \in I$, $y \in J$ and $v \in L$ we have

$$[v,[x,y]] = -[x, \underbrace{[y,v]}_{\in J}] - [y, \underbrace{[v,x]}_{\in I}] \in [I,J].$$

In particular, the *commutator algebra* $L' := [L,L]$ is an ideal of L. Apparently, L' is the "smallest" ideal with an abelian factor algebra (cf. Exercise I.31).

(v) Let A be an ordinary algebra, which we regard as a Lie algebra via $[a,b] = ab - ba$. Then $A' = \gamma(A)$ is exactly the commutator space defined in Definition II.12.32.

(vi) Let $L := \mathfrak{gl}(n,K)$. Since the trace of matrices is linear,

$$\mathfrak{sl}(n,K) := \{a \in L : \mathrm{tr}(a) = 0\}$$

is a subspace of L. For $x, y \in L$ we have $\mathrm{tr}([x,y]) = \mathrm{tr}(xy) - \mathrm{tr}(yx) = 0$, i. e. $L' \leq \mathfrak{sl}(n,K) \trianglelefteq L$. One calls $\mathfrak{sl}(n,K)$ the *special linear* Lie algebra of degree n. The matrices E_{ij} with $i \neq j$ and $E_{11} - E_{ii}$ for $i = 2, \ldots, n$ form a basis of $\mathfrak{sl}(n,K)$. Because of $[E_{i1}, E_{1j}] = E_{ij}$ for $i \neq j$ and $[E_{1i}, E_{i1}] = E_{11} - E_{ii}$, we have $L' = \mathfrak{sl}(n,K)$. For $K = \mathbb{C}$, the map

$$\exp\colon \mathfrak{gl}(n,\mathbb{C}) \to \mathrm{GL}(n,\mathbb{C}), \qquad A \mapsto \sum_{k=0}^{\infty} \frac{A^k}{k!}$$

is well-known to be well-defined. One can furthermore show that exp is surjective (but not injective). Because of $\det(\exp(A)) = \exp(\mathrm{tr}(A))$, we have $\exp(\mathfrak{sl}(n,\mathbb{C})) = \mathrm{SL}(n,\mathbb{C})$.

(vii) The upper triangular matrices are known to form a ring and therefore a Lie subalgebra U of $L := \mathfrak{gl}(n,K)$. Because of $[E_{21}, E_{11}] = E_{21} \notin U$, U is not an ideal of L. On the other hand, the strict upper triangular matrices (with zeros on the main diagonal) form an ideal in U.

(viii) For $S \in K^{n \times n}$, let

$$L := \{A \in K^{n \times n} : A^{\mathrm{t}} S = -SA\}.$$

For $A, B \in L$ we have

$$[A,B]^{\mathrm{t}} S = (B^{\mathrm{t}} A^{\mathrm{t}} - A^{\mathrm{t}} B^{\mathrm{t}}) S = -B^{\mathrm{t}} SA + A^{\mathrm{t}} SB = S(BA - AB) = -S[A,B].$$

Therefore L is a Lie subalgebra of $\mathfrak{gl}(n,K)$. We will return to this in Example III.9.56.

Definition III.9.8. A K-linear map $f\colon L \to M$ between Lie algebras L and M is called a *homomorphism*, if $f([x,y]) = [f(x), f(y)]$ holds for all $x, y \in L$. As usual, one defines mono-, epi-, endo-, iso- and automorphisms of Lie algebras.

Remark III.9.9.

(i) As always, one shows that images and preimages of subalgebras under homomorphisms are mapped to subalgebras. Furthermore, the preimage of an ideal is always an ideal. In particular, kernels of homomorphisms are ideals. For a homomorphism $f\colon L \to M$, the homomorphism theorem $L/\mathrm{Ker}(f) \cong M$ holds. From this, the correspondence theorem and the isomorphism theorems $(U+I)/I \cong U/(U \cap I)$ and $L/J \cong (L/I)/(J/I)$ follow as usual for a subalgebra $U \subseteq L$ and ideals $I, J \trianglelefteq L$ with $J \subseteq I$.

(ii) For every bijective homomorphism $f\colon L \to M$, f^{-1} is also a homomorphism. The isomorphism of Lie algebras is thus an equivalence relation as usual.

(iii) Let $x_1, \ldots, x_n$ be a basis of the Lie algebra L. For $i < j$, let $\lambda_{ijk} \in K$ with $[x_i, x_j] = \sum_{k=1}^{n} \lambda_{jik} x_k$. Obviously, L is uniquely determined up to isomorphism by the *structure constants* λ_{ijk}.

(iv) If $L = I \oplus J$ is a direct sum of ideals, then $L \cong I \times J$ holds. However, if I and J are only subalgebras, this is false. Indeed, if $x_1, \ldots, x_n$ is a basis of L, then Kx_i are (abelian) subalgebras with $L = Kx_1 \oplus \ldots \oplus Kx_n$.

Example III.9.10. For a Lie algebra L, let $\mathrm{ad}\colon L \to \mathfrak{gl}(L)$, $x \mapsto \mathrm{ad}_x$ with $\mathrm{ad}_x(v) := [x, v]$ for $v \in L$. From the bilinearity of the Lie bracket, the well-definedness of ad follows (i. e. ad_x is K-linear for all $x \in L$) and the linearity of ad. For $x, y, z \in L$ holds

$$\begin{aligned}\mathrm{ad}_{[x,y]}(z) &= [[x,y],z] = -[[y,z],x] - [[z,x],y] = [x,[y,z]] - [y,[x,z]] \\ &= (\mathrm{ad}_x \circ \mathrm{ad}_y - \mathrm{ad}_y \circ \mathrm{ad}_x)(z) = [\mathrm{ad}_x, \mathrm{ad}_y](z).\end{aligned}$$

Therefore, ad is a homomorphism of Lie algebras with kernel $\mathrm{Z}(L)$. One calls ad the *adjoint* homomorphism.

Remark III.9.11. In the following, let V always be a finite-dimensional K-vector space. A linear map $f \in \mathfrak{gl}(V)$ is called (as is well known) *nilpotent*, if there exists a $k \in \mathbb{N}$ with $f^k = 0$.

Lemma III.9.12. *For $x \in \mathfrak{gl}(V)$ holds:*

(i) x nilpotent $\Longrightarrow \mathrm{ad}_x$ nilpotent

(ii) x diagonalizable $\Longrightarrow \mathrm{ad}(x)$ diagonalizable

Proof.

(i) Let $x^k = 0$. For $y \in \mathfrak{gl}(V)$, $\mathrm{ad}_x^{2k}(y) = [x, [x, \ldots, [x, y] \ldots]]$ is a sum of terms of the form $x^i y x^{2k-i} = 0$. Thus $\mathrm{ad}_x^{2k} = 0$.

(ii) Let $e_1, \ldots, e_n$ be a basis of V consisting of eigenvectors of x. Then the linear maps f_{ij} with $f_{ij}(e_k) = \delta_{ik} e_j$ form a basis of $\mathfrak{gl}(V)$. Let $x(e_i) = \lambda_i e_i$ for $i = 1, \ldots, n$ and eigenvalues $\lambda_i \in K$. It holds that

$$\mathrm{ad}_x(f_{ij})(e_k) = (xf_{ij} - f_{ij}x)(e_k) = \delta_{ik} x(e_j) - \lambda_k f_{ij}(e_k) = \delta_{ik}(\lambda_j - \lambda_k) e_j = 0$$

and $\mathrm{ad}_x(f_{ij}) = (\lambda_j - \lambda_i) f_{ij}$. Therefore the f_{ij} are eigenvectors of ad_x and ad_x is diagonalizable. □

Definition III.9.13. Let L be a Lie subalgebra of $\mathfrak{gl}(V)$. A linear map $\lambda\colon V \to K$ is called a *weight* of L if

$$V_\lambda := \{v \in V : \forall x \in L : x(v) = \lambda(v)v\} \neq 0.$$

Remark III.9.14. Obviously V_λ consists of common eigenvectors of all elements of L.

Example III.9.15. Let $L \subseteq \mathfrak{gl}(n, K)$ be the Lie algebra of upper triangular matrices. Then $\lambda\colon L \to K$, $(x_{ij}) \mapsto x_{11}$ is a weight and $V_\lambda = K(1, 0, \ldots, 0)$.

Lemma III.9.16 (Invariance Lemma)**.** *Let* $\operatorname{char} K = 0$*. Let* $I \trianglelefteq L \subseteq \mathfrak{gl}(V)$ *and* $\lambda\colon I \to K$ *be a weight of* I*. Then* $\lambda([L, I]) = 0$*. In particular,* λ *is a homomorphism of Lie algebras and* V_λ *is an* L*-invariant subspace of* V*, i. e.* $x(V_\lambda) \subseteq V_\lambda$ *for all* $x \in L$*.*

Proof. Let $x \in L$, $v \in V_\lambda \setminus \{0\}$ and $U := \operatorname{Span}\{x^i(v) : i \in \mathbb{N}_0\} \leq V$ with $d := \dim U$. Then $v, x(v), \ldots, x^{d-1}(v)$ is a basis of U. We show by induction that

$$a(x^i(v)) \in \lambda(a)x^i(v) + \sum_{j=0}^{i-1} Kx^j(v)$$

for all $a \in I$ and $i = 0, \ldots, d-1$. This is clear for $i = 0$. Let inductively $a(x^i(v)) = \lambda(a)x^i(v) + w$ and $[a, x]x^i(v) = \lambda([a, x])x^i(v) + w'$ with $w, w' \in \sum_{j=0}^{i-1} Kx^j(v)$. Then

$$a(x^{i+1}(v)) = (xa + [a, x])x^i(v) = x(\lambda(a)x^i(v) + w) + \lambda([a, x])x^i(v) + w' \in \lambda(a)x^{i+1}(v) + \sum_{j=0}^{i} Kx^j(v).$$

In particular, the matrix of the restriction $a_{|U}$ is an upper triangular matrix and $\operatorname{tr}(a_{|U}) = d\lambda(a)$.

We apply this argument with $b := [x, a] \in I$ instead of a. Because of $x(U) \subseteq U$, it holds that $d\lambda(b) = \operatorname{tr}(b_{|U}) = \operatorname{tr}([x_{|U}, a_{|U|}]) = 0$. From $\operatorname{char} K = 0$ it follows that $\lambda(b) = 0$ and $\lambda([L, I]) = 0$ as claimed. In particular, $\lambda(I') = 0 = K'$ and λ is a homomorphism of Lie algebras. Finally, it holds that

$$a(x(v)) = xa(v) + [a, x](v) = \lambda(a)x(v) + \lambda([a, x])(v) = \lambda(a)x(v)$$

and $x(v) \in V_\lambda$. This shows that V_λ is L-invariant. □

Corollary III.9.17. *Let* $\operatorname{char} K = 0$ *and* $x, y \in \mathfrak{gl}(n, K)$ *such that* $[x, y]$ *commutes with* x *and* y*. Then* $[x, y]$ *is nilpotent.*

Proof. Wlog. we can assume that K is algebraically closed. According to the Jordan normal form, it suffices to show that every eigenvalue λ of $[x, y]$ is equal to 0. Let $U := \{v \in V : [x, y](v) = \lambda v\} \leq V$ be the corresponding eigenspace. Because $[x, [x, y]] = 0 = [y, [x, y]]$, $L := \operatorname{Span}\{x, y, [x, y]\} \subseteq \mathfrak{gl}(V)$ is a Lie algebra with ideal $I := K[x, y]$. According to the Invariance Lemma, U is invariant under x and y. Therefore $0 = \operatorname{tr}([x_{|U}, y_{|U}]) = \operatorname{tr}([x, y]_{|U}) = \operatorname{tr}(\lambda \operatorname{id}_U) = \lambda \dim U$ and $\lambda = 0$. □

Lemma III.9.18. *Let* $V \neq 0$ *and* $L \subseteq \mathfrak{gl}(V)$ *be a Lie algebra consisting only of nilpotent elements. Then the trivial map* $\lambda\colon L \to K$*,* $x \mapsto 0$ *is a weight of* L*.*

Proof. Induction on $d := \dim L$. In the case $d = 0$, $V_\lambda = V \neq 0$ by assumption. Let $d > 0$ and I be a maximal Lie subalgebra of L. We show that I is an ideal with dimension $d-1$. Let $\overline{L} := L/I$ and $\overline{\mathrm{ad}}\colon I \to \mathfrak{gl}(\overline{L})$ with $\overline{\mathrm{ad}}_x(a+I) := [x,a]+I$ for $a \in L$. For $a, b \in L$ with $a+I = b+I$, we have $[x, a-b] \in I$ and $\overline{\mathrm{ad}}_x(a+I) = \overline{\mathrm{ad}}_x(b+I)$, i. e. $\overline{\mathrm{ad}}$ is well-defined. The same proof as for ad (Example III.9.10) shows that $\overline{\mathrm{ad}}$ is a homomorphism. From Lemma III.9.12 it follows that $\overline{\mathrm{ad}}(I)$ consists of nilpotent maps. Because $\dim \overline{\mathrm{ad}}(I) < d$, there exists an $a + I \in \overline{L}_\lambda \setminus \{0\}$, i. e. $[x, a] \in I$ for all $x \in I$. Now $I + Ka$ is also a subalgebra of L and the maximality of I shows $L = I + Ka$. This shows $I \trianglelefteq L$ and $\dim I = d - 1$.

We apply the induction hypothesis to I. Then

$$U := \{v \in V : \forall x \in I : x(v) = 0\} \neq 0.$$

For $x \in I$ and $u \in U$, we have $x(a(u)) = (ax + [x, a])(u) = 0$ and $a(u) \in U$. Like a, the restriction $a_{|U}$ is also nilpotent. In particular, there exists $u \in \mathrm{Ker}(a_{|U}) \setminus \{0\}$. Obviously $u \in V_\lambda$ and $V_\lambda \neq 0$. □

Definition III.9.19. Let L be a Lie algebra. We define $L^{(1)} := L'$ and $L^{(k)} := [L^{(k-1)}, L^{(k-1)}]$ for $k \geq 2$. Furthermore, let $L^{[1]} := L$ and $L^{[k]} := [L, L^{[k-1]}]$ for $k \geq 2$. We call L

- *solvable*, if there exists a $k \geq 1$ with $L^{(k)} = 0$.
- *nilpotent*, if there exists a $k \geq 1$ with $L^{[k]} = 0$.
- *semisimple*, if L has no non-trivial solvable ideals.

Lemma III.9.20. *A Lie algebra L is solvable if and only if there exists a sequence of subalgebras $0 = I_0 \trianglelefteq I_1 \trianglelefteq \ldots \trianglelefteq I_n = L$ such that I_k/I_{k-1} is abelian for $k = 1, \ldots, n$ (one does not require $I_i \trianglelefteq L$).*

Proof. If L is solvable, then the sequence $0 = L^{(n)} \trianglelefteq L^{(n-1)} \trianglelefteq \ldots \trianglelefteq L$ has the desired property. Conversely, let $0 = I_0 \trianglelefteq I_1 \trianglelefteq \ldots \trianglelefteq I_n = L$ be as specified. Since L/I_{n-1} is abelian, $L' \subseteq I_{n-1}$ holds. Let inductively $L^{(k)} \subseteq I_{n-k}$. Then $L^{(k+1)} = [L^{(k)}, L^{(k)}] \subseteq [I_{n-k}, I_{n-k}] \leq I_{n-k-1}$ holds. It follows that $L^{(n)} \subseteq I_0 = 0$ and L is solvable. □

Example III.9.21.

(i) Because of $L^{(k)} \subseteq L^{[k+1]}$, every nilpotent Lie algebra is solvable.

(ii) Let $N \subseteq \mathfrak{gl}(n, K)$ be the Lie algebra of strict upper triangular matrices (with zeros on the main diagonal). For the standard basis $e_1, \ldots, e_n$ of K^n and $x \in N$, $x(e_k) \in \sum_{i=1}^{k-1} Ke_i$ holds. One easily sees that every element of $N^{[k]}$ is a linear combination of products of the form $x_1 \ldots x_k$ with $x_1, \ldots, x_k \in N$. Because of $x_1 \ldots x_n(e_i) = 0$ for $i = 1, \ldots, n$ and all $x_1, \ldots, x_n \in N$, it follows that $N^{[n]} = 1$. Thus N is nilpotent.

(iii) Now let $S \subseteq \mathfrak{gl}(n, K)$ be the Lie algebra of all upper triangular matrices. One easily shows $S' \subseteq N$. Since N is nilpotent, S is solvable.

Remark III.9.22.

(i) Apparently $L^{[n]} = \mathrm{Span}\{[x_1, \ldots, x_n] : x_1, \ldots, x_n \in L\}$ holds for $n \geq 2$.

(ii) As in Theorem I.6.5, one shows that subalgebras and factor algebras of solvable (resp. nilpotent) Lie algebras are solvable (resp. nilpotent). Furthermore, a Lie algebra L with ideal I is solvable if and only if I and L/I are solvable.

(iii) If $A, B \trianglelefteq L$ are solvable, then $A + B$ is also solvable, because $(A + B)/A \cong B/(B \cap A)$. The sum $\mathrm{J}(L)$ of all solvable ideals of L is therefore the largest solvable ideal (note $\dim L < \infty$). One calls $\mathrm{J}(L)$ the *radical* of L.

(iv) Apparently L is semisimple if and only if $\mathrm{J}(L) = 0$ holds. In general, $L/\mathrm{J}(L)$ is semisimple. The radical therefore plays a similar role as the Jacobson radical for ordinary algebras (Remark II.8.17).

(v) If $I \neq 0$ is a solvable ideal of L, then there exists a $k \in \mathbb{N}$ with $I^{(k)} \neq 1 = I^{(k+1)}$. Now $I^{(k)}$ is an abelian ideal of L. Therefore L is semisimple if and only if L has no non-trivial abelian ideals.

Definition III.9.23. For a Lie algebra L we define $\mathrm{Z}_0(L) := 0$ and

$$\mathrm{Z}_n(L)/\mathrm{Z}_{n-1}(L) := \mathrm{Z}(L/\mathrm{Z}_{n-1}(L))$$

for $n \geq 1$.

Lemma III.9.24. *For every Lie algebra L and $n, k \in \mathbb{N}_0$ holds:*

(i) $\mathrm{Z}_{n+k}(L)/\mathrm{Z}_n(L) = \mathrm{Z}_k(L/\mathrm{Z}_n(L))$.

(ii) $L^{[n+1]} = 0 \iff \mathrm{Z}_n(L) = L$.

Proof.

(i) Induction on k: For $k = 0, 1$ the claim follows from the definition. Let $\overline{L} := L/\mathrm{Z}_n(L)$. For $k \geq 1$ it holds inductively

$$\begin{aligned} \mathrm{Z}_{k+1}(\overline{L})/\mathrm{Z}_k(\overline{L}) &= \mathrm{Z}\big(\overline{L}/\mathrm{Z}_k(\overline{L})\big) \cong \mathrm{Z}(L/\mathrm{Z}_{n+k}(L)) \\ = \mathrm{Z}_{n+k+1}(L)/\mathrm{Z}_{n+k}(L) &\cong (\mathrm{Z}_{n+k+1}(L)/\mathrm{Z}_n(L))/(\mathrm{Z}_{n+k}(L)/\mathrm{Z}_n(L)) \\ &= (\mathrm{Z}_{n+1+k}(L)/\mathrm{Z}_n(L))/\mathrm{Z}_k(\overline{L}). \end{aligned}$$

Since the two canonical isomorphisms are inverse to each other, it follows

$$\mathrm{Z}_{k+1}(\overline{L}) = \mathrm{Z}_{n+1+k}(L)/\mathrm{Z}_n(L).$$

(ii) For $n = 0$ the claim is trivial. Let $n \geq 1$ and $[L, L^{[n]}] = L^{[n+1]} = 0$. Then $L^{[n]} \leq \mathrm{Z}(L)$. For $\overline{L} := L/\mathrm{Z}(L)$ it therefore holds $\overline{L}^{[n]} = (L^{[n]} + \mathrm{Z}(L))/\mathrm{Z}(L) = 0$. By induction $\mathrm{Z}_{n-1}(\overline{L}) = \overline{L}$. From (i) it follows $\mathrm{Z}_{n-1}(\overline{L}) = \mathrm{Z}_n(L)/\mathrm{Z}(L)$ and $\mathrm{Z}_n(L) = L$.

Conversely, let $\mathrm{Z}_n(L) = L$. By (i) it holds $\mathrm{Z}_{n-1}(L/\mathrm{Z}(L)) = L/\mathrm{Z}(L)$. Inductively it follows

$$(L^{[n]} + \mathrm{Z}(L))/\mathrm{Z}(L) = (L/\mathrm{Z}(L))^{[n]} = 0$$

and $L^{[n]} \subseteq \mathrm{Z}(L)$. Thus $L^{[n+1]} = [L, L^{[n]}] = 0$. □

Remark III.9.25. Let L be nilpotent. The smallest $n \geq 0$ with $L^{[n+1]} = 0$ (resp. $\mathrm{Z}_n(L) = L$) is called the *nilpotency class* of L. One can, if applicable, refine the sequence $0 = \mathrm{Z}_0(L) \leq \ldots \leq \mathrm{Z}_n(L) = L$ to a sequence of subspaces $0 = L_0 \leq \ldots \leq L_m = L$ with $\dim L_k = k$ for $k = 1, \ldots, m$. Since subspaces of the center are ideals, it holds $L_i \trianglelefteq L$ for $i = 0, \ldots, m$.

Lemma III.9.26. *If I and J are nilpotent ideals of a Lie algebra L, then $I + J$ is also nilpotent.*

Proof. Let $k \in \mathbb{N}$ with $I^{[k]} = J^{[k]} = 0$. Every element in $(I+J)^{[2k]}$ is a linear combination of elements of the form $x := [x_1, \ldots, x_{2k}]$ with $x_1, \ldots, x_{2k} \in I \cap J$. Wlog. at least k of these elements lie in I. Because of $I^{[i]} \trianglelefteq L$ it then follows $x \in I^{[k]} = 0$. This shows $(I+J)^{[2k]} = 0$. □

Definition III.9.27. The largest nilpotent ideal of a Lie algebra L is called the *nilradical* of L and is written as $\mathrm{N}(L)$ (exists by Lemma III.9.26).

Theorem III.9.28 (Engel)**.** *Let $L \subseteq \mathfrak{gl}(n, K)$ be a Lie algebra consisting of nilpotent elements. Then there exists an $x \in \mathrm{GL}(n, K)$ such that xLx^{-1} consists of strictly upper triangular matrices. In particular, L is nilpotent.*

Proof. Induction on n. Wlog. let $n \geq 1$ and $V := K^n$. By Lemma III.9.18 there exists a $v \in V \setminus \{0\}$ with $x(v) = 0$ for all $x \in V$. Let $\overline{V} := V/\langle v \rangle$. There is a canonical homomorphism of Lie algebras $L \to \mathfrak{gl}(\overline{V})$. By induction there exists a basis $b_2 + \langle v \rangle, \ldots, b_n + \langle v \rangle$ of $\overline{V}$, such that every $x \in L$ is described by a strict upper triangular matrix on $\overline{V}$. With respect to the basis $v, b_2, \ldots, b_n$ of V, every $x \in L$ is a strict upper triangular matrix. □

Remark III.9.29. Not every nilpotent Lie algebra $L \subseteq \mathfrak{gl}(n, K)$ consists of nilpotent elements. For example, the abelian Lie algebra $L = K1_n$.

Corollary III.9.30. *A Lie algebra L is nilpotent if and only if $\mathrm{ad}(L)$ consists of nilpotent elements.*

Proof. Let L be nilpotent with $L^{[k]} = 0$. For $x \in L$ it holds that $\mathrm{ad}_x(L) \subseteq L'$, $\mathrm{ad}_x^2(L) \subseteq [L, L'] = L^{[3]}$ and inductively $\mathrm{ad}_x^{k-1}(L) \subseteq L^{[k]} = 0$, i. e. ad_x is nilpotent for all $x \in L$.

Conversely, assume that $\mathrm{ad}(L)$ consists of nilpotent elements. By Engel, $\mathrm{ad}(L) \cong L/\mathrm{Z}(L)$ is nilpotent. Therefore there exists a $k \in \mathbb{N}$ with $L^{[k]} \subseteq \mathrm{Z}(L)$. Because of $L^{[k+1]} \subseteq [L, \mathrm{Z}(L)] = 0$, L is nilpotent. □

Lemma III.9.31. *Let $L \subseteq \mathfrak{gl}(V)$ be a Lie algebra and $I \trianglelefteq L$ an ideal consisting of nilpotent elements. Then $\mathrm{tr}(x_1 \ldots x_k) = 0$ for $k \in \mathbb{N}$ and $x_1, \ldots, x_k \in L$, as long as at least one x_i lies in I.*

Proof. Let $n := \dim V$. For $k = 0, \ldots, n$ let

$$V_k := \mathrm{Span}\{x_1 \ldots x_k v : v \in V,\ x_1, \ldots, x_k \in I\}.$$

By Engel it holds that $0 = V_n \subseteq V_{n-1} \subseteq \ldots \subseteq V_0 = V$ (cf. Example III.9.21). We show by induction on k that V_k is invariant under L. This is clear for $k = 0$. So let $k \geq 1$, $x \in I$, $u \in V_{k-1}$, $v = xu \in V_k$ and $a \in L$. Then by induction

$$av = [a, x]u + xau \in V_k + xV_{k-1} \subseteq V_k.$$

Now let $x_1, \ldots, x_k \in L$ and $x_i \in I$. Then

$$x_1 \ldots x_k V_l \subseteq x_1 \ldots x_i V_l \subseteq x_1 \ldots x_{i-1} V_{l+1} \subseteq V_{l+1}.$$

With respect to a suitable basis, $x_1 \ldots x_k$ is therefore a strict upper triangular matrix (with trace 0). □

Lemma III.9.32. *Let $\mathrm{char}\, K = 0$. $a \in \mathfrak{gl}(n, K)$ is nilpotent if and only if $\mathrm{tr}(a^k) = 0$ for $k = 1, \ldots, n$.*

Proof. If a is nilpotent, then a is similar to a strictly upper triangular matrix. This shows $\operatorname{tr}(a^k) = 0$ for $k = 1, \ldots, n$. Conversely, let $\operatorname{tr}(a^k) = 0$ for $k = 1, \ldots, n$. Wlog. let K be algebraically closed and a in Jordan normal form. Let $\lambda_1, \ldots, \lambda_n \in K$ be the eigenvalues and

$$\mu = X^d + c_{d-1}X^{d-1} + \ldots + c_0 \in K[X]$$

be the minimal polynomial of a. According to Vieta, the c_i can be expressed by elementary symmetric polynomials in $\lambda_1, \ldots, \lambda_n$. According to the Girard-Newton identities, the elementary symmetric polynomials can be expressed by the power sum polynomials $\rho_k = X_1^k + \ldots + X_n^k$ (this requires $\operatorname{char} K = 0$). Because of $\rho_k(\lambda_1, \ldots, \lambda_n) = \operatorname{tr}(a^k) = 0$, it follows that $c_i = 0$ for $i = 0, \ldots, d-1$. Thus a is nilpotent. □

Example III.9.33. The non-nilpotent identity matrix $a = 1_p \in \mathfrak{gl}(p, p)$ for $p \in \mathbb{P}$ satisfies $\operatorname{tr}(a^k) = \operatorname{tr}(1_p) = 0$ for $k \in \mathbb{N}$.

Lemma III.9.34. *Let* $\operatorname{char} K = 0$. *Let* $L \subseteq \mathfrak{gl}(V)$ *be a Lie algebra and* $I, J \trianglelefteq L$ *with* $J \subseteq [L, I]$. *If* $[I, J]$ *consists of nilpotent elements, then* J *also consists of nilpotent elements.*

Proof. Let $x \in J$. According to Lemma III.9.32, we must show $\operatorname{tr}(x^k) = 0$ for $k \in \mathbb{N}$. Because of $x \in J \subseteq [L, I]$, it suffices to show $\operatorname{tr}([a, y]x^{k-1}) = 0$ for $a \in L$, $y \in I$ and $k \in \mathbb{N}$. It holds that

$$\operatorname{tr}([a, y]x^{k-1}) = \operatorname{tr}(ayx^{k-1}) - \operatorname{tr}(yax^{k-1}) = \operatorname{tr}(ayx^{k-1}) - \operatorname{tr}(ax^{k-1}y) = \operatorname{tr}(a[y, x^{k-1}]).$$

According to the Leibniz rule (Exercise III.46), we have

$$[y, x^{k-1}] = \sum_{l=1}^{k-1} x^{l-1}[y, x]x^{k-l-1}.$$

Therefore, every summand in $a[y, x^{k-1}]$ has a nilpotent factor in $[I, J]$. The claim follows from Lemma III.9.31. □

Theorem III.9.35. *For every Lie algebra* L *over a field of characteristic* 0, *it holds that* $L' \cap \mathrm{J}(L) \subseteq \mathrm{N}(L)$.

Proof. Let $\overline{L} := L/\mathrm{Z}(L)$. As usual, $\mathrm{J}(\overline{L}) = \overline{\mathrm{J(L)}}$ and $\mathrm{N}(\overline{L}) = \overline{\mathrm{N(L)}}$ hold. From $\overline{L}' \cap \mathrm{J}(\overline{L}) \subseteq \mathrm{N}(\overline{L})$ it follows that

$$L' \cap \mathrm{J}(L) \subseteq (L' + \mathrm{Z}(L)) \cap \mathrm{J}(L) \subseteq \mathrm{N}(L).$$

It thus suffices to show the claim for $\overline{L} \cong \operatorname{ad}(L) \leq \mathfrak{gl}(L)$. We therefore assume $L \subseteq \mathfrak{gl}(V)$. Let $J := \mathrm{J}(L)$ and $J^{(n)} = 0$. We show by induction on $k = n, n-1, \ldots, 0$ that $L' \cap J^{(k)}$ consists of nilpotent elements. This is clear for $k = n$. Suppose the claim has already been shown for $k+1$. Then $[[L, J^{(k)}], J^{(k)}] \subseteq L' \cap J^{(k+1)}$ consists of nilpotent elements. According to Lemma III.9.34, $[L, J^{(k)}]$ consists of nilpotent elements and thus also $[L, L' \cap J^{(k)}]$. Another application of Lemma III.9.34 with $I = L$ shows that $L' \cap J^{(k)}$ consists of nilpotent elements. The case $k = 0$ yields the claim with Engel. □

Corollary III.9.36. *A Lie algebra* L *over a field of characteristic* 0 *is solvable if and only if* L' *is nilpotent.*

Proof. If L' is nilpotent, then L' and L are solvable. The converse follows from Theorem III.9.35. □

Remark III.9.37.

(i) According to Exercise III.50, there exists a 4-dimensional solvable Lie algebra L over $\mathbb{F}_2$ such that L' is not nilpotent.

(ii) Like solvability, nilpotency can also be defined for groups (Exercise III.53). However, Corollary III.9.36 does not hold for groups, because for the solvable group S_4, $S_4' = A_4$ is not nilpotent.

Lemma III.9.38. *Let K be algebraically closed with characteristic 0, $V \neq 0$ and $L \subseteq \mathfrak{gl}(V)$ a solvable Lie algebra. Then there exists a weight $\lambda\colon L \to K$.*

Proof. Wlog. let $L \neq 0$. Then there exists a subspace $I \subseteq L$ with $L' \subseteq I$ and $L = I + Kx$ for some $x \in L \setminus I$. Obviously, I is a solvable ideal of L. By induction, there exists $\lambda\colon I \to K$ with

$$U := \{v \in V : \forall a \in I : a(v) = \lambda(a)v\} \neq 0.$$

According to the invariance lemma, $x(U) \subseteq U$ holds. Since K is algebraically closed, x has an eigenvector $u \in U$ on U with eigenvalue $\mu \in K$. We extend λ linearly to L by setting $\lambda(x) := \mu$. For $a \in I$ and $c \in K$, we have

$$(a + cx)(u) = \lambda(a)u + c\lambda(x)u = \lambda(a + cx)u.$$

This shows $u \in V_\lambda \neq 0$. □

Theorem III.9.39 (Lie)**.** *Let K be algebraically closed with characteristic 0 and $L \subseteq \mathfrak{gl}(n, K)$ a solvable Lie algebra. Then there exists an $x \in \mathrm{GL}(n, K)$ such that xLx^{-1} consists of upper triangular matrices.*

Proof. Let $V := K^n \neq 0$. According to Lemma III.9.38, there exists a weight $\lambda\colon L \to K$. Then $v \in V_\lambda \setminus \{0\}$ is a common eigenvector of all elements of L. In particular, $U := \langle v \rangle$ is L-invariant and L acts on $\overline{V} := V/U$. By induction, $\overline{V}$ has a basis $b_2 + U, \ldots, b_n + U$ such that every $x \in L$ is described by an upper triangular matrix on $\overline{V}$. Now $v, b_2, \ldots, b_n$ is a basis of V with the desired property. □

Example III.9.40. Let K be an (algebraically closed) field of characteristic $p > 0$. Let L be the Lie subalgebra of $\mathfrak{gl}(p, K)$ generated by the matrices

$$x := \begin{pmatrix} 0 & 1 & & 0 \\ \vdots & \ddots & \ddots & \\ & & & \\ 0 & & \ddots & 1 \\ 1 & 0 & \cdots & 0 \end{pmatrix}, \qquad y := \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & p-1 \end{pmatrix}$$

Because of

$$[x, y] = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & p-1 \\ & & & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \ddots & 1 & & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & & & \ddots & p-2 \\ p-1 & 0 & \cdots & \cdots & 0 \end{pmatrix} = x$$

$\dim L = 2$. In particular, L is solvable. Since y has pairwise distinct eigenvalues and none of the standard basis vectors is an eigenvector of x, L possesses no weight. Thus Lie's Theorem does not hold in positive characteristic.

Lemma III.9.41. *Diagonalizable matrices $a, b \in K^{n\times n}$ are commutable if and only if they have diagonal form with respect to a common basis.*

Proof. If $s^{-1}as$ and $s^{-1}bs$ are diagonal matrices for some $s \in \mathrm{GL}(n, K)$, then

$$ab = s(s^{-1}ass^{-1}bs)s^{-1} = s(s^{-1}bss^{-1}as)s^{-1} = ba.$$

Conversely, let $ab = ba$. We can assume that a is a diagonal matrix. For an eigenvalue λ of a, the corresponding eigenspace E_λ then consists of standard basis vectors. For $v \in E_\lambda$, we have $abv = bav = \lambda bv$ and $bv \in E_\lambda$, i. e. E_λ is b-invariant. Thus b has block diagonal form. The minimal polynomial of each block divides the minimal polynomial of b. Since b is diagonalizable, the minimal polynomials split into pairwise distinct linear factors. Therefore, each block of b is diagonalizable. It is thus sufficient to prove the claim for each block. In this case, however, $a = \lambda 1_n$ and for every $t \in \mathrm{GL}(n, K)$ we have $t^{-1}at = a$. □

Theorem III.9.42 (Jordan-Chevalley decomposition)**.** *Let* $\operatorname{char} K = 0$ *and* $a \in K^{m\times m}$*. Then there exist uniquely determined matrices* $d, n \in K^{m\times m}$ *with the following properties:*

(i) $a = d + n$ *and* $dn = nd$*.*

(ii) d *is diagonalizable over* $\overline{K}$ *and* n *is nilpotent.*

Furthermore, there exists $\alpha \in K[X]$ *with* $\alpha(a) = d$*.*

Proof. Let $\mu \in K[X]$ be the minimal polynomial of a and L a splitting field of μ over K. We first prove the claim over L. Let

$$\mu = (X - \lambda_1)^{e_1} \dots (X - \lambda_k)^{e_k}$$

with pairwise distinct eigenvalues $\lambda_1, \dots, \lambda_k \in L$. Let

$$L^m = \operatorname{Ker}\big((a - \lambda_1 1_m)^{e_1}\big) \oplus \dots \oplus \operatorname{Ker}\big((a - \lambda_k 1_m)^{e_k}\big)$$

be the corresponding generalized eigenspace decomposition.[2] According to the Chinese Remainder Theorem, there exists an $\alpha \in L[X]$ with $\alpha \equiv \lambda_i \pmod{(X - \lambda_i)^{e_i}}$ for $i = 1, \dots, k$. For $1 \le i \le k$ and $v \in \operatorname{Ker}((a - \lambda_i 1_m)^{e_i})$, it now holds that $\alpha(a)v = \lambda_i v$. With respect to a suitable basis, $d := \alpha(a)$ is thus a diagonal matrix and a is in Jordan normal form. With respect to this basis, $n := a - d$ is nilpotent as a strictly lower triangular matrix. Furthermore, $dn = \alpha(a)a - d^2 = a\alpha(a) - d^2 = nd$.

Now let also $a = d_1 + n_1$ with $d_1 n_1 = n_1 d_1$, d_1 diagonalizable and n_1 nilpotent. Then d_1 commutes with a and therefore also with $\alpha(a) = d$. According to Lemma III.9.41, d and d_1 are simultaneously diagonalizable. In particular, $d - d_1$ is also diagonalizable. Analogously, n_1 commutes with d and therefore also with n. According to the binomial formula, $n - n_1$ is nilpotent. Overall, $d - d_1 = n_1 - n$ is diagonalizable and nilpotent, i. e. $d = d_1$ and $n = n_1$.

Because $\operatorname{char} K = 0$, $K \subseteq L$ is a Galois extension. For $\sigma \in \mathrm{Gal}(L|K)$, it holds that $a = \sigma(a) = \sigma(d) + \sigma(n)$. Obviously, $\sigma(d)$ and $\sigma(n)$ are also diagonalizable (over L) and nilpotent, respectively. Furthermore, $\sigma(d)\sigma(n) = \sigma(dn) = \sigma(nd) = \sigma(n)\sigma(d)$. From the uniqueness of d and n, it follows that $\sigma(d) = d$ and $\sigma(n) = n$. Since $K \subseteq L$ is a Galois extension, it follows that $d, n \in K^{m\times m}$. Since d is in the L-span of the matrices $1_m, a, a^2, \dots$, d must also lie in the K-span of these matrices. Therefore, one can choose $\alpha \in K[X]$. □

[2] See lecture notes linear algebra

Lemma III.9.43. *Let* $\operatorname{char} K = 0$ *and* $x \in \mathfrak{gl}(m, K)$ *with Jordan-Chevalley decomposition* $x = d + n$. *Then* $\operatorname{ad}_x = \operatorname{ad}_d + \operatorname{ad}_n$ *is the Jordan-Chevalley decomposition of* ad_x.

Proof. Obviously, $\operatorname{ad}_x = \operatorname{ad}_d + \operatorname{ad}_n$. According to Lemma III.9.12, ad_d is diagonalizable and ad_n is nilpotent. Furthermore, $[\operatorname{ad}_d, \operatorname{ad}_n] = \operatorname{ad}_{[d,n]} = \operatorname{ad}_0 = 0$, i. e. $\operatorname{ad}_d \operatorname{ad}_n = \operatorname{ad}_n \operatorname{ad}_d$. □

Theorem III.9.44. *Let* $\operatorname{char} K = 0$ *and* $L \subseteq \mathfrak{gl}(m, K)$ *be a Lie algebra with* $\operatorname{tr}(xy) = 0$ *for all* $x, y \in L$. *Then* L *is solvable.*

Proof. According to Engel, it suffices to show that every $x \in L'$ is nilpotent. Let $x = d + n$ be the Jordan-Chevalley decomposition of x. To show $d = 0$, we can assume that K is algebraically closed and $d = \operatorname{diag}(\lambda_1, \ldots, \lambda_m)$ already has diagonal form. Let $F := \operatorname{Span}_{\mathbb{Q}}(\lambda_1, \ldots, \lambda_m)$. It suffices to show that every linear form $f\colon F \to \mathbb{Q}$ is trivial. Let $d' := \operatorname{diag}(f(\lambda_1), \ldots, f(\lambda_m))$ and $\alpha \in K[X]$ with $\alpha(\lambda_i - \lambda_j) = f(\lambda_i - \lambda_j) = f(\lambda_i) - f(\lambda_j)$ for all $i \neq j$ (interpolation). With respect to the standard basis E_{ij}, ad_d is a diagonal matrix with eigenvalues $\lambda_i - \lambda_j$ (see proof of Lemma III.9.12). This shows $\alpha(\operatorname{ad}_d) = \operatorname{ad}_{d'}$. According to Lemma III.9.43, $\operatorname{ad}_x = \operatorname{ad}_d + \operatorname{ad}_n$ is the Jordan-Chevalley decomposition of ad_x. In particular, there exists a $\beta \in K[X]$ with $\operatorname{ad}_d = \beta(\operatorname{ad}_x)$. For $y \in L$, it holds that $[d', y] = \operatorname{ad}_{d'}(y) = \alpha(\beta(\operatorname{ad}_x))(y) \in L$. By assumption,

$$\operatorname{tr}\big([y, z]d'\big) = \operatorname{tr}(yzd') - \operatorname{tr}(zyd') = \operatorname{tr}(d'yz) - \operatorname{tr}(yd'z) = \operatorname{tr}\big([d', y]z\big) = 0$$

for all $z \in L$. Since $x \in L'$ can be written as a linear combination of $[y, z]$, one obtains

$$\sum_{i=1}^{m} \lambda_i f(\lambda_i) = \operatorname{tr}(xd') = 0.$$

Applying f yields $\sum_{i=1}^{m} f(\lambda_i)^2 = 0$. Since f maps to $\mathbb{Q}$, it follows that $f(\lambda_1) = \ldots = f(\lambda_m) = 0$ as desired. □

Definition III.9.45. For a Lie algebra L,

$$\kappa\colon L \times L \to K, \qquad (x, y) \mapsto \operatorname{tr}(\operatorname{ad}_x \circ \operatorname{ad}_y) \qquad (x, y \in L)$$

is a symmetric bilinear form, which is called the *Killing form* of L.

Remark III.9.46. For $x, y, z \in L$, it holds as usual that $\kappa([x, y], z) = \kappa(x, [y, z])$, i. e. κ is *associative* (cf. Definition II.13.2). For $I \trianglelefteq L$ it follows that

$$I^{\perp} := \{x \in L : \kappa(x, I) = 0\} \trianglelefteq L.$$

The form κ is non-degenerate if and only if $L^{\perp} = 0$ holds.

Theorem III.9.47 (Cartan criterion for solvability)**.** *Let* $\operatorname{char} K = 0$. *A Lie algebra* L *is solvable if and only if* $\kappa(L, L') = 0$ *holds.*

Proof. Let L be solvable. According to Lie, we can assume that $\operatorname{ad}(L)$ in $\overline{K}^{n \times n}$ consists of upper triangular matrices. Consequently, every $\operatorname{ad}_y \in L'$ is a strictly upper triangular matrix. This shows $\kappa(x, y) = \operatorname{tr}(\operatorname{ad}_x \operatorname{ad}_y) = 0$ for all $x \in L$. Conversely, let $\operatorname{tr}(\operatorname{ad}_x \operatorname{ad}_y) = 0$ for all $x \in L$ and $y \in L'$. According to Theorem III.9.44, $\operatorname{ad}(L') = (L' + \mathrm{Z}(L))/\mathrm{Z}(L)$ is solvable and thus so is L. □

Lemma III.9.48. *Let I be an ideal of the Lie algebra L. Then the Killing forms of L and I coincide on $I \times I$.*

Proof. Let κ be the Killing form of L and κ_I the Killing form of I. We extend a basis of I to a basis of L. The matrix of ad_x for $x \in I$ with respect to this basis has the form $\left(\begin{smallmatrix} A_x & B_x \\ 0 & 0 \end{smallmatrix}\right)$, where A_x is the matrix of ad_x in I. For $y \in I$ it holds that

$$\kappa(x,y) = \mathrm{tr} \begin{pmatrix} A_x A_y & * \\ 0 & 0 \end{pmatrix} = \mathrm{tr}(A_x A_y) = \kappa_I(x,y). \qquad \square$$

Theorem III.9.49 (Cartan criterion for semisimplicity)**.** *Let* $\mathrm{char}\, K = 0$*. A Lie algebra is semisimple if and only if the Killing form is non-degenerate.*

Proof. Let L be a Lie algebra with Killing form κ. For $x, y \in L^\perp$ it holds that $\kappa(x,y) = 0$. According to the first Cartan criterion and Lemma III.9.48, $L^\perp$ is solvable. If L is semisimple, then $L^\perp = 0$ must hold, i. e. κ is non-degenerate.

Now let L be not semisimple. According to Remark III.9.22 there exists an abelian ideal $I \neq 0$. For $x \in I$ and $y \in L$ it holds that $(\mathrm{ad}_x \mathrm{ad}_y)^2(L) \subseteq (\mathrm{ad}_x \mathrm{ad}_y)(I) = 0$. Thus $\mathrm{ad}_x \mathrm{ad}_y$ is nilpotent and $\kappa(x,y) = \mathrm{tr}(\mathrm{ad}_x \mathrm{ad}_y) = 0$. This shows $I \subseteq L^\perp$ and κ is degenerate. $\square$

Corollary III.9.50. *Let* $\mathrm{char}\, K = 0$*. Let L be a semisimple Lie algebra and $I \trianglelefteq L$. Then I is semisimple and $L = I \oplus I^\perp$.*

Proof. The Killing form on $J := I \cap I^\perp$ is trivial according to Lemma III.9.48. According to the first Cartan criterion, J is solvable and therefore $J = 0$. Because of $\dim L = \dim(I) + \dim(I^\perp)$, we have $L = I \oplus I^\perp$. Let $x \in I$ with $\kappa(x, I) = 0$. Then also $\kappa(x, L) = \kappa(x, I) + \kappa(x, I^\perp) = 0$. From the second Cartan criterion for L it follows that $x = 0$. The criterion applied to I shows that I is semisimple. $\square$

Corollary III.9.51. *Let* $\mathrm{char}\, K = 0$*. For every semisimple Lie algebra L it holds that $L' = L$.*

Proof. According to Corollary III.9.50 there exists an ideal $I \trianglelefteq L$ with $L = L' \oplus I$. For $x, y \in I$ it holds that $[x,y] \in I \cap L' = 0$. Therefore I is abelian and $I = 0$. $\square$

Remark III.9.52. We now prove a version of Artin-Wedderburn for Lie algebras.

Theorem III.9.53. *Let* $\mathrm{char}\, K = 0$*. A Lie algebra L is semisimple if and only if L is a direct sum of simple ideals.*

Proof. Let L be semisimple and $I \trianglelefteq L$ a maximal ideal. According to Corollary III.9.50, $L = I \oplus I^\perp$ with I semisimple and $I^\perp \cong L/I$ simple. By induction, I is a direct sum of simple ideals. It is easily shown that the ideals of I are also ideals of L. Thus the claim holds.

Now let $L = L_1 \oplus \ldots \oplus L_n$ be a direct sum of simple Lie algebras $L_1, \ldots, L_n$. Let $I \trianglelefteq L$ be solvable. Then $[I, L_i] \subseteq L_i$ is also solvable and $[I, L_i] = 0$. It follows that $[I, L] \subseteq [I, L_1] + \ldots + [I, L_n] = 0$ and $I \subseteq \mathrm{Z}(L)$. Obviously $\mathrm{Z}(L) = \mathrm{Z}(L_1) + \ldots + \mathrm{Z}(L_n) = 0$ and $I = 0$. Thus L is semisimple. $\square$

Remark III.9.54. In the following, we deal with the classification of simple Lie algebras.

Theorem III.9.55. *Let $n \geq 2$ and $\operatorname{char} K \nmid 2n$. Then $\mathfrak{sl}(n, K)$ is a simple Lie algebra.*

Proof. Let $0 \neq x = (x_{ij}) \in I \trianglelefteq L := \mathfrak{sl}(n, K)$. Let us first assume that x is a diagonal matrix. Because of $x_{11} + \ldots + x_{nn} = \operatorname{tr}(x) = 0$ and $\operatorname{char} K \nmid n$, there exist $s \neq t$ with $x_{ss} \neq x_{tt}$. It follows that

$$0 \neq x' := (x_{ss} - x_{tt})E_{st} = \sum_{i=1}^{n} x_{ii}[E_{ii}, E_{st}] = [x, E_{st}] \in I.$$

By replacing x with x' if necessary, we can assume $x_{ts} \neq 0$ for certain $s \neq t$. For $1 \leq i, j \leq n$ we have

$$\begin{aligned}[[E_{ij}, E_{st}], E_{st}] &= [[\delta_{js}E_{it} - \delta_{it}E_{sj}], E_{st}] = \delta_{js}(\delta_{ts}E_{it} - \delta_{it}E_{st}) - \delta_{it}(\delta_{js}E_{st} - \delta_{st}E_{sj}) \\ &= -2\delta_{it}\delta_{js}E_{st} = \begin{cases} -2E_{st} & \text{if } (i,j) = (t,s), \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

It follows that

$$0 \neq -2x_{ts}E_{st} = \sum_{i,j=1}^{n} x_{ij}[[E_{ij}, E_{st}], E_{st}] = [[x, E_{st}], E_{st}] \in I$$

(note $\operatorname{char} K \neq 2$) and $E_{st} \in I$. For $k \notin \{s, t\}$ one obtains

$$E_{sk} = [E_{st}, E_{tk}] \in I, \qquad E_{kt} = [E_{ks}, E_{st}] \in I, \qquad E_{ss} - E_{tt} = [E_{st}, E_{ts}] \in I.$$

One can now vary the roles of s and t so that all basis elements E_{ij} $(i \neq j)$ and $E_{11} - E_{ii}$ of L lie in I. This shows $I = L$. □

Example III.9.56.

(i) The Lie algebra $L := \mathfrak{sl}(2, 2)$ is not simple because of $1_2 \in \mathrm{Z}(L)$.

(ii) For $n \in \mathbb{N}$ and $S = \left(\begin{smallmatrix} 0 & 1_n \\ -1_n & 0 \end{smallmatrix}\right) \in K^{2n \times 2n}$,

$$L := \mathfrak{sp}(2n, K) := \{A \in K^{2n \times 2n} : A^{\mathrm{t}}S = -SA\}$$

is a Lie algebra according to Example III.9.7. Let $A = \left(\begin{smallmatrix} A_1 & A_2 \\ A_3 & A_4 \end{smallmatrix}\right) \in L$. From

$$\begin{pmatrix} -A_3^{\mathrm{t}} & A_1^{\mathrm{t}} \\ -A_4^{\mathrm{t}} & A_2^{\mathrm{t}} \end{pmatrix} = \begin{pmatrix} A_1^{\mathrm{t}} & A_3^{\mathrm{t}} \\ A_2^{\mathrm{t}} & A_4^{\mathrm{t}} \end{pmatrix} \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1_n \\ 1_n & 0 \end{pmatrix} \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} = \begin{pmatrix} -A_3 & -A_4 \\ A_1 & A_2 \end{pmatrix}$$

it follows that $A_1^{\mathrm{t}} = -A_4$, $A_2^{\mathrm{t}} = A_2$ and $A_3^{\mathrm{t}} = A_3$. In particular, $\operatorname{tr}(A) = \operatorname{tr}(A_1) + \operatorname{tr}(A_4) = 0$. Therefore, L is a subalgebra of $\mathfrak{sl}(2n, K)$. One calls L the *symplectic* Lie algebra of degree $2n$. For the choice of A_1 one has n^2 free parameters, while the symmetric matrices A_2 and A_3 each grant $n(n+1)/2$ degrees of freedom. This shows $\dim L = 2n^2 + n$. In particular, $\mathfrak{sp}(2, K) = \mathfrak{sl}(2, K)$.

(iii) Let $S = \left(\begin{smallmatrix} 0 & 1_n \\ 1_n & 0 \end{smallmatrix}\right) \in K^{2n \times 2n}$ and $T := \left(\begin{smallmatrix} 1 & 0 \\ 0 & S \end{smallmatrix}\right) \in K^{(2n+1) \times (2n+1)}$. One calls

$$\begin{aligned}\mathfrak{so}(2n, K) &= \{A \in K^{2n \times 2n} : A^{\mathrm{t}}S = -SA\}, \\ \mathfrak{so}(2n+1, K) &= \{A \in K^{(2n+1) \times (2n+1)} : A^{\mathrm{t}}T = -TA\}\end{aligned}$$

the *special orthogonal* Lie algebras of degree $2n$ and $2n+1$, respectively. A calculation as in (ii) shows $\mathfrak{so}(n, K) \subseteq \mathfrak{sl}(n, K)$ and $\dim \mathfrak{so}(n, K) = \frac{1}{2}(n^2 - n)$ for $n \geq 2$. One can show $\mathfrak{so}(3, \mathbb{C}) \cong \mathfrak{sl}(2, \mathbb{C})$, $\mathfrak{so}(5, \mathbb{C}) \cong \mathfrak{sp}(4, \mathbb{C})$ and $\mathfrak{so}(6, \mathbb{C}) \cong \mathfrak{sl}(4, \mathbb{C})$.

Remark III.9.57. Killing and Cartan have proven that every complex simple Lie algebra is isomorphic to exactly one of the following Lie algebras:

(a) $\mathfrak{sl}(n, \mathbb{C})$ for $n \geq 2$.

(b) $\mathfrak{sp}(2n, \mathbb{C})$ for $n \geq 2$.

(c) $\mathfrak{so}(n, \mathbb{C})$ for $n = 4, 7, 8, \ldots$.

(d) one of the exceptional ones $\mathfrak{g}_2$, $\mathfrak{f}_4$, $\mathfrak{e}_6$, $\mathfrak{e}_7$, $\mathfrak{e}_8$ with dimensions 14, 52, 78, 133, 248.

Definition III.9.58. A *representation* of a Lie algebra L is a homomorphism of Lie algebras $\Delta\colon L \to \mathfrak{gl}(V)$, where V is a finite-dimensional K-vector space. If applicable, V becomes a (*Lie*) *module* of L, i.e., for $x, y \in L$, $v, w \in V$ and $\lambda \in K$ we have

- $x(v + w) = xv + xw$,
- $(x + y)(v) = xv + yv$,
- $(\lambda x)(v) = \lambda xv$,
- $[x, y](v) = x(yv) - y(xv)$

(note that $(xy)(v)$ is not defined).

Example III.9.59.

(i) For every degree (or every dimension) there is always the trivial representation $L \to \mathfrak{gl}(V)$, $x \mapsto 0$ (and the trivial module).

(ii) The analogue of the regular representation (for ordinary algebras) is the adjoint representation $\mathrm{ad}\colon L \to \mathfrak{gl}(L)$. We call L the *adjoint* Lie module of L. In contrast to the regular representation, ad is generally not faithful ($\mathrm{Ker}(\mathrm{ad}) = \mathrm{Z}(L)$). We prove in Theorem III.9.97 that every Lie algebra possesses a faithful representation.

(iii) For Lie modules V and W of L, $V \times W$ is also a Lie module of L. Furthermore, $\mathrm{Hom}(V, W)$ is a Lie module with

$$(x\varphi)(v) := x\varphi(v) - \varphi(xv)$$

for $\varphi \in \mathrm{Hom}(V, W)$ and $v \in V$, because

$$\begin{aligned}([x, y]\varphi)(v) &= x(y\varphi(v)) - y(x\varphi(v)) - \varphi(x(yv)) + \varphi(y(xv)) \\ &= x(y\varphi)(v) - (y\varphi)(xv) - y(x\varphi)(v) + (x\varphi)(yv) = (x(y\varphi))(v) - (y(x\varphi))(v).\end{aligned}$$

(iv) If $W = K$ is the trivial Lie module in the situation of (iii), one obtains the *dual* Lie module $V^* := \mathrm{Hom}(V, K)$ with $(x\varphi)(v) = -\varphi(xv)$ for $x \in L$, $\varphi \in V^*$ and $v \in V$.

(v) Let A be an ordinary algebra and V an A-module. If one considers A as a Lie algebra via $[a, b] := ab - ba$ for $a, b \in A$, then V is also a Lie module.

Remark III.9.60.

(i) As usual, one defines submodules of Lie modules. A Lie module $M \neq 0$ is called *simple*, if 0 and M are the only submodules. The corresponding representation is called *irreducible* if applicable. The trivial 1-dimensional module is simple. In contrast to ordinary (finite-dimensional) algebras, a Lie algebra can possess simple modules with arbitrarily large dimensions (Theorem III.9.64).

(ii) As usual, one defines homomorphisms between Lie modules and proves the homomorphism theorem and the isomorphism theorems. One easily shows that $\mathrm{End}_L(V)$ for an L-module is an algebra in the conventional sense. If V is simple, then $\mathrm{End}_L(V)$ is a division algebra (Schur's Lemma).

(iii) The submodules of the adjoint module L are the ideals of L. Therefore, L is simple if and only if ad is irreducible.

(iv) The isomorphism of Lie modules corresponds, as usual, to the similarity of representations.

Lemma III.9.61. *Let V be a Lie module of a Lie algebra L. Then the following statements are equivalent:*

(1) V is a sum of simple Lie modules.

(2) V is a direct sum of simple Lie modules.

(3) For every submodule $U \leq V$ there exists a submodule $W \leq V$ with $V = U \oplus W$.

If applicable, V is called semisimple.

Proof. The proof works similarly to Theorem II.7.4, except that one can dispense with Zorn's Lemma since all modules are finite-dimensional.

(1) $\Rightarrow$ (2): Let $U \leq V$ be a maximal direct sum of simple modules. Suppose there exists a simple module $S \leq V$ with $S \not\subseteq U$. Since S is simple, $U \cap S = 0$ holds and therefore $U + S = U \oplus S$ in contradiction to the choice of U. By assumption, $U = V$ follows.

(2) $\Rightarrow$ (3): Let $V = S_1 \oplus \ldots \oplus S_n$ with simple modules $S_1, \ldots, S_n$. Let $W \leq V$ be a maximal sum of S_i with $W \cap U = 0$. Suppose $U + W < V$ holds. Then there exists an S_i with $S_i \not\subseteq U + W$. Because of the simplicity of S_i, $(U + W) \cap S_i = 0$ and $(W + S_i) \cap U = 0$ in contradiction to the choice of W. This shows $V = U \oplus W$.

(3) $\Rightarrow$ (1): Let U be the sum of all simple submodules of V. Then there exists $W \leq V$ with $V = U \oplus W$. In the case $W \neq 0$, W would have a simple submodule, which would also have to lie in U. Therefore $W = 0$ and $V = U$. □

Theorem III.9.62. *Let K be algebraically closed with* $\mathrm{char}\, K = 0$. *Then every simple module of a solvable Lie algebra is* 1*-dimensional.*

Proof. Let $\Delta\colon L \to \mathfrak{gl}(n, K)$ be an irreducible representation of the solvable Lie algebra L. According to Lie, we can assume that $\Delta(L)$ consists of upper triangular matrices. Then $K(1, 0, \ldots, 0)$ is a submodule and it follows that $n = 1$. □

Example III.9.63. Let K be algebraically closed with $\mathrm{char}\, K = 0$ and $L \neq 0$ a solvable Lie algebra. Then the irreducible representations are exactly the linear maps $\Delta\colon L \to K$ with $L' \subseteq \mathrm{Ker}(\Delta)$. In particular, in the case $|K| = \infty$, L possesses infinitely many non-isomorphic simple modules.

Theorem III.9.64. *Let K be algebraically closed with* $\mathrm{char}\, K = 0$. *For every $d \in \mathbb{N}$, $\mathfrak{sl}(2, K)$ possesses exactly one simple module of dimension d up to isomorphism.*

Proof. For $d \geq 0$ let $V_d := \bigoplus_{k=0}^{d} KX^kY^{d-k} \subseteq K[X,Y]$ be the space of all homogeneous polynomials in X, Y of degree d. Then $\dim V_d = d+1$. Obviously, $\mathfrak{sl}(2,K)$ is spanned as a vector space by $x := E_{12}$, $y := E_{21}$ and $z := E_{11} - E_{22}$. We show that V_d becomes a Lie module via

$$\begin{aligned} x(X^kY^{d-k}) &:= (d-k)X^{k+1}Y^{d-k-1}, \\ y(X^kY^{d-k}) &:= kX^{k-1}Y^{d-k+1}, \\ z(X^kY^{d-k}) &:= (2k-d)X^kY^{d-k}. \end{aligned}$$

It holds that $[x,y] = z$, $[x,z] = -2x$ and $[y,z] = 2y$. On the other hand,

$$\begin{aligned} (xy-yx)(X^kY^{d-k}) &= x(kX^{k-1}Y^{d-k+1}) - y((d-k)X^{k+1}Y^{d-k-1}) \\ &= k(d-k+1)X^kY^{d-k} - (d-k)(k+1)X^kY^{d-k} \\ &= (2k-d)X^kY^{d-k} = z(X^kY^{d-k}), \\ (xz-zx)(X^kY^{d-k}) &= x((2k-d)X^kY^{d-k}) - z((d-k)X^{k+1}Y^{d-k-1}) \\ &= (2k-d)(d-k)X^{k+1}Y^{d-k-1} - (d-k)(2(k+1)-d)X^{k+1}Y^{d-k-1} \\ &= 2(k-d)X^{k+1}Y^{d-k-1} = -2x(X^kY^{d-k}), \\ (yz-zy)(X^kY^{d-k}) &= y((2k-d)X^kY^{d-k}) - z(kX^{k-1}Y^{d-k+1}) \\ &= (2k-d)kX^{k-1}Y^{d-k+1} - k(2(k-1)-d)X^{k-1}Y^{d-k+1} \\ &= 2kX^{k-1}Y^{d-k+1} = 2y(X^kY^{d-k}). \end{aligned}$$

Let $U \leq V_d$ be a submodule. Since $\{X^kY^{d-k} : k = 0, \ldots, d\}$ is a basis of V_d consisting of eigenvectors of z, the restriction $z_{|U}$ is also diagonalizable (the minimal polynomial has no multiple roots). Since the eigenvalues $-d, 2-d, \ldots, d$ of z are pairwise distinct, the eigenspaces are 1-dimensional. Thus U must contain one of the eigenvectors X^kY^{d-k}. By applying x and y, it follows that $U = V_d$, i.e., V_d is simple.

Now let V be any simple Lie module for $\mathfrak{sl}(2,K)$. Let $v \in V$ be an eigenvector of z with eigenvalue λ. Suppose $x(v) \neq 0$. Then

$$z(xv) = x(zv) - [x,z]v = \lambda xv + 2xv = (\lambda+2)xv,$$

i.e., xv is an eigenvector of z with eigenvalue $\lambda + 2$. If $yv \neq 0$, it follows analogously that yv is an eigenvector of z with eigenvalue $\lambda - 2$. We set $x^kv := x(x(\ldots xv)\ldots)$ for $k \in \mathbb{N}_0$. Because $\dim V < \infty$, there exists a $k \in 0$ with $x^{k+1}v = 0 \neq x^kv$. By replacing v with x^kv, we can assume $xv = 0$. By the same argument, we find $y^{d+1}v = 0 \neq y^dv$. The elements $v_i := y^iv$ for $i = 0, \ldots, d$ are linearly independent, as they are eigenvectors of z for pairwise distinct eigenvalues. Obviously, $U := \langle v_0, \ldots, v_d \rangle$ is invariant under y and z. We show $xv_i \in U$ by induction on i. For $i = 0$, $xv_0 = xv = 0 \in U$. Suppose $xv_{i-1} \in U$ has already been shown. Then

$$xv_i = x(yv_{i-1}) = [x,y]v_{i-1} + y(xv_{i-1}) = zv_{i-1} + y(xv_{i-1}) \in U.$$

Thus $U \leq V$ is a submodule and $U = V$, since V is simple. In particular, $\dim V = d+1$.

The matrix of z as a linear map on V with respect to the basis $v_0, \ldots, v_d$ is diagonal with trace

$$\lambda + (\lambda - 2) + \ldots + (\lambda - 2d) = (d+1)(\lambda - d).$$

On the other hand, $\mathrm{tr}(z) = \mathrm{tr}([x,y]) = 0$. This shows $\lambda = d$. Thus V is uniquely determined as a Lie module and it follows that $V \simeq V_d$. □

Definition III.9.65. For a representation $\Delta\colon L \to \mathfrak{gl}(V)$ of a Lie algebra L, we define the symmetric bilinear form

$$\kappa_V\colon L \times L \to K, \qquad (x, y) \mapsto \operatorname{tr}(\Delta(x)\Delta(y)).$$

Remark III.9.66. For the adjoint representation $\operatorname{ad}\colon L \to \mathfrak{gl}(L)$, one obtains the Killing form $\kappa_L = \kappa$. As in Remark III.9.46, one shows that κ_V is associative in general.

Lemma III.9.67. *Let* $\operatorname{char} K = 0$. *Let* $\Delta\colon L \to \mathfrak{gl}(V)$ *be a faithful representation of a semisimple Lie algebra* L. *Then* κ_V *is non-degenerate.*

Proof. Let $I := \{x \in L : \kappa_V(x, L) = 0\} \trianglelefteq L$. According to Theorem III.9.44, $\Delta(I)$ is solvable. Since Δ is faithful and L is semisimple, $I = 0$ must hold. □

Definition III.9.68. Let L, Δ and V be as in Lemma III.9.67. Let $e_1, \dots, e_n$ be a basis of L and $f_1, \dots, f_n$ the corresponding dual basis with respect to κ_V. We call the map

$$\gamma := \sum_{i=1}^{n} \Delta(e_i)\Delta(f_i)\colon V \to V$$

the *Casimir operator* on V (cf. Remark II.13.5).

Remark III.9.69. With the notation from Definition III.9.68, it holds that

$$x = \sum_{i=1}^{n} \kappa_V(x, e_i) f_i = \sum_{i=1}^{n} \kappa_V(x, f_i) e_i$$

for all $x \in L$.

Lemma III.9.70. *The Casimir operator* γ *on* V *does not depend on the choice of the dual bases. Furthermore,* γ *is a homomorphism of Lie modules with trace* $\dim V$.

Proof. Certainly γ is a K-linear map. Let (e_i'), (f_i') be another pair of dual bases with respect to κ_V. Then it holds that

$$\sum_{i=1}^{n} \Delta(e_i')\Delta(f_i') \overset{\text{III.9.69}}{=} \sum_{i=1}^{n}\sum_{j=1}^{n} \kappa_V(e_i', f_j)\Delta(e_j)\Delta(f_i') = \sum_{j=1}^{n} \Delta(e_j) \sum_{i=1}^{n} \kappa_V(e_i', f_j)\Delta(f_i') = \sum_{j=1}^{n} \Delta(e_j)\Delta(f_j).$$

Therefore, γ does not depend on the choice of the bases.

For $x \in L$ and $v \in V$ it holds that

$$\begin{aligned}
\gamma(xv) &= \sum_{i=1}^{n} e_i(f_i(xv)) = \sum_{i=1}^{n} \big(e_i([f_i, x]v) + e_i(x(f_i v))\big) = \sum_{i=1}^{n} \big(e_i([f_i, x]v) - [x, e_i](f_i v) + x(e_i(f_i v))\big) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} \kappa_V([f_i, x], e_j) e_i(f_j v) - \sum_{i=1}^{n}\sum_{j=1}^{n} \kappa_V(f_j, [x, e_i]) e_j(f_i v) + \sum_{i=1}^{n} x(e_i(f_i v)) \\
&= \sum_{i=1}^{n} x(e_i(f_i v)) = x\gamma(v),
\end{aligned}$$

i. e. γ is a homomorphism. Finally, it holds that

$$\operatorname{tr}(\gamma) = \sum_{i=1}^{n} \operatorname{tr}(\Delta(e_i)\Delta(f_i)) = \sum_{i=1}^{n} \kappa_V(e_i, f_i) = n. \qquad \square$$

Remark III.9.71. We prove Lemma II.8.4 for Lie algebras.

Theorem III.9.72 (Weyl)**.** *Let* $\operatorname{char} K = 0$*. A Lie algebra* L *is semisimple if and only if every* L*-module is semisimple.*

Proof. First, let us assume that the adjoint Lie module L is semisimple. Then there exists a decomposition into simple submodules $L = S_1 \oplus \ldots \oplus S_n$. According to Theorem III.9.53, it suffices to show that each S_i is a simple Lie algebra. So let $0 \neq I \trianglelefteq S_i$. For $j \neq i$, we have $[S_j, I] \subseteq S_i \cap S_j = 0$. This shows $[L, I] \subseteq [S_1, I] + \ldots + [S_n, I] = [S_i, I] \subseteq I$. Therefore, I is a submodule of the simple module S_i. It follows that $I = S_i$ and S_i is simple.

Now let L be semisimple and $\Delta\colon L \to \mathfrak{gl}(V)$ be a representation. According to Corollary III.9.50, $L/\operatorname{Ker}(\Delta) \cong \operatorname{Ker}(\Delta)^{\perp} \trianglelefteq L$ is semisimple. We can therefore assume that Δ is faithful. Let $0 \neq U \leq V$ be a submodule. According to Lemma III.9.61, we must show that U possesses a complement. We argue by induction on $\dim V$.

Step 1: $\dim(V/U) = 1$.
Assume U is not simple. Then there exists a submodule $0 < U_1 < U$. By induction, there exists a $W \leq V$ with $V/U_1 = (U/U_1) \oplus (W/U_1)$. Here $\dim(W/U_1) = \dim(V/U) = 1$ holds. Again by induction, there exists $W_1 \leq W$ with $W = U_1 \oplus W_1$. Because of $W_1 \cap U \leq W_1 \cap W \cap U = W_1 \cap W_1 \cap U_1 = 1$, we have $V = U \oplus W_1$. Now let U be simple. According to Corollary III.9.51, $L = L'$. For $x, y \in L$ and $v \in V$, we have $[x, y]v = x(yv) - y(xv) \in U$ because of $V/U \simeq K$. It follows that $LV \subseteq U$. For the Casimir operator, it holds in particular that $\gamma(V) \subseteq U$ and $W := \operatorname{Ker}(\gamma) \neq 0$. According to Lemma III.9.70, $\operatorname{tr}(\gamma_{|U}) = \operatorname{tr}(\gamma) = \dim V \neq 0$ because of $\operatorname{char} K = 0$. By Schur's Lemma, $\gamma_{|U}$ is invertible. This shows $U \cap W = 0$ and $V = U \oplus W$ because of $\dim(U + W) \geq \dim(U) + 1 = \dim V$.

Step 2: $U \leq V$ arbitrary.
As is well known, $H := \operatorname{Hom}(V, W)$ is an L-module with $(x\varphi)(v) = x\varphi(v) - \varphi(xv)$ for $x \in L$, $\varphi \in H$ and $v \in V$. Obviously, $H_1 := \{\varphi \in H : \varphi_{|U} \in K \operatorname{id}_U\}$ and $H_1 := \{\varphi \in H : \varphi_{|U} = 0\}$ are submodules of H. Let $V = U \oplus W_1$ be a vector space decomposition. Then the projection $V \to U$ lies in $H_1 \setminus H_0$. Therefore, the restriction $H_1 \to K \operatorname{id}_U$ is an epimorphism with kernel H_0. Thus $\dim(H_1/H_0) = 1$ holds and by Step 1 there exists an L-module $H_2 \leq H$ with $H_1 = H_0 \oplus H_2$. Let $\varphi \in H_2 \setminus \{0\}$. Because of $L = L'$, we have $x\varphi = 0$, i. e. $\varphi\colon V \to U$ is an epimorphism of Lie modules. For $W := \operatorname{Ker}(\varphi) \leq V$, we have $\dim(U) + \dim(W) = \dim(V)$ by the homomorphism theorem. Because of $U \cap W = \operatorname{Ker}(\varphi_{|U}) = 0$, we have $V = U \oplus W$. $\square$

Remark III.9.73. For a prime $p > 2$, $L := \mathfrak{sl}(2, p)$ is simple according to Theorem III.9.55. We show that Weyl's Theorem does not hold in this situation. Let

$$V_p := \sum_{k=0}^{p} K X^k Y^{p-k} \leq K[X, Y]$$

be the L-module from the proof of Theorem III.9.64. Then $U := KX^p + KY^p \leq V$ is a (trivial) submodule. Suppose there exists a submodule $W \leq V_p$ with $V_p = U \oplus W$. As in Theorem III.9.64, $z := E_{11} - E_{22}$ is diagonalizable on W with eigenvalues $2 - p, 4 - p, \ldots, p - 2$. Therefore W contains an eigenvector $X^k Y^{p-k}$ with $0 < k < p$. By applying $x := E_{12}$, the contradiction $X^p \in W$ follows easily.

Theorem III.9.74 (Levi)**.** *Let* $\operatorname{char} K = 0$ *and* L *be a Lie algebra. Then there exists a subalgebra* U *with* $L = \mathrm{J}(L) \oplus U$*.*

Proof. Induction on $\dim L$. Let $J := \mathrm{J}(L)$. Suppose there exists an ideal $0 \neq I \trianglelefteq L$ with $I \subsetneq J$. With J, J/I is also solvable and $(L/I)/(J/I) \cong L/J$ is semisimple. This shows $\mathrm{J}(L/I) = J/I$. By induction, there exists a subalgebra $V \leq L$ with $L/I = (J/I) \oplus (V/I)$. Since $V/I \cong (L/I)/(J/I)$ is semisimple, $\mathrm{J}(V) = I$ holds. Again by induction, there exists a subalgebra $U \leq V$ with $V = I \oplus U$. Now $L = J + V = J + U$ and $J \cap U = J \cap V \cap U = I \cap U = 0$ hold.

We can therefore assume that J is a minimal ideal. In particular, J is abelian and $[L, J] \in \{0, J\}$. Let us assume $[L, J] = 0$. Then $J = \mathrm{Z}(L)$ holds. Through the adjoint representation, L becomes an L/J-module. By Weyl, there exists a submodule $U \leq L$ with $L = J \oplus U$. In this case, U is even an ideal. Now let $[L, J] = J$. Then $\mathrm{Z}(L) = 0$. According to Example III.9.59, $E := \mathfrak{gl}(L)$ is an L-module via $(x\varphi)(v) = [\mathrm{ad}_x, \varphi](v) = [x, \varphi(v)] - \varphi([x, v])$ for $x, v \in L$ and $\varphi \in \mathfrak{gl}(L)$. We define the subspaces

$$\begin{aligned} P &:= \{\varphi \in E : \varphi(L) \subseteq J,\ \varphi_{|J} \in K \operatorname{id}_J\}, \\ Q &:= \{\varphi \in P : \varphi(J) = 0\}, \\ R &:= \mathrm{ad}(J) \end{aligned}$$

of E. Let $\varphi \in P$ and $\lambda \in K$ with $\varphi_{|J} = \lambda \operatorname{id}_J$. For $x, v \in L$ and $y \in J$, $(x\varphi)(v) \in J$ and $(x\varphi)(y) = \lambda[x, y] - \lambda[x, y] = 0$ hold. This shows that P is a submodule with $LP \subseteq Q$. Analogously, Q is also a submodule. Because of $[\mathrm{ad}_x, \mathrm{ad}_y] = \mathrm{ad}_{[x,y]} \in R$, R is likewise a submodule. Since J is abelian, $R \subseteq Q \subseteq P$ holds. As in the proof of Weyl, $\dim(P/Q) = 1$. Furthermore, P/R is an L/J-module. By Weyl, there exists a submodule $S/R \leq P/R$ with $P/R = (Q/R) \oplus (S/R)$. We choose $\varphi \in S$ with $\varphi_{|J} = \mathrm{id}_J$. Obviously $U := \{x \in L : x\varphi = 0\}$ is a subalgebra of L. For $x \in L$, $x\varphi \in S \cap Q = R$ holds. Let $y \in J$ with $x\varphi = \mathrm{ad}_y$. For $v \in L$,

$$(y\varphi)(v) = [y, \varphi(v)] - \varphi([y, v]) = -[y, v] = -\mathrm{ad}_y(v)$$

holds. This shows $x + y \in U$ and $L = J + U$. For $y \in J \cap U$, one obtains $y \in \mathrm{Z}(L) = 0$. Therefore $L = J \oplus U$. □

Remark III.9.75. Levi's Theorem transfers the existence statement of Wedderburn-Malcev to Lie algebras. The uniqueness of the subalgebra can be formulated as follows: If U, V are subalgebras of L with $L = \mathrm{J}(L) \oplus U = \mathrm{J}(L) \oplus V$, then there exists an $x \in \mathrm{N}(L)$ with $\exp(\mathrm{ad}_x)(U) = V$, where exp is defined in Exercise III.51 (without proof).

Example III.9.76. For $n \geq 2$, $\mathfrak{sl}(n, \mathbb{C})$ is (semi)simple according to Theorem III.9.55. On the other hand, $\mathrm{Z}(\mathfrak{gl}(n, \mathbb{C})) = \mathbb{C}1_n \cong \mathfrak{gl}(n, \mathbb{C})/\mathfrak{sl}(n, \mathbb{C})$ is abelian. This shows $\mathrm{J}(\mathfrak{gl}(n, \mathbb{C})) = \mathbb{C}1_n$ and $\mathfrak{gl}(n, \mathbb{C}) = \mathbb{C}1_n \oplus \mathfrak{sl}(n, \mathbb{C})$.

Corollary III.9.77. *Let* $\operatorname{char} K = 0$ *and* L *be a Lie algebra. Then* $[L, \mathrm{J}(L)] = L' \cap \mathrm{J}(L)$ *holds.*

Proof. Obviously $[L, \mathrm{J}(L)] \subseteq L' \cap \mathrm{J}(L)$. Let $U \leq L$ be a subalgebra with $L = \mathrm{J}(L) \oplus U$. Then $L' \subseteq [L, \mathrm{J}(L)] + [U, U] \subseteq [L, \mathrm{J}(L)] + U$ holds. From the Dedekind identity (for vector spaces) it follows that

$$L' \cap \mathrm{J}(L) \subseteq ([L, \mathrm{J}(L)] + U) \cap \mathrm{J}(L) = [L, \mathrm{J}(L)] + (U \cap \mathrm{J}(L)) \subseteq [L, \mathrm{J}(L)] + \mathrm{J}(U) = [L, \mathrm{J}(L)]. \qquad \square$$

Definition III.9.78.

- Let $X_1, X_2, \ldots$ be at most countably many non-commutative variables. Let $M := \langle X_1, X_2, \ldots \rangle$ be the monoid of all monomials of the form $X_{i_1} \ldots X_{i_k}$ with $k \in \mathbb{N}_0$ and $i_1, \ldots, i_k \in \mathbb{N}$ with respect to concatenation (for $k = 0$ one obtains the identity element 1). We order the monomials first by length and subsequently lexicographically, i. e.

$$X_{i_1} \ldots X_{i_k} \leq X_{j_1} \ldots X_{j_l} \ :\Longleftrightarrow\ k < l \vee (k = l \wedge (i_1, \ldots, i_k) \leq (j_1 \ldots, j_k)).$$

  For example,

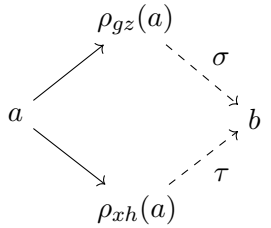
$$1 < X_1 < X_2 < \ldots < X_1^2 < X_1X_2 < \ldots < X_2^2 < \ldots < X_1^3 < \ldots.$$

  This defines a well-ordering on M.

- Let $A := K\langle X_1, \ldots \rangle$ be the infinite-dimensional K-algebra with basis M. One calls A the *free* algebra in $X_1, \ldots$. The elements of A we call (non-commutative) *polynomials*.

- For $a \in A$ let $a_0 := \lambda X_{i_1} \ldots X_{i_k}$ with $\lambda \in K^\times$ be the leading term of a with respect to the order on M defined above (where λ has no influence on the order). We call a *monic*, if $\lambda = 1$. Let $I := (G) \trianglelefteq A$ be an ideal with a set of monic generators $G \subseteq A$. For $g \in G$ and $x, y \in M$ let $\rho_{xgy} \colon A \to A$ be the linear map that maps xg_0y to $x(g_0 - g)y$ and leaves all other monomials fixed ($x = 1$ or $y = 1$ is permissible). We call ρ_{xgy} a *reduction* modulo I. A polynomial $a \in A$ is called *reduced*, if a remains fixed under all reductions modulo I. Since every monomial in $x(g_0 - g)y$ is smaller than xg_0y, every polynomial can be transformed into a reduced polynomial with finitely many reductions. If there is only one reduced polynomial r into which a can be transformed, then a is called *uniquely reducible* and one sets $\rho_\infty(a) := r$.

- Let $a = xyz \in M$ and $g, h \in G$ with $g_0 = xy$ and $h_0 = yz$. If there exist compositions of reductions σ and τ modulo I with $\sigma(\rho_{gz}(a)) = \tau(\rho_{xh}(a))$, then we say "the overlap is resolvable".
- Now let $a = g_0 = xh_0y \in M$ with $g, h \in G$. If there exist compositions of reductions σ and τ modulo I with $\sigma(\rho_g(a)) = \tau(\rho_{xhy}(a))$, then we say "the inclusion is resolvable".



Lemma III.9.79 (Diamond Lemma[3])**.** *With the notation above, the following statements are equivalent:*

(1) All overlaps and inclusions are resolvable.

(2) All polynomials in A are uniquely reducible.

(3) The cosets of the reduced monomials form a K-basis of A/I.

Proof.

(1)⇒(2): We first show that the uniquely reducible polynomials form a subspace $R \subseteq A$. Obviously $0 \in R$. Let $a, b \in R$ and $\lambda \in K$. Let ρ, σ, τ be compositions of reductions such that $\rho(a + \lambda b)$, $\sigma\rho(a)$ and $\tau\sigma\rho(b)$ are reduced. Then

$$\rho(a + \lambda b) = \tau\sigma\rho(a + \lambda b) = \tau\sigma\rho(a) + \lambda\tau\sigma\rho(b) = \rho_\infty(a) + \lambda\rho_\infty(b).$$

Thus $a + \lambda b$ is uniquely reducible with $\rho_\infty(a + \lambda b) = \rho_\infty(a) + \lambda\rho_\infty(b)$. Hence R is a subspace and $\rho_\infty \colon A \to A$ is linear.

[3]The name results from the diagram above.

It now suffices to show that all monomials $a \in M$ are uniquely reducible. This is clear for $a = 1$. So let $a \neq 1$ and inductively assume all $b < a$ are uniquely reducible. Let $\sigma := \sigma_k \sigma_{k-1} \dots \sigma_1$ and $\tau := \tau_l \dots \tau_1$ be compositions of reductions such that $\sigma(a)$ and $\tau(a)$ are reduced. We must show $\sigma(a) = \tau(a)$. Wlog. let $\sigma_1(a) \neq a \neq \tau_1(a)$. Then $\sigma_1(a)$ and $\tau_1(a)$ are uniquely reducible by induction. In the case $\sigma_1(a) = \tau_1(a)$, it follows that $\sigma(a) = \tau(a)$. So let $\sigma_1(a) \neq \tau_1(a)$. Then one of the following cases occurs:

Case 1: $a = xg_0yh_0z$, $\sigma_1 = \rho_{xgyh_0z}$ and $\tau_1 = \rho_{xg_0yhz}$ with $g, h \in G$.
From the linearity of ρ_∞ it follows that

$$\begin{aligned}\sigma(a) &= \rho_\infty(\sigma_1(a)) = \rho_\infty(x(g_0 - g)yh_0z) = \rho_\infty(x(g_0 - g)y(h_0 - h)z) \\ &= \rho_\infty(xgy(h_0 - h)z) = \rho_\infty(\tau_1(a)) = \tau(a).\end{aligned}$$

Case 2: $a = xg_0yz = xwh_0z$, $\sigma_1 = \rho_{xgyz}$ and $\tau_1 = \rho_{xwhz}$ with $g, h \in G$.
Since overlaps are resolvable, there exist compositions of reductions σ' and τ' modulo I with $\sigma'(\rho_{gy}(g_0y)) = \tau'(\rho_{wh}(wh_0))$. One can now replace every reduction ρ_{rgs} in σ' and τ' by ρ_{xrgsz}. One then obtains $\sigma'(\sigma_1(a)) = \tau'(\tau_1(a))$. By induction it follows that

$$\sigma(a) = \rho_\infty(\sigma_1(a)) = \rho_\infty(\sigma'(\sigma_1(a))) = \rho_\infty(\tau'(\tau_1(a))) = \rho_\infty(\tau_1(a)) = \tau(a).$$

Case 3: $a = xg_0y = xwh_0vy$, $\sigma_1 = \rho_{xgy}$ and $\tau_1 = \rho_{xwhvy}$ with $g, h \in G$.
Since all inclusions are resolvable, there exist compositions of reductions σ' and τ' modulo I with $\sigma'(\rho_g(g_0)) = \tau'(\rho_{whv}(wh_0v))$. By multiplying from the left and right with x and y respectively as in Case 2, one obtains $\sigma'(\sigma_1(a)) = \tau'(\tau_1(a))$. As in Case 2, it follows that $\sigma(a) = \tau(a)$.

(2)⇒(3): For monomials x, y and $g \in G$, we have $xg_0y = x(g_0-g)y+xgy \equiv x(g_0-g)y \pmod I$. For all $a \in A$, we therefore have $\rho_\infty(a) \equiv a \pmod I$. It follows that $A = I+\rho_\infty(A)$. Every $a = \rho_\infty(a) \in I$ is a linear combination of elements of the form $xgy = xg_0y - x(g_0 - g)y$ with monomials x, y and $g \in G$. Because of $\rho_{xgy}(xgy) = 0$, it follows that $a = 0$, since ρ_∞ is well-defined and linear. Thus $A = I \oplus \rho_\infty(A)$ and the cosets of the reduced monomials form a basis of $A/I \cong \rho_\infty(A)$.

(3)⇒(1): Let $S \subseteq A$ be the subspace of all reduced polynomials. By assumption, $A = I \oplus S$. Let $a \in A$ and σ, τ be reductions modulo I. Then there exist compositions of reductions σ' and τ' with $\sigma'(\sigma(a)), \tau'(\tau(a)) \in S$. Since reductions do not change the coset modulo I, it follows on the other hand that $\sigma'\sigma(a) - \tau'\tau(a) \in I$. It follows that $\sigma'\sigma(a) = \tau'\tau(a)$. In particular, all overlaps and inclusions are resolvable. □

Remark III.9.80. One can view the basis obtained from the diamond lemma as a non-commutative version of a Gröbner basis.

Example III.9.81.

(i) Let $g_{ij} := X_iX_j - X_jX_i$ and $G := \{g_{ij} : j < i\}$. By applying the corresponding reductions, one can sort the X_i by indices. The reduced monomials are therefore $X_{i_1} \dots X_{i_k}$ with $i_1 \leq \dots \leq i_k$. Since g_0 is a product of two variables for all $g \in G$, there can be no inclusions. Every overlap has the form $X_iX_jX_k$ with $i > j > k$. This overlap is resolvable because of

$$\begin{aligned}X_iX_jX_k &\xrightarrow{\rho_{g_{ij}X_k}} X_jX_iX_k \xrightarrow{\rho_{X_jg_{ik}}} X_jX_kX_i \xrightarrow{\rho_{g_{jk}X_i}} X_kX_jX_i, \\ X_iX_jX_k &\xrightarrow{\rho_{X_ig_{jk}}} X_iX_kX_j \xrightarrow{\rho_{g_{ik}X_j}} X_kX_iX_j \xrightarrow{\rho_{X_kg_{ij}}} X_kX_jX_i.\end{aligned}$$

The diamond lemma shows $K\langle X_1, \dots\rangle/I \cong K[X_1, \dots]$.

(ii) Let $(X_1, X_2) = (X, Y)$ and $G := \{g\}$ with $g := Y^2 - XY - YX$. Here Y^3 is a non-resolvable overlap, since

$$Y^3 \xrightarrow{\rho_{gY}} XY^2 + YXY \xrightarrow{\rho_{Xg}} X^2Y + XYX + YXY,$$
$$Y^3 \xrightarrow{\rho_{Yg}} YXY + Y^2X \xrightarrow{\rho_{gX}} YXY + XYX + YX^2$$

are reduced, but not equal (other reductions are not possible).

Definition III.9.82. By $[a, b] := ab - ba$, $K\langle X_1, \ldots\rangle$ becomes a Lie algebra as is well known. Let L be a Lie algebra over K with basis $x_1, \ldots$ (finite or countable). For $i > j$, let $a_{ijk} \in K$ be the structure constants with $[x_i, x_j] = \sum_{k=1}^{\infty} a_{ijk}x_k$ (the sum is finite). Let $g_{ij} := [X_i, X_j] - \sum_{k=1}^{\infty} a_{ijk}X_k$ and $I := (g_{ij} : i > j) \trianglelefteq K\langle X_1, \ldots\rangle$ be the ordinary ideal generated by the g_{ij}. One calls

$$U(L) := K\langle X_1, \ldots\rangle / I$$

the *universal enveloping algebra* of L. The coset of X_i modulo I in $U(L)$ is denoted by $\overline{X_i}$. By construction, $L \to U(L)$, $x_i \mapsto \overline{X_i}$ defines a homomorphism of Lie algebras.

Theorem III.9.83 (Poincaré-Birkhoff-Witt)**.** *For every Lie algebra L, $\{\overline{X_{i_1} \ldots X_{i_k}} : k \in \mathbb{N}_0, i_1 \leq \ldots \leq i_k\}$ is a basis of $U(L)$.*

Proof. We apply the Diamond Lemma to the generating set $G := \{g_{ij} : i > j\}$ of $I \trianglelefteq K\langle X_1, \ldots\rangle$. Obviously $g := g_{ij}$ is normalized with $g_0 = X_iX_j$. One easily sees that the reduced monomials have the form $X_{i_1} \ldots X_{i_k}$ with $i_1 \leq \ldots \leq i_k$. Therefore, it suffices to show that overlaps and inclusions are resolvable. Inclusions cannot occur as in Example III.9.81, since all g_0 are a product of two variables. Overlaps have the form $a = X_iX_jX_k$ with $i > j > k$. We must show that one can reduce $\rho_{g_{ij}X_k}(a)$ and $\rho_{X_ig_{jk}}(a)$ to a common element. Let $\alpha\colon L \to K\langle X_1, \ldots, X_n\rangle$ be the linear map with $\alpha(x_i) = X_i$. Then $g_{ij} = X_iX_j - X_jX_i - \alpha([x_i, x_j])$ holds. It follows that

$$\begin{aligned}
a &\xrightarrow{\rho_{g_{ij}X_k}} X_jX_iX_k + \alpha([x_i, x_j])X_k \xrightarrow{\rho_{X_jg_{ik}}} X_jX_kX_i + X_j\alpha([x_i, x_k]) + \alpha([x_i, x_j])X_k \\
&\xrightarrow{\rho_{g_{jk}X_i}} X_kX_jX_i + \alpha([x_j, x_k])X_i + X_j\alpha([x_i, x_k]) + \alpha([x_i, x_j])X_k =: p, \\
a &\xrightarrow{\rho_{X_ig_{jk}}} X_iX_kX_j + X_i\alpha([x_j, x_k]) \xrightarrow{\rho_{g_{ik}X_j}} X_kX_iX_j + \alpha([x_i, x_k])X_j + X_i\alpha([x_j, x_k]) \\
&\xrightarrow{\rho_{X_kg_{ij}}} X_kX_jX_i + X_k\alpha([x_i, x_j]) + \alpha([x_i, x_k])X_j + X_i\alpha([x_j, x_k]) =: q \\
p - q &= [\alpha([x_j, x_k]), X_i] + [X_j, \alpha([x_i, x_k])] + [\alpha([x_i, x_j]), X_k] \\
&= [\alpha([x_j, x_k]), X_i] + [\alpha([x_k, x_i]), X_j] + [\alpha([x_i, x_j]), X_k].
\end{aligned}$$

Let $T \subseteq \mathbb{N}$ be the (finite) set of all indices t such that X_t occurs as a factor of a summand in p or q. For $\sigma := \prod_{\substack{s,t\in T\\ s>t}} \rho_{g_{st}}$ we have

$$\sigma([X_s, X_t]) = \begin{cases} \rho_{g_{st}}(X_sX_t) - X_tX_s = \alpha([x_s, x_t]) & \text{if } s > t, \\ X_sX_t - \rho_{g_{ts}}(X_tX_s) = -\alpha([x_t, x_s]) = \alpha([x_s, x_t]) & \text{if } s < t, \\ 0 = \alpha([x_s, x_t]) & \text{if } s = t. \end{cases}$$

It follows that

$$\sigma\big([\alpha([x_j, x_k]), X_i]\big) = \sum_{l=1}^{\infty} a_{jkl}\sigma([X_l, X_i]) = \sum_{l=1}^{\infty} a_{jkl}\alpha([x_l, x_i]) = \alpha\Big(\Big[\sum_{l=1}^{\infty} a_{jkl}x_l, x_i\Big]\Big) = \alpha\big([[x_j, x_k], x_i]\big).$$

This shows

$$\sigma(p) - \sigma(q) = \sigma(p-q) = \alpha\big([[x_j, x_k], x_i] + [[x_k, x_i], x_j] + [[x_i, x_j], x_k]\big) = 0$$

by the Jacobi identity. □

Corollary III.9.84. *For every Lie algebra L with basis $x_1, \ldots$ the linear map $L \to U(L)$, $x_i \mapsto \overline{X_i}$ is a monomorphism of Lie algebras.*

Remark III.9.85.

(i) Let L be a Lie algebra with an arbitrary basis B (possibly uncountable). By the Well-Ordering Theorem, there exists a total order on B. In this way, the Poincaré-Birkhoff-Witt Theorem can also be proven for L.

(ii) In the following, we will often regard L as a Lie subalgebra of $U(L)$.

Theorem III.9.86 (Universal Property)**.** *Let L be a Lie algebra with basis $x_1, \ldots$ and A a K-algebra. Then every homomorphism of Lie algebras $L \to A$ has exactly one extension to a homomorphism of algebras $U(L) \to A$.*

Proof. Let $f\colon L \to A$ be a homomorphism of Lie algebras. We first define an algebra homomorphism $\hat{F}\colon K\langle X_1, \ldots\rangle \to A$ by $\hat{F}(X_i) := f(x_i)$. It suffices to show $g_{ij} \in \operatorname{Ker}(\hat{F})$. It holds that

$$\hat{F}(g_{ij}) = [f(x_i), f(x_j)] - \sum_{k=1}^{\infty} a_{ijk} f(x_k) = f\Big([x_i, x_j] - \sum_{k=1}^{\infty} a_{ijk} x_k\Big) = 0.$$

The uniqueness of F is obvious, since every element in $U(L)$ is a sum of monomials of the $\overline{X_i}$. □

Remark III.9.87. Suppose the universal property also holds for a K-algebra $U \supseteq L$. Then one can extend the embeddings $L \hookrightarrow U(L)$ and $L \hookrightarrow U$ to homomorphisms $\Phi\colon U \to U(L)$ and $\Psi\colon U(L) \to U$ respectively. Now $\Phi\Psi$ is an extension of $L \hookrightarrow U(L)$. On the other hand, $\mathrm{id}_{U(L)}$ is the only such extension. This shows $\Phi\Psi = \mathrm{id}_{U(L)}$ and analogously $\Psi\Phi = \mathrm{id}_U$. Thus $U(L) \cong U$ is uniquely determined by the universal property. In particular, $U(L)$ does not depend on the choice of the basis of L.

Definition III.9.88. The *free Lie algebra of rank n* is the Lie subalgebra $\mathfrak{L}_n$ of $K\langle X_1, \ldots, X_n\rangle$ generated by $X_1, \ldots, X_n$. As a vector space, $\mathfrak{L}_n$ is spanned by all Lie brackets $[X_{i_1}, \ldots, X_{i_k}]$.

Theorem III.9.89.

(i) Every Lie algebra L with n generators is isomorphic to a quotient algebra of $\mathfrak{L}_n$.

(ii) $U(\mathfrak{L}_n) \cong K\langle X_1, \ldots, X_n\rangle$.

Proof.

(i) We can extend the set of generators $x_1, \ldots, x_n$ of L to a (at most) countable basis $x_1, \ldots$. By Corollary III.9.84 there exists a monomorphism $\varphi\colon L \to U(L)$. Let $I = (g_{ij}) \trianglelefteq K\langle X_1, \ldots\rangle$ as in Definition III.9.82. One easily sees that φ maps exactly onto the cosets of $\mathfrak{L}_n$ modulo I. Thus $L \cong \varphi(L) = (\mathfrak{L}_n + I)/I \cong \mathfrak{L}_n/(\mathfrak{L}_n \cap I)$.

(ii) Let $\varphi\colon \mathfrak{L}_n \to A$ be a homomorphism into an ordinary algebra A. Because of

$$\varphi(X_iX_j) - \varphi(X_jX_i) = \varphi([X_i, X_j]) = [\varphi(X_i), \varphi(X_j)] = \varphi(X_i)\varphi(X_j) - \varphi(X_j)\varphi(X_i)$$

for $1 \leq i, j \leq n$, φ can be extended to exactly one homomorphism $K\langle X_1, \ldots, X_n\rangle \to A$. The claim follows from Remark III.9.87. □

Example III.9.90. Let L be a Lie algebra with n generators and $\Phi\colon \mathfrak{L}_n \to L$ an epimorphism as in Theorem III.9.89. For $k \in \mathbb{N}$ there exists an epimorphism

$$\mathfrak{L}_n^{[k]} \xrightarrow{\Phi} L^{[k]} \to L^{[k]}/L^{[k+1]},$$

with $\mathfrak{L}_n^{[k+1]}$ in the kernel. Therefore $L^{[k]}/L^{[k+1]}$ is isomorphic to a factor algebra of $\mathfrak{L}_n^{[k]}/\mathfrak{L}_n^{[k+1]}$. The following theorem provides an optimal estimate for $\dim(L^{[}k]/L^{[k+1]})$.

Theorem III.9.91 (Witt's formula)**.** *For $k \in \mathbb{N}$ we have*

$$\boxed{\dim\bigl(\mathfrak{L}_n^{[k]}/\mathfrak{L}_n^{[k+1]}\bigr) = \frac{1}{k}\sum_{d|k}\mu(d)n^{k/d},}$$

where μ is the Möbius function.

Proof. For $k \in \mathbb{N}$ let $b_{k,1} + \mathfrak{L}_n^{[k+1]}, \ldots, b_{k,d_k} + \mathfrak{L}_n^{[k+1]}$ be a basis of $\mathfrak{L}_n^{[k]}/\mathfrak{L}_n^{[k+1]}$. According to Poincaré-Birkhoff-Witt and Theorem III.9.89, $A := K\langle X_1, \ldots, X_n\rangle$ has a basis consisting of elements of the form

$$b := b_{i_1,j_1} \ldots b_{i_l,j_l},$$

where the pairs $(i_1, j_1), \ldots, (i_l, j_l)$ are ordered lexicographically. Inductively one sees that b is a homogeneous polynomial of degree $i_1 + \ldots + i_l$. Let A_k be the subspace of A spanned by the monomials $X_{i_1} \ldots X_{i_k}$. Obviously $\dim A_k = n^k$ holds. On the other hand, b lies in A_k if and only if $i_1 + \ldots + i_l = k$ holds. Each of the d_i basis elements $b_{i,j}$ can be chosen s times and then contributes si to the degree k. The number of $b \in A_k$ is therefore the coefficient of X^k in the formal power series[4]

$$(1 + X + X^2 + \ldots)^{d_1}(1 + X^2 + X^4 + \ldots)^{d_2} \ldots = \prod_{i=1}^{\infty}(1 - X^i)^{-d_i}.$$

Overall one obtains

$$(1 - nX)^{-1} = \sum_{k=0}^{\infty} n^k X^k = \sum_{k=0}^{\infty} \dim(A_k)X^k = \prod_{i=1}^{\infty}(1 - X^i)^{-d_i}.$$

Taking the logarithm yields

$$\sum_{k=1}^{\infty}\frac{n^k}{k}X^k = -\log(1 - nX) = -\sum_{i=1}^{\infty} d_i \log(1 - X^i) = \sum_{i=1}^{\infty}\sum_{k=1}^{\infty}\frac{d_i}{k}X^{ik} = \sum_{k=1}^{\infty}\sum_{l|k}\frac{d_l l}{k}X^k.$$

A comparison of coefficients shows

$$n^k = \sum_{l|k} d_l l$$

for all $k \in \mathbb{N}$. The claim now follows by Möbius inversion. □

[4] See lecture notes Combinatorics

Example III.9.92.

(i) For $n = 2$, the following dimensions result

k	1	2	3	4	5	6	7	8
$\dim\big(\mathfrak{L}_2^{[k]}/\mathfrak{L}_2^{[k+1]}\big)$	2	1	2	3	6	9	18	30

The first basis elements are

$$X, Y, [X,Y], [X,X,Y], [Y,X,Y], [X,X,X,Y], [X,Y,X,Y] = [Y,X,X,Y], [Y,Y,X,Y]$$

according to Exercise III.42. A nilpotent Lie algebra with two generators and nilpotency class 4 thus has at most dimension $2+1+2+3 = 8$. Analogous statements hold for p-groups (Exercise III.53).

(ii) For $k = 2$, it holds that $\dim\big(\mathfrak{L}_n^{[2]}/\mathfrak{L}_n^{[3]}\big) = \binom{n}{2}$. The Lie brackets $[X_i, X_j]$ with $i < j$ form a corresponding basis.

(iii) For $p \in \mathbb{P}$, $\dim\big(\mathfrak{L}_p^{[k]}/\mathfrak{L}_p^{[k+1]}\big)$ is the number of irreducible polynomials of degree k in $\mathbb{F}_p[X]$ (see Exercise I.61).

Theorem III.9.93 (Iwasawa)**.** *Let* $\operatorname{char} K > 0$ *and* L *be a Lie algebra. Then there exists a faithful representation* $L \to \mathfrak{gl}(V)$.

Proof (Jacobson). Let $p := \operatorname{char} K$ and $d := \dim L$. For $x, y \in L$, $\operatorname{ad}_x^p(y) = x^p y - y x^p$ holds according to Exercise III.46 (even if $p = 2$), i. e. $\operatorname{ad}_x^p = \operatorname{ad}_{x^p}$. Let $\mu_x \in K[X]$ be the minimal polynomial of ad_x. For $i \in \mathbb{N}_0$ there exist $\gamma_i, \rho_i \in K[X]$ with $X^{p^i} = \mu_x \gamma_i + \rho_i$ with $\deg \rho_i < \deg \mu_x \leq d$. Furthermore, there exist $a_0, \ldots, a_d \in K$ (not all 0) with $\sum_{i=0}^d a_i \rho_i = 0$. For the polynomial $\sigma_x := \sum_{i=0}^d a_i X^{p^i} = \mu_x \sum_{i=0}^d a_i \gamma_i$ it holds that

$$\operatorname{ad}_{\sigma_x(x)} = \sum_{i=0}^{d} a_i \operatorname{ad}_x^{p^i} = \sigma_x(\operatorname{ad}_x) = 0,$$

i. e. $\sigma_x(x) \in \mathrm{Z}(L)$.

Let $x_1, \ldots, x_d$ be a basis of L, $p^{k_i} := \deg \sigma_{x_i}$ and $z_i := \sigma_{x_i}(x_i) \in \mathrm{Z}(L)$ as above. According to Corollary III.9.84 we can consider L as a Lie subalgebra of the universal enveloping algebra $U(L)$. In doing so, we identify x_i with $\overline{X_i}$. According to Poincaré-Birkhoff-Witt, $U(L)$ is spanned by the elements

$$\alpha := z_1^{b_1} \ldots z_d^{b_d} x_1^{c_1} \ldots x_d^{c_d} = z_1^{b_1} x_1^{c_1} \ldots z_d^{b_d} x_d^{c_d} \tag{III.9.1}$$

with $b_i \geq 0$ and $0 \leq c_i < p^{k_i}$ for $i = 1, \ldots, d$. Let $r(\alpha) := b_1 p^{k_1} + c_1 + \ldots + b_d p^{k_d} + c_d$ and $V_{\alpha(r)}$ be the subspace of $U(L)$ spanned by the elements $x_1^{e_1} \ldots x_d^{e_d}$ with $e_1 + \ldots + e_d < r(\alpha)$. Then

$$\alpha \equiv x_1^{b_1 p^{k_1} + c_1} \ldots x_d^{b_d p^{k_d} + c_d} \pmod{V_{\alpha(r)}}.$$

Let $\beta := \lambda_1 \alpha_1 + \ldots + \alpha_m \alpha_m = 0$ with $\lambda_i \in K$ and pairwise distinct α_i as in (III.9.1) for $i = 1, \ldots, m$. Then the exponent tuples $(b_j p^{k_j} + c_j)_j$ of the α_i are also pairwise distinct. Let $r := \max\{r(\alpha_i) : i = 1, \ldots, m\} = r(\alpha_s)$. From $\beta \equiv 0 \pmod{V_r}$ it now follows easily that $\lambda_s = 0$. Thus the elements in (III.9.1) form a basis of $U(L)$.

Let $S = (z_1, \ldots, z_d) \subseteq \mathrm{Z}(U(L))$ be the ordinary ideal in $U(L)$ generated by the elements $z_1, \ldots, z_d$. Then the elements $x_1^{c_1} \ldots x_d^{c_d} + S$ with $0 \leq c_i < p^{k_i}$ for $i = 1, \ldots, d$ form a basis of $U := U(L)/S$. In particular, $\dim U < \infty$ and $L \cap S = 0$. By left multiplication one obtains a faithful representation $L \to \mathfrak{gl}(U)$. □

Lemma III.9.94. *Let L be a Lie algebra and $I \trianglelefteq L$. Then the adjoint representation* $\mathrm{ad}\colon L \to \mathfrak{gl}(I)$ *can be extended to a representation* $\nabla\colon L \to \mathfrak{gl}(U(I))$ *with* $\nabla_x(ab) = \nabla_x(a)b + a\nabla_x(b)$ *for all* $x \in L$ *and* $a, b \in U(I)$.

Proof. Let $x_1, \dots, x_n$ be a basis of $I \subseteq U(I)$. According to Poincaré-Birkhoff-Witt, there exists exactly one linear map $\nabla_y\colon U(I) \to U(I)$ with

$$\nabla_y(x_{i_1} \dots x_{i_r}) = \sum_{k=1}^{r} x_{i_1} \dots x_{i_{k-1}} \mathrm{ad}_y(x_{i_k}) x_{i_{k+1}} \dots x_{i_r} \tag{III.9.2}$$

for $1 \le i_1 \le \ldots \le i_r \le n$. Obviously, ∇_y is an extension of ad_y and $\nabla\colon L \to \mathfrak{gl}(U(I))$, $y \mapsto \nabla_y$ is linear. For $y, z \in L$ it holds that

$$\begin{aligned}
\nabla_{[y,z]}(x_{i_1} \dots x_{i_r}) &= \sum_{k=1}^{r} x_{i_1} \dots x_{i_{k-1}} (\mathrm{ad}_y \mathrm{ad}_z(x_{i_k}) - \mathrm{ad}_z \mathrm{ad}_y(x_{i_k})) x_{i_{k+1}} \dots x_{i_r} \\
&= \sum_{k,l=1}^{r} x_{i_1} \dots \mathrm{ad}_y(x_{i_k}) \dots \mathrm{ad}_z(x_{i_l}) \dots x_{i_r} - \sum_{k,l=1}^{r} x_{i_1} \dots \mathrm{ad}_z(x_{i_k}) \dots \mathrm{ad}_y(x_{i_l}) \dots x_{i_r} \\
&= \nabla_y \nabla_z(x_{i_1} \dots x_{i_r}) - \nabla_z \nabla_y(x_{i_1} \dots x_{i_r}).
\end{aligned}$$

Therefore, ∇ is a representation. For $i < j$ it holds that

$$\begin{aligned}
\nabla_y(x_j x_i) &= \nabla_y(x_i x_j + [x_j, x_i]) = \mathrm{ad}_y(x_i) x_j + x_i \mathrm{ad}_y(x_j) + \mathrm{ad}_y([x_j, x_i]) \\
&= x_j \mathrm{ad}_y(x_i) + \mathrm{ad}_y(x_j) x_i + [\mathrm{ad}_y(x_i), x_j] + [x_i, \mathrm{ad}_y(x_j)] + \mathrm{ad}_y([x_j, x_i]) \\
&= x_j \mathrm{ad}_y(x_i) + \mathrm{ad}_y(x_j) x_i + [[y, x_i], x_j] + [[x_j, y], x_i] + [[x_i, x_j], y] = x_j \mathrm{ad}_y(x_i) + \mathrm{ad}_y(x_j) x_i.
\end{aligned}$$

We show (III.9.2) for arbitrary $i_1, \dots, i_r$ by induction first on r and then on the number of inversions of the permutation $\pi(j) = i_j$. Wlog. let $i_k > i_{k+1}$. Then it holds that

$$\begin{aligned}
\nabla_y(x_{i_1} \dots x_{i_r}) &= \nabla_y(x_{i_1} \dots x_{i_{k+1}} x_{i_k} \dots x_{i_r} + x_{i_1} \dots [x_{i_k}, x_{i_{k+1}}] \dots x_{i_r}) \\
&= \sum_{l=1}^{k-1} x_{i_1} \dots \mathrm{ad}_y(x_{i_l}) \dots x_{i_k} x_{i_{k+1}} \dots x_{i_r} + x_{i_1} \dots \nabla_y\big(x_{i_{k+1}} x_{i_k} + [x_{i_k}, x_{i_{k+1}}]\big) \dots x_{i_r} \\
&\quad + \sum_{l=k+2}^{r} x_{i_1} \dots x_{i_k} x_{i_{k+1}} \dots \mathrm{ad}_y(x_{i_l}) \dots x_{i_r} \\
&= \sum_{l=1}^{r} x_{i_1} \dots x_{i_{l-1}} \mathrm{ad}_y(x_{i_l}) x_{i_{l+1}} \dots x_{i_r}
\end{aligned}$$

as claimed. From this, $\nabla_y(ab) = \nabla_y(a)b + a\nabla_y(b)$ follows easily for all $a, b \in U(I)$. □

Remark III.9.95. In the following theorem, we construct a representation $\Delta\colon L \to \mathfrak{gl}(V)$ that maps the nilradical to a nilpotent ideal of the ordinary algebra $\mathfrak{gl}(V)$, i.e., $\Delta(\mathrm{N}(L))^n = \{\Delta(x_1) \dots \Delta(x_n) : x_1, \dots, x_n \in \mathrm{N}(L)\} = 0$ holds for some $n \in \mathbb{N}$.

Theorem III.9.96 (Ado)**.** *Let* $\operatorname{char} K = 0$ *and L be a Lie algebra. Then there exists a faithful representation* $\Delta\colon L \to \mathfrak{gl}(V)$ *with* $\Delta(\mathrm{N}(L))^n = 0$ *for some* $n \in \mathbb{N}$.

Proof. We construct inductively a representation $\Delta\colon L \to \mathfrak{gl}(V)$ with $\operatorname{Ker}(\Delta) \cap \operatorname{Z}(L) = 0$ and $\Delta(\operatorname{N}(L))^n = 0$ for some $n \in \mathbb{N}$. Then the representation

$$\Delta \oplus \operatorname{ad}\colon L \to \mathfrak{gl}(V \times L), \qquad x \mapsto \Delta(x) \oplus \operatorname{ad}_x$$

is faithful. Let $\operatorname{N}(L)^{[k]} = 0$. For all $x \in \operatorname{N}(L)$ and $y \in L$ it then holds that $\operatorname{ad}_x^k(y) = [x, [x, \dots, [x, y] \dots]] = 0$, i. e. ad_x is nilpotent. By Engel, $\operatorname{ad}(\operatorname{N}(L))^n = 0$ for some $n \in \mathbb{N}$. Thus also $(\Delta \oplus \operatorname{ad})(\operatorname{N}(L))^n = 0$ if n is large enough. Therefore it suffices to construct Δ.

Step 1: L is abelian.
We consider the injective map $\Delta\colon L \to \mathfrak{gl}(L \times K)$ with $\Delta(x)(v, \lambda) := (\lambda x, 0)$ for $x, v \in L$ and $\lambda \in K$. For $x, y \in L$ we have $\Delta(x)(\Delta(y)(v, \lambda)) = \Delta(x)(\lambda y, 0) = 0$ and $\Delta([x, y]) = \Delta(0) = 0 = [\Delta(x), \Delta(y)]$. Thus Δ is a faithful representation with $\Delta(L)^2 = 0$.

Step 2: L is nilpotent.
According to Remark III.9.25 there exists a sequence of ideals

$$\operatorname{Z}(L) = L_0 \trianglelefteq L_1 \trianglelefteq \dots \trianglelefteq L_m =: L$$

with $\dim(L_i / L_{i-1}) = 1$ for $i = 1, \dots, m$. Inductively there exists a representation $\Delta_k\colon L_k \to \mathfrak{gl}(V_k)$ with $\operatorname{Ker}(\Delta_k) \cap \operatorname{Z}(L) = 0$ and $\Delta_k(L_k)^{n_k} = 0$ (for $k = 0$ the claim follows from Step 1). By the universal property, Δ_k can be extended to a representation $\hat{\Delta}_k\colon U(L_k) \to \mathfrak{gl}(V_k)$. Here we identify a basis $x_1, \dots, x_d$ of L_k as usual with $\overline{X_1}, \dots, \overline{X_d} \in U(L_k)$.

Let S be the (ordinary) ideal of the (ordinary) algebra $U(L_k)$ generated by the elements $x_{i_1} \dots x_{i_r}$ with $r \geq n_k$. We set $U := U(L_k)/S$ and identify x_i with $x_i + S$. By Poincaré-Birkhoff-Witt, $\dim U < \infty$. Because $us \in S$ for $u \in U(L_k)$ and $s \in S$, U becomes a Lie module of L_k via left multiplication. Let $L_{k+1} = L_k \oplus Y$ with a 1-dimensional (abelian) subalgebra Y. We consider the representation $\nabla\colon Y \to \mathfrak{gl}(U(L_k))$ from Lemma III.9.94 (restricted to Y). Because $\nabla_y(S) \subseteq S$ for $y \in Y$, $\nabla\colon Y \to \mathfrak{gl}(U)$ is also a well-defined representation. For $u \in U$, $x \in L_k$ and $y \in Y$ we define

$$(x + y)u := xu + \nabla_y(u).$$

For $x' \in I$ and $y' \in Y$ it holds that

$$\begin{aligned}(x + y)((x' + y')u) - (x' + y')((x + y)u) &= (x + y)(x'u + \nabla_{y'}(u)) - (x' + y')(xu + \nabla_y(u)) \\ &= xx'u + x\nabla_{y'}(u) + \nabla_y(x'u) + \nabla_y\nabla_{y'}(u) - x'xu - x'\nabla_y(u) - \nabla_{y'}(xu) - \nabla_{y'}\nabla_y(u) \\ &= [x, x']u + (x\nabla_{y'}(u) - \nabla_{y'}(xu)) + (\nabla_y(x'u) - x'\nabla_y(u)) + [y, y']u.\end{aligned}$$

For $x = x_s$ and $u = x_{i_1} \dots x_{i_r}$ it holds that

$$x\nabla_{y'}(u) - \nabla_{y'}(xu) = -[y', x_s]x_{i_1} \dots x_{i_r} = [x, y']u.$$

This shows

$$(x + y)((x' + y')u) - (x' + y')((x + y)u) = \big([x, x'] + [x, y'] + [y, x'] + [y, y']\big)u = [x + y, x' + y']u.$$

In this way one obtains a representation $\Delta_{k+1}\colon L_{k+1} \to \mathfrak{gl}(U)$.

By construction $S \subseteq \operatorname{Ker}(\hat{\Delta}_k)$. One can therefore view $\hat{\Delta}_k$ as a representation $\hat{\Delta}_k\colon U \to \mathfrak{gl}(V_k)$. Let $x \in \operatorname{Ker}(\Delta_{k+1}) \cap \operatorname{Z}(L) \subseteq L_k$. Then $x1_U = 0$ and $x \in S \cap \operatorname{Z}(L) \subseteq \operatorname{Ker}(\Delta_k) \cap \operatorname{Z}(L) = 0$. This shows $\operatorname{Ker}(\Delta_{k+1}) \cap \operatorname{Z}(L) = 0$. For $x \in L_k$ and $u \in U$ it holds that $x^{n_k}u = 0$. Each application of ∇_y replaces a factor $x \in L^{[l]}$ by $[y, x] \in L^{[l+1]}$. Since L is nilpotent, $\nabla_y^t = 0$ for some $t \in \mathbb{N}$. For $n_{k+1} := \max\{n_k, t\}$ it thus also holds that $\Delta_{k+1}(L_{k+1}))^{n_{k+1}} = 0$.

Step 3: L is solvable.
Let $N := \mathrm{N}(L)$. By Corollary III.9.36 we have $L' \subseteq N$. Thus there exists a sequence $N = L_0 \trianglelefteq \ldots \trianglelefteq L_m =: L$ with $\dim(L_i/L_{i-1}) = 1$ for $i = 1, \ldots, m$. For $0 \leq k \leq m$ we have

$$[L, \mathrm{N}(L_k)] \leq L' \leq N \leq \mathrm{N}(L_k).$$

Thus $\mathrm{N}(L_k)$ is a nilpotent ideal of L and $\mathrm{N}(L_k) = N$. Inductively (or by Step 2) there exists a representation $\Delta_k \colon L_k \to \mathfrak{gl}(V_k)$ with $\mathrm{Ker}(\Delta_k) \cap \mathrm{Z}(L) = 0$ and $\Delta_k(N)^{n_k} = 0$. This extends to $\hat{\Delta}_k \colon U(L_k) \to \mathfrak{gl}(V_k)$. Unlike in Step 2, this time let S be the ordinary ideal of $U(L_k)$ generated by $\mathrm{Ker}(\hat{\Delta}_k)$ and N. Because $N^{n_k} \subseteq \mathrm{Ker}(\hat{\Delta}_k)$, it holds that $S^{n_k} \subseteq \mathrm{Ker}(\hat{\Delta}_k)$. Let $U := U(L_k)/S^{n_k}$. One then again obtains a well-defined representation $\hat{\Delta}_k \colon U \to \mathfrak{gl}(V_k)$. Let $L_{k+1} = L_k \oplus Y$. We again use the representation $\nabla \colon Y \to \mathfrak{gl}(U(L_k))$ from Lemma III.9.94. The application of ∇_y to a monomial $x_{i_1} \ldots x_{i_r}$ replaces each factor x_{i_l} by $[y, x_{i_l}] \in N$. This shows $\nabla_y(U(L_k)) \subseteq S$. Because $\nabla_y(st) = \nabla_y(s)t + s\nabla_y(t)$ for $s, t \in S$, it also holds that $\nabla_y(S^{n_k}) \subseteq S^{n_k}$. Consequently $\nabla \colon Y \to \mathfrak{gl}(U)$ is well-defined. One can thus construct a representation $\Delta_{k+1} \colon L_{k+1} \to \mathfrak{gl}(U)$ as in Step 2. Certainly $\Delta_{k+1}(N)^{n_k} = 0$. Let $x \in \mathrm{Ker}(\Delta_{k+1}) \cap \mathrm{Z}(L)$. Then $x \in S^{n_k} \cap \mathrm{Z}(L) \subseteq \mathrm{Ker}(\Delta_k) \cap \mathrm{Z}(L) = 0$. Therefore $\mathrm{Ker}(\Delta_{k+1}) \cap \mathrm{Z}(L) = 0$.

It remains to show $\dim U < \infty$. Let $\mu_i \in K[X]$ be the minimal polynomial of $\Delta_k(x_i) \in \mathfrak{gl}(V_k)$ and $d_i := \deg \mu_i$. Then $\mu_i(x_i)^{n_k} \in \mathrm{Ker}(\Delta_k)^{n_k} \subseteq S^{n_k}$. One can thus replace $x_i^{n_k d_i}$ by a polynomial of smaller degree modulo S^{n_k}. By Poincaré-Birkhoff-Witt, $\dim U < \infty$.

Step 4: L is arbitrary.
By Levi there exists a semisimple subalgebra $Y \leq L$ with $L = \mathrm{J}(L) \oplus Y$. By Step 3 there exists a representation $\Gamma \colon \mathrm{J}(L) \to \mathfrak{gl}(V)$ with $\mathrm{Ker}(\Gamma) \cap \mathrm{Z}(L) = 0$ and $\Gamma(\mathrm{J}(L))^n = 0$ for some $n \in \mathbb{N}$. With the same reasoning as in Step 3 one constructs a representation Δ of L with the desired properties. □

Theorem III.9.97. *Every Lie algebra possesses a faithful representation.*

Proof. Follows from Theorem III.9.93 and Theorem III.9.96. □

III.10 Valuation Rings

Remark III.10.1. In the representation theory of finite groups, we have seen that the choice of the underlying field plays a crucial role (both the characteristic and the existence of roots of unity). Valuation rings serve to transport representations from one field to another field. The irreducible representations of $G = S_3$ over $\mathbb{C}$, for example, can be realized over $\mathbb{Z}$ and subsequently reduced modulo a prime number p, so that one obtains representations over $\mathbb{F}_p$ (irreducible representations do not, in general, remain irreducible in this process). For arbitrary groups, one must construct larger rings with corresponding properties. This leads to complete normed spaces with interesting and at the same time unusual analytic convergence behavior.

Definition III.10.2. A (*multiplicative*) *valuation* of an integral domain R is a map $\nu\colon R \to \mathbb{R}$ with the following properties:

- $\nu(x) \geq 0$ and $\nu(x) = 0 \iff x = 0$ (*positive definite*),
- $\nu(xy) = \nu(x)\nu(y)$ (*multiplicative*),
- $\nu(x + y) \leq \nu(x) + \nu(y)$ (*subadditive* or *triangle inequality*)

for all $x, y \in R$. One calls ν

- *complete*, if R with the norm $|x| := \nu(x)$ is a complete normed space.
- *archimedean*, if there exists an $n \in \mathbb{N}$ with $\nu(n \cdot 1) > 1$.
- *ultrametric*, if $\nu(x + y) \leq \max\{\nu(x), \nu(y)\}$ holds for all $x, y \in R$.

Example III.10.3.

(i) Every integral domain R possesses the *trivial* valuation ν with $\nu(x) = 1$ for all $x \in R \setminus \{0\}$. It is complete, archimedean, and ultrametric. Finite fields K possess only the trivial valuation, because from $\nu(x)^{|K|-1} = \nu(x^{|K|-1}) = 1$ it follows that $\nu(x) = 1$ for $x \in K^\times$.

(ii) Every subring $R \subseteq \mathbb{C}$ possesses the *euclidean* valuation $\nu(x) := |x| = \sqrt{x\overline{x}}$. It is archimedean and, as is well known, complete for $R \in \{\mathbb{R}, \mathbb{C}\}$.

(iii) For $x = \pm \prod_{p \in \mathbb{P}} p^{a_p} \in \mathbb{Z} \setminus \{0\}$ with $a_p \in \mathbb{N}_0$, $\nu_p(x) := p^{-a_p}$ defines the ultrametric *p-adic* valuation on $\mathbb{Z}$.

(iv) For $\alpha = \sum_{k=0}^{\infty} a_k X^k \in R[X] \setminus \{0\}$, $\nu(\alpha) := 2^{-\min\{k : a_k \neq 0\}}$ defines an ultrametric valuation on $R[X]$ (one can replace 2 by any other number > 1). The same construction also works for the ring $R[[X]]$ of formal power series from Exercise II.30.

(v) Let R be a Dedekind domain with prime ideal $P \neq 0$. According to Theorem II.11.29, the principal ideal (x) for $x \in R \setminus \{0\}$ possesses a unique prime ideal factorization $(x) = \prod_{Q \in \operatorname{Spec}(\mathbb{Z}_K)} Q^{a_Q}$ with $a_Q \in \mathbb{N}_0$. Then $\nu_P(x) := 2^{-a_P}$ defines a valuation on R. If R is the ring of integers of a number field, then $\nu_P(x) := |R : P|^{-a_P}$ yields the *P-adic* valuation as a generalization of the p-adic valuation (according to Theorem II.11.16, $|R : P| < \infty$).

(vi) Let K be a field with valuation ν and $\sigma \in \mathrm{Aut}(K)$. Then $K \to \mathbb{R}$, $x \mapsto \nu(\sigma(x))$ is also a valuation.

Remark III.10.4. Let ν be a valuation of R.

(i) Because of $\nu(-1) > 0$ and $\nu(-1)^2 = \nu((-1)^2) = \nu(1) = 1$, it holds that $\nu(-1) = 1$. More generally, $\nu(-x) = \nu(x)$ for $x \in K$.

(ii) Because of $\nu(x) = \nu(x-y+y) \leq \nu(x-y)+\nu(y)$, it holds that $|\nu(x)-\nu(y)| \leq \nu(x-y)$ for $x, y \in R$. If the sequence $(x_n)_n$ in R converges to x with respect to ν, then $|\nu(x) - \nu(x_n)| \leq \nu(x - x_n) \to 0$ as $n \to \infty$ and

$$\lim_{n\to\infty} \nu(x_n) = \nu\Big(\lim_{n\to\infty} x_n\Big) = \nu(x),$$

i. e. ν is continuous with respect to the Euclidean norm in $\mathbb{R}$.

(iii) The ultrametric inequality $\nu(x + y) \leq \max\{\nu(x), \nu(y)\}$ implies the triangle inequality.

(iv) If ν is ultrametric and $\nu(x) < \nu(y)$, then

$$\nu(y) = \nu(x + y - x) \leq \max\{\nu(x + y), \nu(x)\} \leq \max\{\nu(x), \nu(y)\} = \nu(y).$$

This shows $\nu(x + y) = \nu(y)$. Formulated geometrically: All triangles are isosceles.

(v) In some books, one uses *additive* valuations $\nu\colon R \to \mathbb{R} \cup \{\infty\}$ with the axioms

- $\nu(x) = \infty \iff x = 0$,
- $\nu(xy) = \nu(x) + \nu(y)$,
- $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$

for all $x, y \in R$. Under these assumptions, $R \to \mathbb{R}$, $x \mapsto 2^{-\nu(x)}$ is an ultrametric multiplicative valuation and vice versa. Archimedean valuations are not taken into account in this way.

Lemma III.10.5. *Every valuation ν of an integral domain R can be uniquely extended to a valuation $\hat{\nu}$ on the quotient field $Q(R)$. In this case, $\hat{\nu}\big(\frac{x}{y}\big) = \frac{\nu(x)}{\nu(y)}$ holds for $\frac{x}{y} \in Q(R)$. If ν is Archimedean (resp. ultrametric), then so is $\hat{\nu}$.*

Proof. For $\frac{x}{y} \in Q(R) =: K$, we have $y \neq 0$ and $\nu(y) \neq 0$. If $\frac{x}{y} = \frac{a}{b}$ holds in K, then $\nu(x)\nu(b) = \nu(xb) = \nu(ya) = \nu(y)\nu(a)$. Thus $\hat{\nu}\colon K \to \mathbb{R}$ is well-defined and obviously also positive definite and multiplicative. For arbitrary $\frac{x}{y}, \frac{a}{b} \in K$, it holds that

$$\hat{\nu}\Big(\frac{x}{y} + \frac{a}{b}\Big) = \frac{\nu(xb + ya)}{\nu(yb)} \leq \frac{\nu(x)\nu(b) + \nu(y)\nu(a)}{\nu(y)\nu(b)} = \frac{\nu(x)}{\nu(y)} + \frac{\nu(a)}{\nu(b)} = \hat{\nu}\Big(\frac{x}{y}\Big) + \hat{\nu}\Big(\frac{a}{b}\Big).$$

Therefore $\hat{\nu}$ is a valuation of K. For any other extension $\hat{\nu}'$ of ν, it holds that

$$\nu(x) = \hat{\nu}'(x) = \hat{\nu}'\Big(\frac{x}{y}\Big)\hat{\nu}'(y) = \hat{\nu}'\Big(\frac{x}{y}\Big)\nu(y)$$

and $\hat{\nu}'\big(\frac{x}{y}\big) = \frac{\nu(x)}{\nu(y)} = \hat{\nu}\big(\frac{x}{y}\big)$.

If ν is archimedean, then so is $\hat{\nu}$. If ν is ultrametric, then it holds that

$$\hat{\nu}\Big(\frac{x}{y} + \frac{a}{b}\Big) = \frac{\nu(xb + ya)}{\nu(yb)} \leq \frac{\max\{\nu(x)\nu(b), \nu(y)\nu(a)\}}{\nu(y)\nu(b)} = \max\Big\{\frac{\nu(x)}{\nu(y)}, \frac{\nu(a)}{\nu(b)}\Big\} = \max\Big\{\hat{\nu}\Big(\frac{x}{y}\Big), \hat{\nu}\Big(\frac{a}{b}\Big)\Big\}.$$

Therefore $\hat{\nu}$ is also ultrametric. □

Example III.10.6. The p-adic valuation on $\mathbb{Z}$ extends to $\mathbb{Q}$. The valuations on $K[X]$ and $K[[X]]$ for a field K defined in Example III.10.3 extend to $K(X)$ and $K((X))$ respectively (Exercise II.30).

Lemma III.10.7. *Every non-trivial valuation ν of a field K is either archimedean or ultrametric. If* $\operatorname{char} K > 0$*, then ν is ultrametric.*

Proof. If ν is ultrametric, then $\nu(n \cdot 1) \leq \max\{\nu((n-1)\cdot 1), \nu(1)\} \leq \ldots \leq \nu(1) = 1$ and ν is not archimedean. Conversely, let us assume that ν is not archimedean. For $x, y \in K$ with $M := \max\{\nu(x), \nu(y)\}$, it holds that

$$\nu(x+y)^n = \nu((x+y)^n) = \nu\Big(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\Big) \leq \sum_{k=0}^{n} \nu\Big(\binom{n}{k}\Big)\nu(x)^k \nu(y)^{n-k} \leq (n+1)M^n.$$

Because of

$$n\big(\log \nu(x+y) - \log(M)\big) \leq \log(n+1) \tag{III.10.1}$$

for all $n \in \mathbb{N}$, it follows that $\nu(x+y) \leq M = \max\{\nu(x), \nu(y)\}$. Thus ν is ultrametric.

For $\operatorname{char} K = p > 0$, every valuation satisfies $\nu(\lambda)^{p-1} = \nu(\lambda^{p-1}) = \nu(1) = 1$ for $\lambda \in \mathbb{F}_p$. Therefore ν cannot be archimedean. □

Definition III.10.8. A valuation ν of a field K is called *discrete* if $\nu(K^\times) = \langle c \rangle \cong C_\infty$.

Theorem III.10.9. *Let ν be an ultrametric valuation of a field K. Then*

$$R := \{x \in K : \nu(x) \leq 1\}$$

is a local subring of K with $\mathrm{J}(R) = \{x \in R : \nu(x) < 1\}$. Conversely, K is isomorphic to the quotient field of R. If ν is discrete, then R is a principal ideal domain.

Proof. One easily shows that R is a subring and $P := \{x \in R : \nu(x) < 1\}$ is a proper ideal of R. Let $x \in I \lhd R$ be given. In the case $\nu(x) = 1$, we also have $\nu(x^{-1}) = 1$ and $x^{-1} \in R$. Then $1 = xx^{-1} \in R$ would hold. Thus $I \subseteq P = \mathrm{J}(R)$ and R is local. The inclusion $R \to K$ extends to an isomorphism $Q(R) \to K$, since for $x \in K \setminus R$, $x^{-1} \in R$ always holds.

Now let ν be discrete and $\nu(K^\times) = \langle c \rangle$ with $c \in \mathbb{R}$. Wlog. let $c < 1$ (otherwise replace c by c^{-1}). Choose $r \in R$ with $\nu(r) = c$. Let $I \trianglelefteq R$. Then there exists a minimal $k \in \mathbb{N}$ with $\nu(x) \leq c^k$ for all $x \in I$. It follows that $\nu(xr^{-k}) \leq 1$ and $xr^{-k} \in R$. This shows $I \subseteq (r^k)$. For $x \in I$ with $\nu(x) = c^k$, one obtains $r^k x^{-1} \in R^\times$ and $(r^k) \subseteq I$. Thus $I = (r^k)$ is a principal ideal. □

Remark III.10.10. In the situation of Theorem III.10.9, R is called the *valuation ring* and $\mathrm{J}(R)$ the *valuation ideal* of K.

Example III.10.11.

(i) For the trivial valuation on K, K is the valuation ring and 0 is the valuation ideal.

(ii) For the p-adic valuation on $\mathbb{Q}$, the valuation ring is $R = \mathbb{Z}_{(p)}$, the localization from Example III.1.7.

(iii) Let ν be the valuation of $K(X)$ with $\nu(X) = 2^{-1}$. Then $K[X]$ is the valuation ring and (X) is the valuation ideal. For $K((X))$, analogously $K[[X]]$ is the valuation ring.

Lemma III.10.12. *For non-trivial valuations ν_1 and ν_2 of a field K, the following properties are equivalent:*

(1) $\nu_1(x) < 1 \Longrightarrow \nu_2(x) < 1$ for all $x \in K$.

(2) There exists an $s > 0$ with $\nu_1(x) = \nu_2(x)^s$ for all $x \in K$.

(3) The open sets of K with respect to ν_1 and ν_2 coincide.

If applicable, ν_1 and ν_2 are called equivalent.

Proof.

(1) $\Rightarrow$ (2): For $x, y \in K$, first we have

$$\nu_1(x) < \nu_2(y) \implies \nu_1(x/y) < 1 \implies \nu_2(x/y) < 1 \implies \nu_2(x) < \nu_2(y).$$

Since ν_1 is non-trivial, there exists $a \in K$ with $\rho_1 := \nu_1(a) > 1 = \nu_1(1)$. It follows that $\rho_2 := \nu_2(a) > 1$. For every $x \in K^\times$ there exist $\alpha, \beta \in \mathbb{R}$ with $\nu_1(x) = \rho_1^\alpha$ and $\nu_2(x) = \rho_2^\beta$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, we can approximate α arbitrarily well by rational numbers, say $\frac{n}{m} < \alpha < \frac{k}{m}$ with $n, m, k \in \mathbb{Z}$. Since the function $\mathbb{R} \to \mathbb{R}$, $r \mapsto \rho_1^r$ is strictly monotonically increasing, it follows that

$$\begin{aligned} \rho_1^n < \rho_1^{\alpha m} < \rho_1^k, \\ \nu_1(a)^n < \nu_1(x)^m < \nu_1(a)^k, \\ \nu_2(a)^n < \nu_2(x)^m < \nu_2(a)^k, \\ \rho_2^n < \rho_2^{\beta m} < \rho_2^k. \end{aligned}$$

Because $\rho_2 > 1$, we have $\frac{n}{m} < \beta < \frac{k}{m}$ and $\alpha = \beta$. For $s := \frac{\log \rho_2}{\log \rho_1} > 0$ we have

$$\nu_2(x) = e^{\beta \log \rho_2} = e^{\alpha s \log \rho_1} = (\rho_1^\alpha)^s = \nu_1(x)^s$$

for all $x \in K$.

(2) $\Rightarrow$ (3): Let $U \subseteq K$ be open with respect to ν_1 and $x \in U$. Then there exists an $\epsilon > 0$ with $\{y \in K : \nu_1(x - y) < \epsilon\} \subseteq U$. Because $\nu_2(x - y) = \nu_1(x - y)^{1/s}$, it follows that $\nu_2(x - y) < \epsilon^{1/s} \Rightarrow y \in U$. Thus U is open with respect to ν_2. Because $\nu_2(x) = \nu_1(x)^{1/s}$ for all $x \in K$, the converse also holds.

(3) $\Rightarrow$ (1): Let $x \in K$ with $\nu_1(x) < 1$. Then $\lim_{n\to\infty} x^n = 0$ with respect to ν_1. By assumption, $(K, \nu_1) \to (K, \nu_2)$, $a \to a$ is continuous (preimages of open sets are open). Thus x^n also converges to 0 with respect to ν_2. This implies $\nu_2(x) < 1$. □

Remark III.10.13. The equivalence of valuations is obviously an equivalence relation. If ν is a discrete (resp. complete) valuation, then every valuation equivalent to ν is also discrete (resp. complete). Equivalent ultrametric valuations define the same valuation ring.

Theorem III.10.14 (Ostrowski)**.** *Every non-trivial valuation on $\mathbb{Q}$ is equivalent either to the Euclidean valuation or to exactly one p-adic valuation.*

Proof. Let ν be a non-trivial valuation on $\mathbb{Q}$.

Case 1: ν is ultrametric.
Then $\nu(n) \leq 1$ for all $n \in \mathbb{Z}$ and there exists a minimal $p \in \mathbb{N}$ with $\nu(p) < 1$. Let $p = ab$ with $a, b \in \mathbb{N}$. From $\nu(a)\nu(b) = \nu(ab) < 1$ it follows that $a = p$ or $b = p$, i. e. $p \in \mathbb{P}$. Let $q \in \mathbb{P} \setminus \{p\}$. Then there exist $a, b \in \mathbb{Z}$ with $ap + bq = 1$ and it follows

$$1 = \nu(ap + bq) \leq \max\{\underbrace{\nu(a)\nu(p)}_{<1}, \nu(b)\nu(q)\} = \nu(b)\nu(q) = 1.$$

Therefore $\nu(q) = 1$. Let $x = \pm \prod_{q \in \mathbb{P}} q^{a_q} \in \mathbb{Q}^\times$. Then

$$\nu(x) < 1 \implies \nu(p)^{a_p} < 1 \implies a_p > 0 \implies \nu_p(x) = p^{-a_p} < 1.$$

According to Lemma III.10.12, ν is equivalent to the p-adic valuation. For $q \in \mathbb{P} \setminus \{p\}$, ν is not equivalent to ν_q because of $\nu_q(q) < 1 = \nu(q)$.

Case 2: ν is archimedean.
Let $a \in \mathbb{N}$ with $\nu(a) > 1$ and $b \in \mathbb{N} \setminus \{1\}$. For $n \in \mathbb{N}$ there exist integers $0 \leq \alpha_i \leq b - 1$ with

$$a^n = \sum_{i=0}^{k} \alpha_i b^i \geq b^k$$

and $\alpha_k \neq 0$ (b-adic expansion). Here $k \leq n\frac{\log a}{\log b}$ holds. Let $\delta := \frac{\log a}{\log b}$. By the triangle inequality, $\nu(\alpha_i) = \nu(1) + \ldots + \nu(1) \leq b$ for $i = 0, \ldots, k$. With $M := \max\{1, \nu(b)\}$ it follows

$$\nu(a)^n \leq \sum_{i=0}^{k} \nu(\alpha_i)\nu(b)^i \leq b(k+1)M^k \leq b(n\delta + 1)(M^\delta)^n.$$

As in (III.10.1), it follows that $\nu(a) \leq M^\delta$. Because $\nu(a) > 1$, $M = \nu(b) > 1$ and $\frac{\log \nu(a)}{\log a} \leq \frac{\log \nu(b)}{\log b}$. By swapping a and b one obtains

$$s := \frac{\log \nu(a)}{\log a} = \frac{\log \nu(b)}{\log b} > 0.$$

Thus $\nu(b) = b^s$ for all $b \in \mathbb{N}$. It follows that $\nu(q) = |q|^s$ for all $q \in \mathbb{Q}$. Thus ν is equivalent to the Euclidean valuation. □

Corollary III.10.15. *Every discrete valuation of a field is ultrametric.*

Proof. Let K be a field with discrete valuation ν. Suppose that ν is archimedean. According to Lemma III.10.7, $\operatorname{char} K = 0$ and wlog. $\mathbb{Q} \subseteq K$. Furthermore, there exists an $n \in \mathbb{N}$ with $\nu(n) > 1$. Therefore, the restriction of ν to $\mathbb{Q}$ is also an archimedean valuation. According to Ostrowski, ν is the Euclidean valuation on $\mathbb{Q}$. In particular, $\nu(\mathbb{Q}^\times) = \mathbb{Q}_+^\times$ is not cyclic. Thus $\nu(K^\times)$ cannot be cyclic either. Contradiction. □

Remark III.10.16.

(i) We show in Remark III.10.42 that the converse of Corollary III.10.15 is false.

(ii) Interestingly, the product over all non-trivial non-equivalent valuations of $\mathbb{Q}$ yields the trivial valuation:

$$|x| \prod_{p \in \mathbb{P}} \nu_p(x) = 1 \qquad (x \in \mathbb{Q}^\times).$$

Theorem III.10.17. *For every field K with valuation ν, the following holds:*

(i) There exists a field $\hat{K}$ with a complete valuation $\hat{\nu}$ and a monomorphism $\Gamma\colon K \to \hat{K}$, such that $\Gamma(K)$ is dense[1] in $\hat{K}$ and $\hat{\nu} \circ \Gamma = \nu$ holds.

(ii) If $\tilde{\Gamma}\colon K \to \tilde{K}$ is also as in (i)*, then there exists exactly one continuous isomorphism $\Theta\colon \hat{K} \to \tilde{K}$ with $\Theta \circ \Gamma = \tilde{\Gamma}$.*

One calls $\hat{K}$ the completion *of K with respect to ν.*

Proof.

(i) **Step 1:** Construction of $\hat{K}$.
Let R be the set of all Cauchy sequences[2] $\alpha := (a_n)_{n\in\mathbb{N}}$ of elements from K. According to Remark III.10.4, $(\nu(a_n))_n$ is a real Cauchy sequence. Since $\mathbb{R}$ is complete, there exists $\|\alpha\| := \lim_{n\to\infty} \nu(a_n) \in \mathbb{R}$. For $\alpha := (a_n) \in R$ and $\beta := (b_n) \in R$ it holds that

$$\begin{aligned} \nu(a_n + b_n - a_m - b_m) &\leq \nu(a_n - a_m) + \nu(b_n - b_m), \\ \nu(a_n b_n - a_m b_m) = \nu(a_n b_n - a_n b_m + a_n b_m - a_m b_m) &\leq \nu(a_n)\nu(b_n - b_m) + \nu(b_m)\nu(a_n - a_m). \end{aligned}$$

From this follows $\alpha + \beta := (a_n + b_n)_n \in R$ and $\alpha \cdot \beta := (a_n b_n)_n \in R$. In this way, R becomes a ring with $0 := (0, 0, \ldots)$ and $1 := (1, 1, \ldots)$. Furthermore, $I := \{\alpha \in R : \|\alpha\| = 0\} \lhd R$. For $\alpha \in R \setminus I$ there exists an $N \in \mathbb{N}$ with $\nu(a_n) > \frac{1}{2}\|\alpha\| > 0$ for all $n \geq N$. We define $\beta := (b_n)_n = (1, \ldots, 1, a_N^{-1}, a_{N+1}^{-1}, \ldots)$. Then it holds that

$$\nu(b_n - b_m) = \nu\Big(\frac{a_m - a_n}{a_n a_m}\Big) \leq 4\|\alpha\|^{-1}\nu(a_m - a_n)$$

for $n, m \geq N$ and it follows that $\beta \in R$. Furthermore, $\|1 - \alpha\beta\| = 0$, i. e. $(\alpha + I)(\beta + I) = 1 + I$. Therefore I is a maximal ideal and $\hat{K} := R/I$ is a field. Obviously $\Gamma\colon K \to \hat{K}$, $a \mapsto (a, a, \ldots) + I$ is a monomorphism.

Step 2: Construction of $\hat{\nu}$.
For $\alpha, \beta \in R$, according to the usual rules for limits, it holds that

$$\begin{aligned} \|\alpha\| \geq 0 \text{ and } \|\alpha\| = 0 &\iff \alpha \in I, \\ \|\alpha\beta\| = \lim_{n\to\infty} \nu(a_n b_n) = \lim_{n\to\infty} \nu(a_n)\nu(b_n) &= \|\alpha\|\|\beta\|, \\ \|\alpha + \beta\| = \lim_{n\to\infty} \nu(a_n + b_n) \leq \lim_{n\to\infty} (\nu(a_n) + \nu(b_n)) &= \|\alpha\| + \|\beta\|, \\ \alpha \equiv \beta \pmod{I} \implies \|\alpha\| = \|\alpha - \beta + \beta\| \leq \|\alpha - \beta\| + \|\beta\| &= \|\beta\| \leq \|\alpha\|. \end{aligned}$$

Thus $\hat{\nu}\colon \hat{K} \to \mathbb{R}$, $\overline{\alpha} := \alpha + I \mapsto \|\alpha\|$ is a well-defined valuation on $\hat{K}$ with $\hat{\nu}(\Gamma(a)) = \lim \nu(a) = \nu(a)$ for $a \in K$. For $\epsilon > 0$ let $N \in \mathbb{N}$ with $\nu(a_n - a_m) < \epsilon$ for $n, m \geq N$. Then it holds that

$$\hat{\nu}(\overline{\alpha} - \Gamma(a_N)) = \lim_{n\to\infty} \nu(a_n - a_N) \leq \epsilon.$$

Thus $\Gamma(K)$ lies dense in $\hat{K}$.

Step 3: $\hat{\nu}$ is complete.
Let $(\overline{\alpha_n})_n$ be a Cauchy sequence in $\hat{K}$. Since $\Gamma(K)$ lies dense in $\hat{K}$, there exists for every $n \in \mathbb{N}$

[1] Reminder: For all $a \in \hat{K}$ and $\epsilon > 0$ there exists a $b \in K$ with $\hat{\nu}(a - b) < \epsilon$.
[2] Reminder: For every $\epsilon > 0$ there exists an $N \in \mathbb{N}$ with $\nu(a_n - a_m) < \epsilon$ for all $n, m \geq N$

an $a_n \in K$ with $\hat{\nu}(\overline{\alpha_n} - \Gamma(a_n)) < \frac{1}{n}$. Let $\alpha := (a_n)_n$ and $\epsilon > 0$. Then there exists an $N \in \mathbb{N}$ with $\frac{1}{N} < \epsilon/4$ and $\hat{\nu}(\overline{\alpha_n} - \overline{\alpha_m}) < \epsilon/2$ for all $n, m \geq N$. It follows that

$$\begin{aligned}\nu(a_n - a_m) &= \hat{\nu}\big(\Gamma(a_n - a_m)\big) = \hat{\nu}\big(\Gamma(a_n) - \overline{\alpha_n} + \overline{\alpha_n} - \overline{\alpha_m} + \overline{\alpha_m} - \Gamma(a_m)\big) \\ &< \frac{1}{n} + \frac{\epsilon}{2} + \frac{1}{m} < \epsilon.\end{aligned}$$

This shows $\alpha \in R$. Furthermore,

$$\begin{aligned}\hat{\nu}(\overline{\alpha} - \overline{\alpha_n}) &= \hat{\nu}(\overline{\alpha} - \Gamma(a_n) + \Gamma(a_n) - \overline{\alpha_n}) \leq \hat{\nu}(\overline{\alpha} - \Gamma(a_n)) + \hat{\nu}(\overline{\alpha_n} - \Gamma(a_n)) \\ &< \lim_{k\to\infty} \nu(a_k - a_n) + \frac{1}{n} \xrightarrow{n\to\infty} 0,\end{aligned}$$

i. e. $(\overline{\alpha_n})_n$ converges to $\overline{\alpha}$ in K. Therefore $\hat{\nu}$ is complete.

(ii) **Step 1:** Construction of Θ.
For $\alpha = (a_n) \in R$, $\tilde{\nu}(\tilde{\Gamma}(a_n) - \tilde{\Gamma}(a_m)) = \nu(a_n - a_m)$. Thus $(\tilde{\Gamma}(a_n))_n$ is a Cauchy sequence in $\tilde{K}$. Since $\tilde{\nu}$ is complete, there exists

$$\Theta(\overline{\alpha}) := \lim_{n\to\infty} \tilde{\Gamma}(a_n) \in \tilde{K}.$$

For $\beta = (b_n) \equiv \alpha \pmod{I}$, $(\tilde{\Gamma}(a_n) - \tilde{\Gamma}(b_n))_n$ is a null sequence. This shows that Θ is well-defined. Furthermore, $\Theta(\Gamma(a)) = \lim \tilde{\Gamma}(a) = \tilde{\Gamma}(a)$ for all $a \in K$. With $\tilde{\Gamma}$, Θ is also a ring homomorphism. Since $\hat{K}$ is a field, Θ is injective. Since $\tilde{\Gamma}(K)$ lies dense in $\tilde{K}$, every element of $\tilde{K}$ is the limit of a sequence $(\tilde{\Gamma}(a_n))_n$. With $(\tilde{\Gamma}(a_n))_n$, $(a_n)_n$ is also a Cauchy sequence. From this follows the surjectivity of Θ. Because of

$$\tilde{\nu}\big(\Theta(\overline{\alpha})\big) = \tilde{\nu}\Big(\lim_{n\to\infty} \tilde{\Gamma}(a_n)\Big) \overset{\text{III.10.4}}{=} \lim_{n\to\infty} \nu(a_n) = \hat{\nu}(\overline{\alpha})$$

Θ is isometric and therefore (uniformly) continuous.

Step 2: Uniqueness of Θ.
Let $\Psi\colon \hat{K} \to \tilde{K}$ be another continuous isomorphism with $\Psi \circ \Gamma = \tilde{\Gamma}$. Since $\Gamma(K)$ lies dense in $\hat{K}$, there exists for $\overline{\alpha} \in \hat{K}$ a sequence $(\Gamma(a_n))_n$ with $\overline{\alpha} = \lim_{n\to\infty} \Gamma(a_n)$. Since Θ and Ψ are continuous, it holds that

$$\Psi(\overline{\alpha}) = \lim_{n\to\infty} \Psi(\Gamma(a_n)) = \lim_{n\to\infty} \tilde{\Gamma}(a_n) = \lim_{n\to\infty} \Theta(\Gamma(a_n)) = \Theta(\overline{\alpha}). \qquad \square$$

Example III.10.18.

(i) If ν is already complete, then $\hat{K} \cong K$ due to the uniqueness of $\hat{K}$. This holds, for example, for the trivial valuation (every Cauchy sequence is constant).

(ii) As is well known, $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the Euclidean valuation.

(iii) According to Exercise III.59, $K((X))$ is the completion of $K(X)$.

(iv) Let $(a_n)_n$ be an integer Cauchy sequence with respect to the p-adic valuation for $p \in \mathbb{P}$. Then for every $k \in \mathbb{N}$ there exists an $N \in \mathbb{N}$ with $\nu_p(a_n - a_m) < p^{-k}$, i. e. $a_n \equiv a_m \pmod{p^k}$ for $n, m \geq N$. This motivates the following definition.

Definition III.10.19. For $p \in \mathbb{P}$,

$$\mathbb{Z}_{[p]} := \Big\{(a_n + p^n\mathbb{Z})_n \in \bigtimes_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : \forall n \in \mathbb{N} : a_n \equiv a_{n+1} \pmod{p^n}\Big\}$$

is the ring of *p-adic integers*. For $\alpha = (a_n + p^n\mathbb{Z})_n \in \mathbb{Z}_{[p]} \setminus \{0\}$ there exists a maximal power p^k with $p^k \mid a_k$. We define $\hat{\nu}_p(\alpha) := p^{-k}$ as well as $\hat{\nu}_p(0) := 0$.

Remark III.10.20.

(i) Let $\alpha := (a_n + p^n\mathbb{Z})_n \neq 0$ and $\beta := (b_n + p^n\mathbb{Z})_n \neq 0$ be p-adic integers. Let $k, l \in \mathbb{N}$ be maximal with $p^k \mid a_k$, $p^l \mid b_l$ and wlog. $k \leq l$. Because of $b_k \equiv b_l \equiv 0 \pmod{p^k}$, it holds that $p^k \mid a_k + b_k$ and it follows that

$$\hat{\nu}_p(\alpha + \beta) \leq p^{-k} = \max\big\{\hat{\nu}_p(\alpha), \hat{\nu}_p(\beta)\big\}.$$

Because of $p^{k+l} \mid a_{k+l}b_{k+l}$ and $p^n \nmid a_nb_n$ for all $n > k+l$, we also have $\hat{\nu}_p(\alpha\beta) = \hat{\nu}(\alpha)\hat{\nu}(\beta)$. Overall, $\hat{\nu}_p$ is an ultrametric valuation on $\mathbb{Z}_{[p]}$. From $\alpha\beta \neq 0$ it further follows that $\mathbb{Z}_{[p]}$ is an integral domain.

(ii) The quotient field $\mathbb{Q}_{[p]}$ of $\mathbb{Z}_{[p]}$ is called the field of *p-adic numbers*.[3] According to Lemma III.10.5, $\hat{\nu}_p$ extends to a valuation on $\mathbb{Q}_{[p]}$. Obviously, $\mathbb{Z}_{[p]}$ is the valuation ring of $\mathbb{Q}_{[p]}$ with valuation ideal $p\mathbb{Z}_{[p]}$. According to Theorem III.10.9, $\mathbb{Z}_{[p]}$ is local and $\mathbb{Z}_{[p]}^{\times} = \mathbb{Z}_{[p]} \setminus p\mathbb{Z}_{[p]}$.

(iii) By means of the isometric ring monomorphism $\mathbb{Z} \to \mathbb{Z}_{[p]}$, $a \mapsto (a + p^n\mathbb{Z})_n$, one can consider $\mathbb{Z}$ as a subring of $\mathbb{Z}_{[p]}$ and $\mathbb{Q}$ as a subfield of $\mathbb{Q}_{[p]}$. In particular, $\operatorname{char}\mathbb{Q}_{[p]} = 0$. For $\alpha := (a_n + p^n\mathbb{Z})_n \in \mathbb{Z}_{[p]}$, we can assume $0 \leq a_n < p^n$ for all $n \in \mathbb{N}$. The numbers $b_0 := a_1$ and $b_n := \frac{a_{n+1}-a_n}{p^n}$ for $n \geq 1$ then lie in $\{0, \ldots, p-1\}$. As a telescoping sum, one obtains an (infinite) p-adic expansion

$$\alpha = \sum_{n=0}^{\infty} b_n p^n.$$

For $\alpha \in \mathbb{N}$, this coincides with the usual p-adic expansion (Exercise III.64). Conversely, every sequence $(b_n) \in \{0, \ldots, p-1\}^{\mathbb{N}_0}$ of coefficients defines exactly one p-adic integer. In particular, $\mathbb{Z}_{[p]}$ is uncountable. In contrast to the ring of formal power series $\mathbb{F}_p[[X]]$, p-adic expansions in $\mathbb{Z}_{[p]}$ are added with a "carry" (furthermore, $\operatorname{char}\mathbb{F}_p[[X]] = p$).

(iv) Let $\frac{\alpha}{\beta} \in \mathbb{Q}_{[p]}$ and $\hat{\nu}_p(\beta) = p^{-k}$ with $k \in \mathbb{N}_0$. Then $p^{-k}\beta \in \mathbb{Z}_{[p]}^{\times}$ and there exists a p-adic expansion $\alpha(p^{-k}\beta)^{-1} = \sum_{n=0}^{\infty} b_n p^n$. Thus

$$\frac{\alpha}{\beta} = p^{-k}\frac{\alpha}{p^{-k}\beta} = \sum_{n=-k}^{\infty} b_{n+k}p^n =: \ldots b_{k+1}b_k{,}b_{k-1}\ldots b_0$$

(this also shows that $\mathbb{Q}_{[p]}$ coincides with the localization $\mathbb{Z}_{[p]}[p^{-1}]$ (Example III.1.7)). Therefore, $\mathbb{Q}_{[p]}$ has similarities with the field of formal Laurent series $\mathbb{F}_p((X))$.

Example III.10.21.

(i) The addition and multiplication in $\mathbb{Z}_{[p]}$ can be performed by hand as in the decimal system. For $p = 3$, for example, it holds that

$$12{,}1 + 2{,}21 = (p + 2p^0 + p^{-1}) + (2p^0 + 2p^{-1} + p^{-2}) = 2p + 2p^0 + p^{-2} = 22{,}01,$$
$$12{,}1 \cdot 2{,}21 = (p + 2p^0 + p^{-1})(2p^0 + 2p^{-1} + p^{-2}) = p^2 + p + 2p^0 + 2p^{-1} + p^{-2} + p^{-3} = 112{,}211.$$

[3] In the literature, the notation $\mathbb{Q}_p$ is often chosen, which in our case is already occupied by the cyclotomic field.

(ii) According to Remark III.10.20, $3 \in \mathbb{Z}_{[2]}^\times$. For $\alpha = (a_n)_n = 3^{-1}$, it holds that $3a_n \equiv 1 \pmod{2^n}$ for all $n \in \mathbb{N}$. One easily checks

$$a_n \equiv \begin{cases} \frac{2^n+1}{3} & \text{if } n \text{ is odd,} \\ \frac{2^{n+1}+1}{3} & \text{if } n \text{ is even} \end{cases} \pmod{p^n}.$$

This yields a periodic 2-adic expansion

$$\frac{1}{3} = 1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + \ldots = \ldots 01011 = \ldots \overline{01}1.$$

Alternatively, the result can be interpreted as a geometric series:

$$\frac{1}{3} = 1 + \sum_{k=0}^{\infty} 2^{2k+1} = 1 + \sum_{k=0}^{\infty} (2^{2k+2} - 2^{2k+1}) = \sum_{k=0}^{\infty} (-2)^k$$

(Exercise III.62).

Theorem III.10.22. *There exists a continuous isomorphism $\hat{\mathbb{Q}} \to \mathbb{Q}_{[p]}$, where $\hat{\mathbb{Q}}$ is the completion of $\mathbb{Q}$ w.r.t. ν_p.*

Proof. Let $\Gamma\colon \mathbb{Q} \to \mathbb{Q}_{[p]}$ be the canonical embedding. By construction, $\hat{\nu}_p(\Gamma(a)) = \nu_p(a)$ for $a \in \mathbb{Q}$. For $\alpha = (a_n + p^n\mathbb{Z})_n \in \mathbb{Z}_{[p]}$, it holds that $\hat{\nu}_p(\alpha - \Gamma(a_n)) \leq p^{-n}$. Therefore, $\Gamma(\mathbb{Z})$ is dense in $\mathbb{Z}_{[p]}$. According to Remark III.10.20, every element in $\mathbb{Q}_{[p]}$ can be written in the form $p^{-k}\alpha$ with $k \in \mathbb{N}_0$ and $\alpha \in \mathbb{Z}_{[p]}$. Thus, $\Gamma(\mathbb{Q})$ is dense in $\mathbb{Q}_{[p]}$. For every Cauchy sequence $\left(\frac{\alpha_n}{\beta_n}\right)_n$ in $\mathbb{Q}_{[p]}$, there exists $p^k := \lim_{n\to\infty} \hat{\nu}_p\left(\frac{\alpha_n}{\beta_n}\right)$ according to Remark III.10.4. For some $N \in \mathbb{N}$, it therefore holds that $\hat{\nu}_p(\alpha_n) = p^k\hat{\nu}_p(\beta_n)$ for all $n \geq N$. Wlog. let $N = 1$. After multiplication by p^{-k}, we can thus assume $\beta_n = 1$ for all $n \in \mathbb{N}$.

For $n \in \mathbb{N}$, there exists $a_n \in \mathbb{Z}$ with $\hat{\nu}_p(\alpha_n - \Gamma(a_n)) < \frac{1}{n}$. As in step 3 of the proof of Theorem III.10.17, one shows that $(\Gamma(a_n))_n$ is a Cauchy sequence in $\mathbb{Z}_{[p]}$. For $k \in \mathbb{N}$, let $N_k \in \mathbb{N}$ with $a_n \equiv a_m \pmod{p^k}$ for all $n, m \geq N_k$. Wlog. let $k \leq N_k \leq N_l$ for $k \leq l$. We define $b_k := a_{N_k}$ for $k \in \mathbb{N}$. Then $\beta := (b_k + p^k\mathbb{Z})_k \in \mathbb{Z}_{[p]}$. For $n \geq N_k$, it holds that $b_n = a_{N_n} \equiv a_n \pmod{p^k}$. It follows that

$$\hat{\nu}_p(\beta - \alpha_n) \leq \hat{\nu}_p(\beta - \Gamma(a_n)) + \hat{\nu}_p(\Gamma(a_n) - \alpha_n) < p^{-k} + \frac{1}{n} \xrightarrow{n\to\infty} 0,$$

i.e., $(\alpha_n)_n$ converges to β. Thus, $\mathbb{Q}_{[p]}$ is complete w.r.t. $\hat{\nu}_p$ and Theorem III.10.17(ii) yields a continuous isomorphism $\Theta\colon \hat{\mathbb{Q}} \to \mathbb{Q}_{[p]}$. □

Remark III.10.23. In comparison to $\mathbb{R}$, analysis in $\mathbb{Q}_{[p]}$ is significantly simpler, as one does not need convergence criteria for sequences, for example (Exercise III.56).

Theorem III.10.24 (Ostrowski)**.** *Up to isomorphism, $\mathbb{R}$ and $\mathbb{C}$ with the Euclidean valuation are the only fields with a complete archimedean valuation.*

Proof. Let K be a field with a complete archimedean valuation ν. According to Lemma III.10.7, $\operatorname{char} K = 0$ and we can assume $\mathbb{Q} \subseteq K$.

Step 1: $\mathbb{R} \subsetneq K$ and $\nu(x) = |x|$ for $x \in \mathbb{R}$.
By definition, the restriction of ν to K is archimedean. According to Theorem III.10.14, there exists

an $s > 0$ such that $\nu(x) = |x|^s$ for all $x \in \mathbb{Q}$. Let $\tilde{\nu}(x) := \nu(x)^{1/s}$ for $x \in K$. Obviously, $\tilde{\nu}$ is positive definite and multiplicative. For $x, y \in K$ and $n \in \mathbb{N}$, it holds that

$$\begin{aligned}\tilde{\nu}(x+y)^n = \tilde{\nu}\big((x+y)^n\big) &= \nu\Big(\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\Big)^{1/s} \le \Big(\sum_{k=0}^{n}\binom{n}{k}^s \nu(x)^k\nu(y)^{n-k}\Big)^{1/s}\\ &\le (n+1)^{1/s}\max\Big\{\binom{n}{k}^s \nu(x)^k\nu(y)^{n-k} : k = 0,\dots,n\Big\}^{1/s}\\ &= (n+1)^{1/s}\max\Big\{\binom{n}{k}\tilde{\nu}(x)^k\tilde{\nu}(y)^{n-k} : k = 0,\dots,n\Big\}\\ &\le (n+1)^{1/s}\big(\tilde{\nu}(x)+\tilde{\nu}(y)\big)^n.\end{aligned}$$

As in (III.10.1), the triangle inequality $\tilde{\nu}(x+y) \le \tilde{\nu}(x) + \tilde{\nu}(y)$ follows. By construction, $\nu(x) = |x|$ holds for $x \in \mathbb{Q}$. Since ν is complete, K contains the limit of every Cauchy sequence in $\mathbb{Q}$, i.e., we can assume $\mathbb{R} \subsetneq K$. Then $\nu(x) = |x|$ holds for $x \in \mathbb{R}$.

Step 2: $K \cong \mathbb{C}$.
According to the Fundamental Theorem of Algebra and Theorem II.2.10, it suffices to show that $\mathbb{R} \subseteq K$ is algebraic. Let $x \in K \setminus \mathbb{R}$ and

$$q\colon \mathbb{C} \to \mathbb{R}, \qquad z \mapsto \nu\big((x-z)(x-\overline{z})\big) = \nu(x^2 - (z+\overline{z})x + z\overline{z}).$$

Because $z + \overline{z}, z\overline{z} \in \mathbb{R}$, it is enough to show that q has a zero. With respect to the Euclidean norm, q is continuous, because

$$\begin{aligned}\big|\nu\big((x-z)(x-\overline{z})\big) - \nu\big((x-w)(x-\overline{w})\big)\big| &\le \nu\big(-(z-w+\overline{z}-\overline{w})x + z\overline{z} - w\overline{z} + w\overline{z} - w\overline{w}\big)\\ &\le 2|z-w|\nu(x) + |z-w|\big(|z|+|w|\big).\end{aligned}$$

For $a, b, c \in K$, it is well known that $\nu(a-b+c) \ge \nu(a-b) - \nu(c) \ge \nu(a) - \nu(b) - \nu(c)$. For $|z| > 3\nu(x)$, it therefore holds that

$$q(z) \ge |z|^2 - |z+\overline{z}|\nu(x) - \nu(x)^2 \ge |z|^2 - \frac{2}{3}|z|^2 - \frac{1}{9}|z|^2 > 2\nu(x)^2 \ge \nu(x)^2 = q(0).$$

According to the Extreme Value Theorem, q attains its minimum $m := \min\{q(z) : z \in \mathbb{C}\}$ on the compact set $\{z \in \mathbb{C} : |z| \le 3\nu(x)\}$. Assume indirectly $m > 0$. Then the non-empty, compact set $M := \{z \in \mathbb{C} : q(z) = m\}$ has an element z_0 with the largest possible norm $|z_0|$. We consider

$$\alpha := (X - z_0)(X - \overline{z_0}) + \epsilon = X^2 - (z_0 + \overline{z_0})X + |z_0|^2 + \epsilon \in \mathbb{R}[X],$$

where $0 < \epsilon < m$. For $s \in \mathbb{R}$, it holds that $\alpha(s) = |s - z_0|^2 + \epsilon > 0$. Therefore, α has two complex-conjugate zeros $z_1, \overline{z_1}$. The product of the zeros is the constant term of α, i.e., $|z_1|^2 = |z_0|^2 + \epsilon > |z_0|^2$. This shows $z_1 \notin M$ and $q(z_1) > m$.

For odd $n \in \mathbb{N}$, we now consider

$$\beta := (\alpha - \epsilon)^n + \epsilon^n = (X - z_0)^n(X - \overline{z_0})^n + \epsilon^n \in \mathbb{R}[X]$$

with zero z_1. Because $\beta(s) = |s - z_0|^{2n} + \epsilon^n > 0$ for $s \in \mathbb{R}$, β factorizes into pairs of complex-conjugate linear factors, say

$$\beta = \prod_{i=1}^{n}\big(X^2 - (z_i + \overline{z_i})X + |z_i|^2\big).$$

For $X = x$, one obtains

$$q(z_1)m^{n-1} \leq \prod_{i=1}^{n} q(z_i) = \nu(\beta(x)) = \nu\big((x-z_0)^n(x-\overline{z_0})^n + \epsilon^n\big) \leq q(z_0)^n + \epsilon^n = m^n + \epsilon^n.$$

This yields $q(z_1) \leq m + \frac{\epsilon^n}{m^{n-1}}$. With $n \to \infty$, the contradiction $q(z_1) \leq m$ results. Thus $m = 0$ as claimed. □

Definition III.10.25. Let V be a finite-dimensional vector space over a field K with valuation ν. A map $V \to \mathbb{R}$, $v \mapsto |v|$ is called a *norm* of V, if the following hold:

- $|v| \geq 0$ and $|v| = 0 \iff v = 0$ (positive definite),
- $|\lambda v| = \nu(\lambda)|v|$ (homogeneous),
- $|v + w| \leq |v| + |w|$ (subadditive)

for all $v, w \in V$ and $\lambda \in K$. If applicable, V is called a *normed space*. Two norms $|.|_1$ and $|.|_2$ on V are called *equivalent*, if there exist $s, t > 0$ with $s|v|_1 \leq |v|_2 \leq t|v|_1$ for all $v \in V$.

Example III.10.26. Many norms can be transferred from analysis. The next theorem shows that we usually get by with one norm. On $V = K^n$ there exists the *maximum norm*

$$|v|_{\max} := \max\{\nu(v_i) : i = 1, \ldots, n\} \qquad (v = (v_1, \ldots, v_n) \in V).$$

Theorem III.10.27. *Let V be an n-dimensional normed space over a field K with complete valuation ν. Then there exists a continuous isomorphism $K^n \to V$ with continuous inverse function[4] with respect to $|.|_{\max}$. In particular, V is complete and any two norms on V are equivalent.*

Proof. Let $b_1, \ldots, b_n \in V$ be a basis and $\beta := \max_{1 \leq i \leq n} |b_i|$. Then $f\colon K^n \to V$, $(x_i) \mapsto \sum_{i=1}^n x_i b_i$ defines an isomorphism with

$$|f(x)| \leq \sum_{i=1}^{n} |x_i b_i| \leq n \max_{1 \leq i \leq n} \{\nu(x_i)|b_i|\} \leq n\beta|x|_{\max}.$$

Because of $|f(x) - f(y)| = |f(x-y)| \leq n\beta|x-y|_{\max}$ for $x, y \in K^n$, f is (uniformly) continuous. Now let us assume indirectly that a sequence $(x^{(k)})_{k \in \mathbb{N}}$ with

$$|x^{(k)}|_{\max} > k|f(x^{(k)})|$$

for $k \in \mathbb{N}$ exists. Then there exists $1 \leq i \leq n$ with $\nu(x_i^{(k)}) = |x^{(k)}|_{\max}$ for infinitely many k. After passing to a subsequence and normalizing, we can assume $x_1^{(k)} = |x^{(k)}|_{\max} = 1$ for all $k \in \mathbb{N}$. By choosing a subsequence again, one can assume that all $x^{(k)}$ vanish on the same m coordinates. Let m be as large as possible. Since the vectors $x^{(k)} - x^{(l)}$ vanish on at least $m+1$ coordinates, there exists a $\gamma > 0$ with

$$|x^{(k)} - x^{(l)}|_{\max} \leq \gamma|f(x^{(k)}) - f(x^{(l)})| \leq \gamma\big(|f(x^{(k)})| + |f(x^{(l)})|\big) < \frac{\gamma}{k} + \frac{\gamma}{l}.$$

[4]Thus a *homeomorphism*

Thus $x^{(k)}$ is a Cauchy sequence in K^n. One easily shows that with K, also K^n is complete with respect to $|.|_{\max}$. Therefore $x := \lim_{k\to\infty} x^{(k)} \in K^n$ exists. Because of $x_1 = x_1^{(k)} = 1$, $x \neq 0$. Since f is continuous, one obtains the contradiction

$$0 \neq f(x) = \lim_{k\to\infty} f(x^{(k)}) < \lim_{k\to\infty} \frac{1}{k} = 0.$$

Thus there exists $\gamma > 0$ with $|x|_{\max} \leq \gamma |f(x)|$ for all $x \in K^n$, i. e. f^{-1} is (uniformly) continuous.

The completeness of K^n with respect to $|.|_{\max}$ implies the completeness of V with respect to $|.|$. If $|.|'$ is another norm on V, then there exists a continuous isomorphism $g\colon K^n \to V$ with respect to $|.|'$ with continuous inverse function. Then $g \circ f^{-1}\colon V \to V$ is also such an isomorphism. From this follows the equivalence of $|.|$ and $|.|'$. □

Lemma III.10.28. *Let $\nu_1, \ldots, \nu_n$ be pairwise non-equivalent non-trivial valuations on K. Then there exists $x \in K$ with $\nu_1(x) > 1$ and $\nu_i(x) < 1$ for $i = 2, \ldots, n$.*

Proof. Since ν_1 and ν_2 are not equivalent, there exist $a, b \in K$ with $\nu_1(a) < 1$, $\nu_2(a) \geq 1$ and $\nu_1(b) \geq 1$, $\nu_2(b) < 1$. For $c := b/a \in K$ it then holds that $\nu_1(c) > 1$ and $\nu_2(c) < 1$. Thus the case $n = 2$ is settled. Now let inductively $y \in K$ with $\nu_1(y) > 1$ and $\nu_i(y) < 1$ for $i = 3, \ldots, n$. In the case $\nu_2(y) \leq 1$ there exists a $k \in \mathbb{N}$ with

$$\nu_1(cy^k) = \nu_1(c)\nu_1(y)^k > 1, \qquad \nu_2(cy^k) \leq \nu_2(c) < 1, \qquad \nu_i(cy^k) < 1 \qquad (3 \leq i \leq n).$$

The claim thus holds for $x := cy^k$. Finally, let $\nu_2(y) > 1$. For $k \in \mathbb{N}$ and $1 \leq i \leq n$ it holds as usual

$$|1 - \nu_i(y)^k| \leq \nu_i(1 + y^k) \leq 1 + \nu_i(y)^k.$$

Let $z_k := \frac{y^k}{1+y^k}$. For sufficiently large k it is then

$$\nu_i(cz_k) = \nu_i(c)\frac{\nu_i(y)^k}{\nu_i(1+y^k)} \begin{cases} \geq \nu_1(c)\frac{\nu_1(y)^k}{1+\nu_1(y)^k} > 1 & \text{if } i = 1, \\ \leq \nu_2(c)\frac{\nu_2(y)^k}{\nu_2(y)^k - 1} < 1 & \text{if } i = 2, \\ \leq \nu_i(c)\frac{\nu_i(y)^k}{1-\nu_i(y)^k} < 1 & \text{if } i \geq 3. \end{cases} \tag{III.10.2}$$

We can therefore set $x := cz_k$. □

Theorem III.10.29 (Artin-Whaples Approximation Theorem)**.** *Let $\nu_1, \ldots, \nu_n$ be pairwise non-equivalent non-trivial valuations on K and $x_1, \ldots, x_n \in K$. Then for every $\epsilon > 0$ there exists an $x \in K$ with $\nu_i(x - x_i) < \epsilon$ for $i = 1, \ldots, n$.*

Proof. By Lemma III.10.28 there exist $y_1, \ldots, y_n \in K$ with $\nu_i(y_i) > 1$ and $\nu_i(y_j) < 1$ for $i \neq j$. We define

$$s_k := \sum_{i=1}^{n} x_i \frac{y_i^k}{1 + y_i^k}$$

for $k \in \mathbb{N}$. As in (III.10.2) it holds

$$\nu_i(s_k - x_i) \leq \sum_{j\neq i} \nu_i(x_j)\frac{\nu_i(y_j)^k}{1 - \nu_i(y_j)^k} + \nu_i(x_i)\frac{1}{\nu_i(y_i^k) - 1} \xrightarrow{k\to\infty} 0$$

for $i = 1, \ldots, n$. Therefore the claim holds for $x := s_k$, if k is sufficiently large. □

Example III.10.30. Let $p_1, \ldots, p_n \in \mathbb{P}$ and $x_1, \ldots, x_n \in \mathbb{Z}$. For every $\epsilon > 0$ the Chinese Remainder Theorem provides an $x \in \mathbb{Z}$ with $x \equiv x_i \pmod{p_i^{k_i}}$ for $i = 1, \ldots, n$, where $p_i^{-k_i} < \epsilon$. This means $\nu_p(x - x_i) < \epsilon$. If one adds a further inequality for the Euclidean valuation, i.e., $|x - x_{n+1}| < \epsilon$, then one must choose $x \in \mathbb{Q}$. The Approximation Theorem can therefore be regarded as a generalization of the Chinese Remainder Theorem.

Lemma III.10.31 (Hensel)**.** *Let K be a field with an ultrametric complete valuation ν, valuation ring R and $\overline{R} := R/\mathrm{J}(R)$. Let $\alpha \in R[X]$ and $\overline{\alpha} = \alpha_1\alpha_2 \in \overline{R}[X]$ with $\gcd(\alpha_1, \alpha_2) = 1$ and α_1 monic. Then there exist $\beta, \gamma \in R[X]$ with $\alpha = \beta\gamma$, $\overline{\beta} = \alpha_1$, $\overline{\gamma} = \alpha_2$ and β monic.*

Proof. According to Theorem III.10.9, R is a local ring and $\overline{R}$ is a field. We first choose $\beta_1, \gamma_1 \in R[X]$ with $\overline{\beta_1} = \alpha_1$ and $\overline{\gamma_1} = \alpha_2$. Wlog. let β_1 be monic and $\deg(\alpha - \beta_1\gamma_1) < \deg\alpha =: n$ (i. e. α and γ_1 have the same leading coefficient). Since α_1, α_2 are coprime in the Euclidean ring $\overline{R}[X]$, there exist $\sigma, \tau \in R[X]$ with $\alpha_1\overline{\sigma} + \alpha_2\overline{\tau} = 1$. The coefficients of $\alpha - \beta_1\gamma_1$ and $\beta_1\sigma + \gamma_1\tau - 1$ lie in $\mathrm{J}(R)$. Among these coefficients, we choose $u \in \mathrm{J}(R)$ such that $\nu(u)$ is as large as possible. In the case $u = 0$, we have $\alpha = \beta_1\gamma_1$ and we are finished. So let $u \neq 0$. For $k \in \mathbb{N}$, let $(u^k) \trianglelefteq R[X]$. For every coefficient $s \in \mathrm{J}(R)$ of $\alpha - \beta_1\gamma_1$ or $\beta_1\sigma + \gamma_1\tau - 1$, it holds that $\nu(su^{-1}) \leq 1$, i. e. $su^{-1} \in R$ and $s = su^{-1}u \in (u)$. Therefore, $\alpha \equiv \beta_1\gamma_1 \pmod{(u)}$ and $\beta_1\sigma + \gamma_1\tau \equiv 1 \pmod{(u)}$.

For $k \geq 2$, we inductively construct polynomials $\beta_k, \gamma_k \in R[X]$ with the following properties:

(a) β_k is monic and $\deg(\alpha - \beta_k\gamma_k) < n$,

(b) $\beta_k \equiv \beta_{k+1}$ and $\gamma_k \equiv \gamma_{k+1} \pmod{(u^k)}$,

(c) $\alpha \equiv \beta_k\gamma_k \pmod{(u^k)}$.

For this, let β_k, γ_k be given. Choose $\delta \in R[X]$ with $\alpha = \beta_k\gamma_k + u^k\delta$ and $\deg\delta < n$. Since β_k is monic, we may divide by β_k with remainder without leaving $R[X]$. This yields $\rho, \theta \in R[X]$ with $\tau\delta = \beta_k\rho + \theta$ and $\deg\theta < \deg\beta_k$. Let $d := \deg\gamma_1$ and $\mu, \eta \in R[X]$ with $\sigma\delta + \gamma_k\rho = \mu + \eta X^d$ and $\deg\mu < d$. Then

$$\beta_{k+1} := \beta_k + u^k\theta, \qquad \gamma_{k+1} := \gamma_k + u^k\mu$$

already satisfy (a) and (b). Furthermore, it holds that

$$\delta \equiv (\beta_1\sigma + \gamma_1\tau)\delta \equiv (\beta_k\sigma + \gamma_k\tau)\delta \equiv \beta_k(\sigma\delta + \gamma_k\rho) + \gamma_k\theta \equiv \beta_k\mu + \beta_k\eta X^d + \gamma_k\theta \pmod{(u)}.$$

Here, $\deg\delta < n$, $\deg(\beta_k\mu) < \deg(\beta_k) + d = n$ and $\deg(\gamma_k\theta) < n$. On the other hand, $\beta_k X^d$ is monic of degree n. This is only possible if $\overline{\eta} = 0$. It follows that

$$\beta_{k+1}\gamma_{k+1} \equiv \alpha - u^k\delta + (\beta_k\mu + \gamma_k\theta)u^k \equiv \alpha \pmod{(u^{k+1})},$$

i. e. (c) holds for $k + 1$. This completes the induction.

Now we write $\beta_k = \sum_{j=0}^{e} b_{kj}X^j$ and $\gamma_k = \sum_{j=0}^{d} c_{kj}X^j$ with $b_{ij}, c_{ij} \in R$. By construction, $\nu(b_{kj} - b_{lj}) \leq \nu(u)^k < 1$ for $k \leq l$ and analogously for c_{kj}. Since K is complete, the limits $b_j := \lim_{k\to\infty} b_{kj}$ and $c_j := \lim_{k\to\infty} c_{kj}$ exist in R. We define $\beta := \sum_{j=0}^{e} b_jX^j$ and $\gamma := \sum_{j=0}^{d} c_jX^j$. Since β_k is monic, β is also monic. Furthermore, $\overline{\beta} = \overline{\beta_1} = \alpha_1$ and $\overline{\gamma} = \overline{\gamma_1} = \alpha_2$. Because $\beta\gamma \equiv \beta_k\gamma_k \equiv \alpha \pmod{(u^k)}$ for all $k \geq 1$, we have $\alpha = \beta\gamma$. □

Example III.10.32. Suppose that $\overline{\alpha}$ has a simple root $y \in \overline{R}$ as in Hensel's Lemma. Then one can choose $\alpha_1 = X - y$. Thus there exists a monic polynomial $\beta \in R[X]$ with $\beta \mid \alpha$ and $\overline{\beta} = \alpha_1$. Now β has the form $\beta = X - x$, i. e. x is a root of α with $\overline{x} = y$.

Theorem III.10.33. *Let $p \in \mathbb{P}$ and $E \leq \mathbb{Q}_{[p]}^{\times}$ be the subgroup of roots of unity. Then $E = \langle -1 \rangle \cong C_2$ if $p = 2$ and $E \cong C_{p-1}$ if $p > 2$.*

Proof. Let $\alpha = X^{p-1} - 1 \in \mathbb{Z}_{[p]}[X]$. Because of $\mathbb{Z}_{[p]}/\mathrm{J}(\mathbb{Z}_{[p]}) \cong \mathbb{F}_p$, it holds that $\overline{\alpha} = \prod_{a \in \mathbb{F}_p^{\times}} (X - a)$. Let $\mathbb{F}_p^{\times} = \langle a \rangle$. According to Example III.10.32, α has a root $x \in \mathbb{Z}_{[p]}$ with $\overline{x} = a$. Obviously x is a primitive root of unity of order $p - 1$. For $p = 2$, -1 is obviously a second root of unity (note $\operatorname{char} \mathbb{Q}_{[2]} = 0$).

Conversely, let $x \in E$ with order n. From $\hat{\nu}_p(x)^n = \hat{\nu}_p(x^n) = \hat{\nu}_p(1) = 1$ it follows that $\hat{\nu}_p(x) = 1$ and $x \in \mathbb{Z}_{[p]}$. Thus $\overline{\alpha} := X^n - 1 = \prod_{k=1}^{n} (X - \overline{x}^k) \in \mathbb{F}_p[X]$ holds. First let $p \nmid n$. Because of $\gcd(\overline{\alpha}, \overline{\alpha}') = 1$, it holds that $\overline{x}^k \neq \overline{x}^l$ for $1 \leq k < l \leq n$. Thus $\overline{x}$ also has order n in $\mathbb{F}_p^{\times}$. This shows $n \mid p - 1$. Now let $n = p > 2$. Then $\overline{x} = \overline{x}^p = \overline{x^p} = 1$ and there exists $y \in \mathbb{Z}_{[p]}$ with $x = 1 + py$. For $k \in \mathbb{N}$ it follows that $x^k = \sum_{i=0}^{k} \binom{k}{i} y^i p^i \equiv 1 + kpy \pmod{p^2}$. This yields the contradiction

$$0 = \frac{x^p - 1}{x - 1} = \sum_{k=0}^{p-1} x^k \equiv \sum_{k=0}^{p-1} (1 + kpy) = p + \frac{p-1}{2} p^2 y \equiv p \pmod{p^2}.$$

Finally, let $p = 2$ and $n = 4$. Let again $x = 1 + 2y$. Then $-1 = x^2 \equiv 1 \pmod 4$ would hold. □

Lemma III.10.34. *Let K be a field with an ultrametric complete valuation ν. Let $\alpha = \sum_{k=0}^{n} a_k X^k \in K[X]$ be irreducible. Then $\max_{1 \leq k \leq n} \nu(a_k) = \max\{\nu(a_0), \nu(a_n)\}$.*

Proof. Let $s \geq 0$ be minimal with $\nu(a_s) = \max_{1 \leq k \leq n} \nu(a_k)$. Suppose $s > 0$. Then $\beta := a_s^{-1} \alpha \in R[X]$ is also irreducible in $K[X]$ and $\overline{\beta} = X^s \beta_1 \in \overline{R}[X]$ for some $\beta_1 \in \overline{R}[X]$ with $\beta_1(0) \neq 0$. Thus X^s and β_1 are coprime. By Hensel there exist $\gamma, \delta \in R[X]$ with $\alpha = \gamma\delta$, $\overline{\gamma} = X^s$ and $\overline{\delta} = \beta_1$. Because of $s > 0$, $\deg \delta = 0$ must hold, since β is irreducible. But then also $\deg \beta_1 = 0$ and $s = n$. □

Theorem III.10.35 (Strassmann)**.** *Let K be a field with ultrametric valuation ν and valuation ring R. Let $(a_n)_{n \in \mathbb{N}_0}$ be a sequence in K, such that a maximal $N \in \mathbb{N}_0$ with $\nu(a_N) = \max_{n \in \mathbb{N}_0} \nu(a_n)$ exists. Then there exist at most N elements $x \in R$ with $\sum_{n=0}^{\infty} a_n x^n = 0$.*

Proof. Induction on N: Let $N = 0$ and $x \in R$, such that $\alpha(x) := \sum_{n=0}^{\infty} a_n x^n$ converges. According to Exercise III.56, it holds that

$$\nu(a_1 x + a_2 x^2 + \ldots) \leq \max_{n \in \mathbb{N}} \nu(a_n x^n) < \nu(a_0)$$

due to $\nu(x) \leq 1$. From Remark III.10.4 it follows that $\nu(\alpha(x)) = \nu(a_0) \neq 0$ and $\alpha(x) \neq 0$. Now let $N \geq 1$. Suppose $a_0 = 0$. Then $x = 0$ is a solution of $\alpha(x) = 0$. Every further solution $y \neq 0$ satisfies $b_0 + b_1 y + \ldots = 0$, where $b_n := a_{n+1}$ for $n \in \mathbb{N}_0$. By induction, the number of these y is at most $N - 1$. Thus the claim holds. We can therefore assume $a_0 \neq 0$. For $x \in R$ with $\alpha(x) = 0$, it holds that $x \neq 0$. We divide the formal power series $\alpha = \sum_{n=0}^{\infty} a_n X^n \in K[[X]]$ by $X - x$ and obtain $\beta = \sum_{n=0}^{\infty} b_n X^n \in K[[X]]$ with $b_0 := -a_0 x^{-1}$ and $b_n := (b_{n-1} - a_n) x^{-1}$ for $n \in \mathbb{N}$. Every solution $y \neq x$ of $\alpha(y) = 0$ now satisfies $\beta(y) = 0$. For $k \in \mathbb{N}_0$ it holds that

$$b_k = a_{k+1} + b_{k+1} x = a_{k+1} + x(a_{k+2} + b_{k+2} x) = \ldots = \sum_{n=0}^{\infty} a_{k+n+1} x^n.$$

From $\nu(x) \leq 1$ it follows that $\nu(b_k) \leq \max_{n \in \mathbb{N}_0} \nu(a_{k+n+1}) \nu(x)^n < \nu(a_N)$ for $k \geq N$. Therefore $\nu(b_{N-1}) = \nu(a_N + b_N x) = \max\{\nu(a_N), \nu(b_N x)\} = \nu(a_N)$. For $k < N - 1$ it finally holds that

$$\nu(b_k) \leq \max_{n \in \mathbb{N}_0} \nu(a_{k+n+1}) \nu(x)^n \leq \nu(a_N) = \nu(b_{N-1}).$$

Thus $\nu(b_{N-1}) = \max_{n\in\mathbb{N}_0} \nu(b_n)$. By induction, the number of $y \in R$ with $\beta(y) = 0$ is at most $N-1$. $\square$

Example III.10.36.

(i) Let $a_0 := 0$ and $a_n := \frac{2^n}{n} \in \mathbb{Q}_{[2]}$ for $n \in \mathbb{N}$. Then $N = 2$ holds with the notation from Theorem III.10.35. According to Exercise III.61, $x = 0, 1 \in \mathbb{Z}_{[2]}$ are the only solutions of $\sum a_n x^n = 0$.

(ii) Let $\alpha = X^N - p \in \mathbb{Z}_{[p]}[X]$ with $N \geq 2$. Because of $\langle \hat{\nu}_p(\mathbb{Q}_{[p]})\rangle = \langle p^{-1}\rangle = \langle \nu_p(p)\rangle$, α has no root in $\mathbb{Z}_{[p]}$. Therefore, the estimate in Straßmann's theorem is in general not optimal.

Remark III.10.37. We had already used (for example in Exercise III.35) the norm map $N\colon L \to K$, $x \mapsto \prod_{\sigma\in\mathrm{Gal}(L|K|)} \sigma(x)$ for Galois extensions $K \subseteq L$. We now introduce a more general construction.

Definition III.10.38. Let $K \subseteq L$ be a finite field extension. For $x \in L$, $t_x\colon L \to L$, $y \mapsto xy$ defines a K-linear map. We call $N_K^L\colon L \to K$, $x \mapsto \det(t_x)$ the *norm map* of L with respect to K.[5]

Lemma III.10.39. *For finite field extensions $K \subseteq L \subseteq M$, the following holds:*

(i) For $x \in K$, $N_K^L(x) = x^{|L:K|}$.

(ii) For $x, y \in L$, $N_K^L(xy) = N_K^L(x)N_K^L(y)$.

(iii) For $x \in L$, $N_K^L(x) = N_K^{K(x)}(x)^{|L:K(x)|}$.

(iv) For the minimal polynomial μ_x over K, $N_K^L(x) = (-1)^{|L:K|}\mu_x(0)^{|L:K(x)|}$.

(v) $N_K^M = N_K^L \circ N_L^M$.

(vi) If $K \subseteq L$ is a Galois extension, then $N_K^L(x) = \prod_{\sigma\in\mathrm{Gal}(L|K)|} \sigma(x)$.

Proof.

(i) The matrix of the map t_x with respect to an arbitrary basis of L is $x1_n$, where $n = |L : K|$. Therefore $N_K^L(x) = \det(t_x) = x^n$.

(ii) Obviously $t_{xy} = t_x \circ t_y$ and $N_K^L(xy) = \det(t_{xy}) = \det(t_x)\det(t_y) = N_K^L(x)N_K^L(y)$.

(iii) Let $b_1, \ldots, b_n \in K(x)$ be a K-basis of $K(x)$ and $c_1, \ldots, c_m \in L$ a $K(x)$-basis of L. According to the proof of the Degree Theorem, $B := \{b_i c_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ is a K-basis of L. Let $A \in K^{n\times n}$ be the matrix of $t'_x\colon K(x) \to K(x)$ with respect to $b_1, \ldots, b_n$. Obviously, $\mathrm{diag}(A, \ldots, A) \in K^{nm\times nm}$ is then the matrix of $t_x\colon L \to L$ with respect to B. This shows $N_K^L(x) = \det(A)^m = N_K^{K(x)}(x)^{|L:K(x)|}$.

(iv) By Cayley-Hamilton, μ_x is a divisor of the characteristic polynomial of t_x. Because of $d := \deg \mu_x = |K(x) : K|$, μ_x is the characteristic polynomial of $t'_x\colon K(x) \to K(x)$. From (iii) it follows

$$\begin{aligned} N_K^L(x) = N_K^{K(x)}(x)^{|L:K(x)|} &= \det(t'_x)^{|L:K(x)|} = \big((-1)^d \det(X\,\mathrm{id} - t'_x)(0)\big)^{|L:K(x)|} \\ &= \big((-1)^d \mu_x(0)\big)^{|L:K(x)|} = (-1)^{|L:K|}\mu_x(0)^{|L:K(x)|}. \end{aligned}$$

[5]The norm map should not be confused with the norms from Definition III.10.25.

(v) By (iii) we have

$$N_K^M(x) = N_K^{K(x)}(x)^{|M:K(x)|} = N_K^{L(x)}(x)^{|M:L(x)|}, \qquad N_K^L\big(N_L^M(x)\big) = N_K^L\big(N_L^{L(x)}(x)\big)^{|M:L(x)|}$$

for $x \in M$. We can therefore assume $M = L(x)$. Let $d := |L(x) : L|$. Then $1, x, \ldots, x^{d-1}$ is an L-basis of $L(x)$. Let $b_1, \ldots, b_n \in L$ be a K-basis of L. The matrix of $t_x \colon L(x) \to L(x)$ with respect to the basis

$$\{b_1, \ldots, b_n, b_1x, \ldots, b_nx, \ldots, b_1x^{d-1}, \ldots, b_nx^{d-1}\}$$

has the form

$$A := \begin{pmatrix} 0 & \cdots & 0 & A_1 \\ 1_n & \ddots & \vdots & \vdots \\ & \ddots & 0 & A_{d-1} \\ 0 & & 1_n & A_d \end{pmatrix}.$$

After $n(d-1)$ row swaps, one obtains $\det A = (-1)^{n(d-1)} \det(A_1)$. Let $\mu_x = X^d + \lambda_{d-1}X^{d-1} + \ldots + \lambda_0 \in L[X]$ be the minimal polynomial of x over L. Then $x^d = -\lambda_{d-1}x^{d-1} - \ldots - \lambda_0$ holds. Therefore A_1 is the matrix of $t_{-\lambda_0} \colon L \to L$. By (iv) we have $N_L^{L(x)}(x) = (-1)^d \mu_x(0) = (-1)^{d+1}(-\lambda_0)$ and

$$N_K^L(N_L^{L(x)}(x)) \overset{\text{(i),(ii)}}{=} (-1)^{n(d+1)} N_K^L(-\lambda_0) = (-1)^{n(d+1)} \det(A_1) = (-1)^{2nd} \det A = N_K^{L(x)}(x).$$

(vi) As is well known, $\mathrm{Gal}(L|K)$ permutes the roots of μ_x. Therefore

$$\mu_x^{|L:K(x)|} = \prod_{\sigma \in \mathrm{Gal}(L|K)} (X - \sigma(x))$$

and

$$N_K^L(x) \overset{\text{(iv)}}{=} (-1)^{|L:K|} \mu_x(0)^{|L:K(x)|} = \prod_{\sigma \in \mathrm{Gal}(L|K)} \sigma(x). \qquad \square$$

Theorem III.10.40. *Let K be a field with complete valuation ν. For every finite field extension $K \subseteq L$ there exists exactly one valuation $\tilde{\nu}$ on L that extends ν. Furthermore, $\tilde{\nu}$ is complete and for $x \in L$ we have*

$$\boxed{\tilde{\nu}(x) = \sqrt[|L:K|]{\nu\big(N_K^L(x)\big)}.}$$

Proof. The map $\tilde{\nu} \colon L \to L$, $x \mapsto \sqrt[|L:K|]{\nu(N_K^L(x))}$ is, according to Lemma III.10.39, a positive definite multiplicative extension of ν.

Case 1: ν is trivial.
Here $\tilde{\nu}$ is also trivial and complete. Suppose ν' is a non-trivial extension of ν. Let $x \in L^\times$ with $\tilde{\nu}(x) \neq 1$, wlog. $\tilde{\nu}(x) > 1$ (replace x by x^{-1} if necessary). Because $|L : K| < \infty$, x is algebraic over K. This contradicts Exercise III.55 applied to the minimal polynomial μ_x. Thus $\nu' = \tilde{\nu}$ is the only extension of ν.

Case 2: ν is archimedean.
According to Ostrowski, $K \in \{\mathbb{R}, \mathbb{C}\}$ and $\nu(x) = |x|^s$ for some $s > 0$ and $x \in K$. Since $\mathbb{C}$ is algebraically closed, we can assume $(K, L) = (\mathbb{R}, \mathbb{C})$. Indeed,

$$\tilde{\nu}(z) = \sqrt{\nu(N_{\mathbb{R}}^{\mathbb{C}}(z))} = \sqrt{z\bar{z}}^s = |z|^s$$

for $z \in \mathbb{C}$ is equivalent to the Euclidean valuation on $\mathbb{C}$. Let ν' be another extension of ν. According to Theorem III.10.27, ν' is equivalent to $\tilde{\nu}$ as a norm. In particular, $\tilde{\nu}$ and ν' define the same open sets. According to Lemma III.10.12, $\tilde{\nu}$ and ν' are also equivalent as valuations. Let $t > 0$ with $\nu'(z) = \tilde{\nu}(z)^t$ for all $z \in \mathbb{C}$. Because $2^s = \tilde{\nu}(2) = \nu(2) = \nu'(2) = 2^{st}$, it follows that $t = 1$ and $\nu' = \tilde{\nu}$.

Case 3: ν is ultrametric.
We first show that $\tilde{\nu}$ satisfies the ultrametric inequality. Let $x, y \in L^\times$ with $\tilde{\nu}(x) \geq \tilde{\nu}(y)$. Because $N_K^L(x+y) = N_K^L(x) N_K^L(1+\frac{y}{x})$, it suffices to show the statement $\tilde{\nu}(x) \leq 1 \Rightarrow \tilde{\nu}(1+x) \leq 1$. According to Lemma III.10.39, this is equivalent to

$$\nu\big(N_K^{K(x)}(x)\big) \leq 1 \implies \nu\big(N_K^{K(x)}(1+x)\big) \leq 1.$$

For the minimal polynomial $\mu_x = \sum_{k=0}^d a_k X^k \in K[X]$, we have $\nu(a_0) = \nu((-1)^d a_0) = \nu\big(N_K^{K(x)}(x)\big) \leq 1$ according to Lemma III.10.39. From Lemma III.10.34 it follows that $\max_{0 \leq k \leq d} \nu(a_k) = \max\{\nu(a_0), 1\} = 1$. Obviously $\mu_x(X-1)$ is the minimal polynomial of $1+x$. Therefore

$$\nu\big(N_K^{K(x)}(1+x)\big) = \nu(\mu_x(-1)) = \nu\Big(\sum_{k=0}^d (-1)^k a_k\Big) \leq \max_{0 \leq k \leq d} \nu(a_k) \leq 1$$

as desired. Thus $\tilde{\nu}$ is a valuation on L that extends ν. The uniqueness of $\tilde{\nu}$ is shown as in Case 2 with the help of Lemma III.10.12. From this, the completeness of $\tilde{\nu}$ also follows. □

Corollary III.10.41. *Let K be a field with a complete valuation ν. Then there exists exactly one valuation $\tilde{\nu}$ of the algebraic closure $\overline{K}$ that extends ν.*

Proof. For every finite field extension $K \subseteq L$ with $L \subseteq \overline{K}$, let ν_L be the extension of ν uniquely determined according to Theorem III.10.40. For $x, y \in \overline{K}$, $|K(x,y) : K| < \infty$ holds, since $K \subseteq \overline{K}$ is algebraic. Furthermore, $\nu_{K(x)}(x) = \nu_{K(x,y)}(x)$ holds. This shows that $\tilde{\nu}\colon \overline{K} \to \mathbb{R}$, $x \mapsto \nu_{K(x)}(x)$ is a valuation of $\overline{K}$ that extends ν. If ν' is another extension of ν, then $\tilde{\nu}$ and ν' must coincide on $K(x)$ for all $x \in \overline{K}$. Therefore, $\nu' = \tilde{\nu}$ holds. □

Remark III.10.42.

(i) Let $K := \mathbb{Q}_{[p]}$ and $\tilde{\nu}_p$ be the unique extension of $\hat{\nu}_p$ to $\overline{K}$.[6] Like ν_p, $\tilde{\nu}_p$ is also ultrametric. Let us assume that $\tilde{\nu}_p$ is discrete. Then there exists $x \in \overline{K}$ with $\langle \tilde{\nu}_p(x) \rangle = \tilde{\nu}_p(\overline{K}^\times)$. Since $\overline{K}$ is algebraically closed, there exists $y \in \overline{K}$ with $y^2 = x$. Furthermore, there exists $a \in \mathbb{Z}$ with $\tilde{\nu}_p(y) = \tilde{\nu}_p(x)^a$. Thus one has the contradiction $\tilde{\nu}_p(x) = \tilde{\nu}_p(y)^2 = \tilde{\nu}_p(x)^{2a}$. Therefore, $\tilde{\nu}_p$ is not discrete.

(ii) In contrast to Theorem III.10.40, $\tilde{\nu}_p$ is not complete (Exercise III.65). We show that algebraic closedness is preserved when passing again to the completion (Theorem III.10.45).

Lemma III.10.43 (Krasner)**.** *Let K be a field with a complete ultrametric valuation ν. Let $\overline{K}$ be the algebraic closure of K and $\tilde{\nu}$ the extension of ν to $\overline{K}$. Let $\alpha \in K[X]$ be irreducible and separable with roots $x_1, \ldots, x_d \in \overline{K}$. Let*

$$r := \min_{i \neq j} \tilde{\nu}(x_i - x_j).$$

For $y \in \overline{K}$ with $\tilde{\nu}(x_1 - y) < r$, $K(x_1) \subseteq K(y)$ holds.

[6] By construction, K, $\overline{K}$ and $\mathbb{C}$ have the same cardinality as the power set of $\mathbb{N}$. From Theorem A.5.4 it therefore follows that $\overline{K} \cong \mathbb{C}$.

Proof. Let $L := K(y)$. The splitting field $M \subseteq \overline{K}$ of α over L is a Galois extension according to Artin's Theorem I.10.9, since α is separable. The uniqueness of $\tilde{\nu}$ on M shows $\tilde{\nu}(\sigma(z)) = \tilde{\nu}(z)$ for all $z \in M$ and $\sigma \in G := \mathrm{Gal}(M|L)$. In particular,

$$\tilde{\nu}(\sigma(x_1) - y) = \tilde{\nu}(x_1 - \sigma^{-1}(y)) = \tilde{\nu}(x_1 - y) < r$$

and

$$\tilde{\nu}(x_1 - \sigma(x_1)) = \tilde{\nu}(x_1 - y + y - \sigma(x_1)) \leq \max\{\tilde{\nu}(x_1 - y), \tilde{\nu}(y - \sigma(x_1))\} < r.$$

By the definition of r, this is only possible if $\sigma(x_1) = x_1$. Overall, $x_1 \in M^G = L = K(y)$ as claimed. □

Corollary III.10.44. *With the same assumptions as in Lemma III.10.43 let $\alpha = \sum_{k=0}^{d} a_k X^k \in K[X]$. Then there exists an $\epsilon > 0$ with the following property: Every monic polynomial $\beta = \sum_{k=0}^{d} b_k X^k \in K[X]$ with $\nu(a_k - b_k) < \epsilon$ for $k = 0, \ldots, d$ is irreducible.*

Proof. Let $m := \max_{0 \leq k \leq d} \nu(a_k)$ and $\epsilon := \min\{1, r^d (m+1)^{-d}\} > 0$. Let β be as specified with root $y \in \overline{K}$. According to Exercise III.55 it holds that

$$\tilde{\nu}(y) \leq \max_{0 \leq k \leq d} \nu(b_k) \leq \max_{0 \leq k \leq d} \nu(a_k) + \max_{0 \leq k \leq d} \nu(a_k - b_k) < m + \epsilon \leq m + 1$$

and

$$\prod_{k=0}^{d} \tilde{\nu}(y - x_k) = \tilde{\nu}(\alpha(y)) = \tilde{\nu}((\alpha - \beta)(y)) \leq \max_{0 \leq k \leq d} \nu(a_k - b_k) \tilde{\nu}(y)^k < \epsilon (m+1)^d.$$

Thus there exists a k with $\tilde{\nu}(y - x_k) < \sqrt[d]{\epsilon}(m+1) \leq r$. From Krasner's Lemma it follows that $K(x_k) \subseteq K(y)$. On the other hand $|K(y) : K| \leq \deg \beta = d = |K(x_k) : K|$. This shows $K(x_k) = K(y)$ and β is irreducible. □

Theorem III.10.45 (Kürschák)**.** *Let K be an algebraically closed field with valuation ν. Then the completion $\hat{K}$ with respect to ν is also algebraically closed.*

Proof. If ν is archimedean, then $\mathbb{R} \subseteq \hat{K} \subseteq \mathbb{C}$ according to Ostrowski. Since $X^2 + 1$ already has a root in the algebraically closed field K, the case $\hat{K} \cong \mathbb{R}$ cannot occur. Thus $\hat{K} \cong \mathbb{C}$ is algebraically closed.

Now let ν be ultrametric. We first show that $\hat{K}$ is perfect (Definition I.11.19). For this we can assume $\mathrm{char}\, K = p > 0$. Let $x \in \hat{K}$. Since K is dense in $\hat{K}$, x is the limit of a sequence from K, say $x = \lim_{n \to \infty} x_n$. Since K is algebraically closed, there exist $y_n \in K$ with $y_n^p = x_n$. Because of

$$\nu(y_k - y_l)^p = \nu\big((y_k - y_l)^p\big) = \nu(y_k^p - y_l^p) = \nu(x_k - x_l)$$

(y_n) is also a Cauchy sequence. For $y := \lim_{n \to \infty} y_n \in \hat{K}$ it obviously holds that $y^p = x$. Thus $\hat{K}$ is perfect.

Assume $\hat{K}$ is not algebraically closed. Then there exists an irreducible polynomial $\alpha \in \hat{K}[X]$ of degree $d > 1$. According to Example II.3.3 α is separable. Since K is dense in $\hat{K}$, we find a polynomial $\beta \in K[X]$ whose coefficients are arbitrarily close to the corresponding coefficients of α. According to Corollary III.10.44 we can achieve that β is irreducible and also has degree d. But then K would not be algebraically closed. □

Example III.10.46. Let K be the completion of $\overline{\mathbb{Q}_{[p]}}$. Then K is both algebraically closed and complete. Let R be the valuation ring of K and $\overline{R} := R/\mathrm{J}(R)$. Let $\alpha \in \overline{R}[X] \setminus \overline{R}$. Then there exists $\beta \in R[X] \setminus R$ with $\overline{\beta} = \alpha$. Since K is algebraically closed, β has a root $x \in K$. According to Exercise III.55, $x \in R$ and $\overline{x}$ is a root of α. This shows that $\overline{R}$ is also algebraically closed.

Remark III.10.47. Let K be a number field of degree $n := |K : \mathbb{Q}|$. Because $\operatorname{char} K = 0$, there exist exactly n (injective) homomorphisms $\sigma\colon K \to \mathbb{C}$ according to Exercise II.18. In the case $\sigma(K) \subseteq \mathbb{R}$, σ is called a *real embedding* of K and otherwise a *complex embedding*. The complex embeddings occur in pairs of the form $(\sigma, \overline{\sigma})$, where $\overline{\sigma}(x) := \overline{\sigma(x)}$ holds for $x \in K$.

Lemma III.10.48. *Let K be a number field and $\sigma, \tau\colon K \to \mathbb{C}$ be embeddings with $|\sigma(x)| = |\tau(x)|$ for all $x \in K$. Then $\sigma \in \{\tau, \overline{\tau}\}$ holds.*

Proof. Let $\gamma := \sigma \circ \tau^{-1}\colon \tau(K) \to \sigma(K)$. For $x, y \in K$ we have

$$|\sigma(x) - \sigma(y)| = |\sigma(x - y)| = |\tau(x - y)| = |\tau(x) - \tau(y)|.$$

This shows that γ is continuous with respect to the Euclidean valuation. One can now extend γ to the completion $\widehat{\tau(K)}$ by defining $\hat{\gamma}(x) := \lim_{n\to\infty} \gamma(x_n)$ for every Cauchy sequence $(x_n)_n$ in $\tau(K)$ (this is well-defined since γ maps null sequences to null sequences). It is easy to show that $\hat{\gamma}\colon \widehat{\tau(K)} \to \widehat{\sigma(K)}$ is an isomorphism. According to Ostrowski, $\widehat{\tau(K)} = \widehat{\sigma(K)} \in \{\mathbb{R}, \mathbb{C}\}$ holds. Since $\mathbb{Q}$ lies in the fixed field of γ, $\mathbb{R}$ lies in the fixed field of $\hat{\gamma}$. From this it follows that $\hat{\gamma} = \mathrm{id}$ or $\hat{\gamma}$ is the complex conjugation on $\mathbb{C}$. □

Theorem III.10.49. *Let K be a number field. Let $\sigma_1, \ldots, \sigma_r$ be the real embeddings of K and let $\tau_1, \ldots, \tau_s$ be representatives for the pairs of complex embeddings. Then every Archimedean valuation of K is equivalent to exactly one of the valuations $x \mapsto |\sigma_i(x)|$ or $x \mapsto |\tau_i(x)|$.*

Proof. Let ν be an archimedean valuation of K. According to Ostrowski, there exists a homomorphism $\gamma\colon \hat{K} \to \mathbb{C}$ and $s > 0$ with $\hat{\nu}(x) = |\gamma(x)|^s$ for all $x \in K$. Thus ν is equivalent to one of the specified valuations. Now let σ and τ be arbitrary embeddings of K and $s > 0$ with $|\sigma(x)| = |\tau(x)|^s$ for all $x \in K$. For $x = 2$ one obtains $2 = |\sigma(2)| = |\tau(2)|^s = 2^s$ and $s = 1$. From Lemma III.10.48 it now follows that $\sigma \in \{\tau, \overline{\tau}\}$. Thus the specified valuations are pairwise non-equivalent. □

Remark III.10.50. The ultrametric valuations of a number field K arise by choosing a prime ideal $P \trianglelefteq \mathbb{Z}_K$ as described in Example III.10.3.

Lemma III.10.51. *Let K be a field with ultrametric valuation ν and valuation ring R. Let V be a K-vector space and $W \subseteq V$ a finitely generated R-module. Then there exist linearly independent elements $b_1, \ldots, b_n \in W$ over K with $W = Rb1 + \ldots + Rb_n$.*

Proof. According to Theorem III.10.9, $P := \mathrm{J}(R)$ is a maximal ideal. As in the proof of Theorem II.9.7, we can consider W/PW as an R/P-vector space. Since W is finitely generated, there exists a basis $b_1 + PW, \ldots, b_n + PW$ of W/PW over R/P. Consequently $W = Rb_1 + \ldots + Rb_n + PW$. As a vector space, W/PW is semisimple and $\mathrm{J}(W) \subseteq PW$. Nakayama's Lemma therefore yields $R = Rb_1 + \ldots + Rb_n$. Suppose there exist $\lambda_1, \ldots, \lambda_n \in K$ (not all 0) with $\lambda_1 b_1 + \ldots + \lambda_n b_n = 0$. Let $\mu := \max_{1 \le i \le n} \nu(\lambda_i) > 0$. Then $\frac{\lambda_1}{\mu} b_1 + \ldots + \frac{\lambda_n}{\mu} b_n + PW = 0$ holds in W/PW and it follows that $\frac{\lambda_i}{\mu} \in P$ for $i = 1, \ldots, n$. This gives the contradiction $\nu(\lambda_i) < \mu$ for $i = 1, \ldots, n$. Thus $b_1, \ldots, b_n$ are linearly independent over K. □

Remark III.10.52. For every finite group G, there exists a number field K according to Theorem II.14.44 which is a splitting field for G. Let $\Delta\colon G \to \mathrm{GL}(n, K)$ be a representation and $V := K^n$ the corresponding KG-module. Let $p \in \mathbb{P}$ and $P \trianglelefteq \mathbb{Z}_K$ be a maximal ideal with $p \in P$. The P-adic valuation on K is ultrametric with valuation ring R. Let $e_1, \ldots, e_n \in K^n$ be the standard basis and $W \subseteq V$ the R-module generated by the elements ge_i ($g \in G$, $1 \leq i \leq n$). According to Lemma III.10.51, there exist linearly independent elements $b_1, \ldots, b_n \in W$ over K with $W = Rb_1 + \ldots + Rb_n$. Because of $e_1, \ldots, e_n \in W$, $b_1, \ldots, b_n$ is a K-basis of V. For $g \in G$, $gb_i \in W$ is an R-linear combination of $b_1, \ldots, b_n$. Through the change of basis $\{e_1, \ldots, e_n\} \to \{b_1, \ldots, b_n\}$, one obtains a representation $\Gamma\colon G \to \mathrm{GL}(n, R)$ similar to Δ. With the reduction modulo P, a representation $\overline{\Gamma}\colon G \to \mathrm{GL}(n, R/P)$ arises with entries in the finite field R/P of characteristic p. If one replaces K with the field from Example III.10.46, one achieves that K and R/P are algebraically closed.

III.11 General Galois Theory

Remark III.11.1. In this section, we develop three extensions of the Fundamental Theorem of Galois Theory: for certain algebras, for division rings, and for infinite field extensions.

Definition III.11.2. Let $K \subseteq L$ be a field extension and $G \leq \mathrm{Gal}(L|K)$.

- For a G-set S, let
$$\mathrm{Hom}_G(S, L) := \big\{\varphi\colon S \to L : \forall s \in S, g \in G : \varphi({}^g s) = g(\varphi(s))\big\}.$$
- Two G-sets S and T are called *isomorphic* if there exists a bijection $\varphi\colon S \to T$ with ${}^g\varphi(s) = \varphi({}^g s)$ for all $g \in G$ and $s \in S$.
- For two K-algebras A and B, let $\mathrm{Alg}_K(A, B)$ be the set of algebra homomorphisms $A \to B$.
- A K-algebra A is called *L-separated*, if for every two distinct elements $x, y \in A$ there exists an $f \in \mathrm{Alg}_K(A, L)$ with $f(x) \neq f(y)$.

Remark III.11.3.

(i) One easily shows that $\mathrm{Hom}_G(S, L)$ with the component-wise operations $(\alpha \dot{+} \beta)(s) = \alpha(s) \dot{+} \beta(s)$ and $(\lambda\alpha)(s) = \lambda\alpha(s)$ for $\alpha, \beta \in \mathrm{Hom}_G(S, L)$, $s \in S$ and $\lambda \in K$ is a K-algebra.

(ii) Now let $K \subseteq L$ be a Galois extension and $G := \mathrm{Gal}(L|K)$. Let $R \subseteq S$ be a system of representatives for the orbits of G on S. For $r \in R$ let G_r be the stabilizer of r. For $g \in G_r$ and $\varphi \in \mathrm{Hom}_G(S, L)$ it holds that $g(\varphi(r)) = \varphi({}^g r) = \varphi(r) \in L^{G_r}$. Conversely, if $x_r \in L^{G_r}$ for $r \in R$ are given, then there exists exactly one $\varphi \in \mathrm{Hom}_G(S, L)$ with $\varphi(r) = x_r$ for $r \in R$. This shows
$$\dim_K \mathrm{Hom}_G(S, L) = \sum_{r \in R} |L^{G_r} : K| = \sum_{r \in R} |G : G_r| = \sum_{r \in R} |{}^G r| = |S|.$$

(iii) Every L-separated K-algebra is commutative, because for $x, y \in A$ and $f \in \mathrm{Alg}_K(A, L) =: S$ it holds that $f(xy) = f(x)f(y) = f(y)f(x) = f(yx)$. By ${}^g\varphi(a) := g(\varphi(a))$ for $g \in G$, $a \in A$ and $\varphi \in S$, S becomes a G-set. As in Dedekind's Lemma I.14.1, one shows that S is linearly independent over L. In particular, $|S| \leq \dim_K A$ holds.

Theorem III.11.4 (General Galois Correspondence)**.** *Let $K \subseteq L$ be a Galois extension and $G := \mathrm{Gal}(L|K)$. Then the maps $S \mapsto \mathrm{Hom}_G(S, L)$ and $A \mapsto \mathrm{Alg}_K(A, L)$ induce mutually inverse bijections between the set of isomorphism classes of finite G-sets and the set of K-isomorphism classes of finite-dimensional L-separated K-algebras.*

Proof. Let S be a finite G-set and $A := \mathrm{Hom}_G(S, L)$. According to Remark III.11.3, $\dim_K A = |S| < \infty$. Let $\alpha, \beta \in A$ and $s \in S$ with $\alpha(s) \neq \beta(s)$. Obviously, the map $\Gamma_s \colon A \to L$, $\varphi \mapsto \varphi(s)$ is a homomorphism of K-algebras with $\Gamma_s(\alpha) \neq \Gamma_s(\beta)$. Therefore, A is L-separated. Let $T := \mathrm{Alg}_K(A, L)$ and $\Gamma \colon S \to T$, $s \mapsto \Gamma_s$. Let $s, s' \in S$ with $s \neq s'$. If s and s' are in different orbits of G, then by Remark III.11.3 there exists a $\varphi \in A$ with

$$\Gamma_s(\varphi) = \varphi(s) = 0 \neq 1 = \varphi(s') = \Gamma_{s'}(\varphi).$$

Otherwise, we choose $g \in G \setminus G_s$ with ${}^g s = s'$ and $x \in L^{G_s} \setminus L^g$. Then there exists a $\varphi \in A$ with $\varphi(s) = x$ and $\varphi(s') = {}^g\varphi(s) = {}^g x \neq x = \varphi(s)$. In both cases, $\Gamma_s \neq \Gamma_{s'}$ holds and Γ is injective. Because $|T| \leq \dim_K A = |S|$, Γ is also surjective. For $g \in G$ and $s \in S$, finally $\Gamma_{{}^g s}(\varphi) = \varphi({}^g s) = {}^g\varphi(s) = {}^g\Gamma_s(\varphi)$ and $\Gamma({}^g s) = {}^g\Gamma(s)$. This shows that S and T are isomorphic G-sets.

Conversely, let A be a finite-dimensional L-separated K-algebra. According to Remark III.11.3, $S := \mathrm{Alg}_K(A, L)$ is a finite G-set. Let $B := \mathrm{Hom}_G(S, L)$ and $\Gamma \colon A \to B$, $a \mapsto \Gamma_a$ with $\Gamma_a(f) := f(a)$ for $f \in S$. For $g \in G$, it holds that

$$\Gamma_a({}^g f) = {}^g f(a) = g(f(a)) = g(\Gamma_a(f)) = {}^g\Gamma_a(f).$$

Therefore, Γ is well-defined. As usual, Γ is a homomorphism of K-algebras. For distinct $a, b \in A$, there exists an $f \in S$ with $f(a) \neq f(b)$, since A is L-separated. This shows the injectivity of Γ. According to Remark III.11.3, $\dim B = |S| \leq \dim A$ and Γ is also surjective. It follows that the specified maps are bijections inverse to each other. □

Example III.11.5. In the situation of Theorem III.11.4, let S be a finite transitive G-set and $s \in S$. Then the map $\Gamma \colon \mathrm{Hom}_G(S, L) \to L^{G_s}$, $\varphi \mapsto \varphi(s)$ is a homomorphism of K-algebras. According to Remark III.11.3, Γ is even an isomorphism of fields. On the other hand, according to the proof of Theorem I.4.7, $G/G_s \to S$, $gG_s \mapsto {}^g s$ is an isomorphism of G-sets, where G acts by left multiplication on G/G_s. In this way, one obtains a bijection between the K-isomorphism classes of intermediate fields. We prove a more general correspondence for skew fields in Theorem III.11.21.

Remark III.11.6. Let $R \subseteq S$ be an extension of skew fields. According to Theorem II.9.10, S can be understood as a free R-left module or R-right module. For better distinction, we write ${}_R S$ and S_R, respectively. As mentioned in Remark II.9.12, the dimensions $\dim({}_R S)$ and $\dim(S_R)$ do not necessarily coincide. Let V be an S-module. Then, as with fields, the degree theorem $\dim({}_R V) = \dim({}_S V)\dim({}_R S)$ and $\dim(V_R) = \dim(V_S)\dim(S_R)$ holds (see proof of Theorem I.9.5). In the case $R \subseteq \mathrm{Z}(S)$, every basis of the R-left module S is also a basis of the R-right module. Thus, $\dim_R(S) = \dim({}_R S) = \dim(S_R)$ holds.

Theorem III.11.7. *Let $R \subseteq S$ be an extension of skew fields with $\dim_{\mathrm{Z}(S)}(S) < \infty$. Then $\dim({}_R S) = \dim(S_R)$ holds.*

Proof. Let $Z := \mathrm{Z}(S)$ and

$$A := \Big\{ \sum_{i=1}^{n} \lambda_i z_z : n \in \mathbb{N},\ \lambda_1, \ldots, \lambda_n \in R,\ z_1, \ldots, z_n \in Z \Big\}$$

be the subring in S generated by Z and R. Then A as an R-left module possesses a basis with elements from Z. Obviously, this is also a basis of A as an R-right module. At the same time, A is a finite-dimensional Z-vector space. For $a \in A \setminus \{0\}$, the Z-linear map $f_a \colon A \to A$, $x \mapsto ax$ is injective, since S

is a skew field. Because of $\dim_Z(A) \leq \dim_Z(S) < \infty$, f_a is also surjective and it follows that $a^{-1} \in A$. Thus A is a skew field. From Remark III.11.6 it follows that

$$\begin{aligned}\dim({}_RS) &= \dim({}_AS)\dim({}_RA) = \frac{\dim({}_AS)\dim_Z(A)}{\dim_Z(A)}\dim(A_R) = \frac{\dim_Z(S)}{\dim_Z(A)}\dim(A_R)\\ &= \dim(S_A)\dim(A_R) = \dim(S_R).\end{aligned}$$

□

Remark III.11.8.

(i) Let S be a skew field and $\mathrm{End}(L,+)$ the endomorphism ring of the abelian group $(L,+)$. For $s \in S$ and $\varphi \in \mathrm{End}(L,+)$, let $\varphi s\colon S \to S$, $x \mapsto \varphi(x)s$. Obviously, $\varphi s \in \mathrm{End}(L,+)$ and $\mathrm{End}(L,+)$ becomes an S-right module in this way.

(ii) Now let $R \subseteq S$ be an extension of skew fields and $E := \mathrm{End}({}_RS)$ the ring of all R-linear maps $S \to S$. Obviously, E is an S-submodule of $\mathrm{End}(L,+)$. If B is a basis of ${}_RS$, then the "dual basis" $\{b^* : b \in B\}$ with $b^*(c) := \delta_{bc}$ for $c \in B$ is a basis of E_S. Thus, $\dim({}_RS) = \dim(E_S)$ holds.

(iii) For $G \leq \mathrm{Aut}(S)$, let as usual

$$S^G := \{s \in S : \forall g \in G : g(s) = s\} \subseteq S$$

be the *fixed skew field* of G in S. In the case $R \subseteq S^G$, we have $G \subseteq E$ and one can form the S-span $GS \leq E_S$.

(iv) Let $E^* := \mathrm{Hom}(E_S, S_S)$ be the set of homomorphisms between the S-right modules E and S. For $\lambda \in S$, one has the "dual map" $\lambda^* \in E^*$ with $\lambda^*(f) := f(\lambda)$. For $\Gamma \in E^*$ and $s \in S$, $s\Gamma \in E^*$ with $(s\Gamma)(f) := s\Gamma(f)$. In this way, E^* becomes an S-left module. Analogously, one defines $(GS)^*$.

(v) Let V be a (left or right) module over a skew field R with basis B. For $u \in U \leq V$, let $B(u) \subseteq B$ be minimal with $u \in \langle B(u)\rangle$. We call $u \neq 0$ *minimal with respect to* B if $U \cap \langle B(u)\rangle = \langle u\rangle$ holds. According to Exercise III.66, the minimal elements form a generating system of U.

Lemma III.11.9 (Ninot)**.** *Let S be a skew field, $G \leq \mathrm{Aut}(S)$ and $R := S^G$. For $s_1, \ldots, s_n \in S$, the following are equivalent:*

(1) $s_1, \ldots, s_n$ are linearly independent in ${}_RS$.

(2) $s_1^*, \ldots, s_n^*$ are linearly independent in ${}_S(GS)^*$.

Proof. (1) ⇒ (2)**:** Let

$$U := \left\{(\lambda_1, \ldots, \lambda_n) \in S^n : \sum_{i=1}^n \lambda_i s_i^* = 0\right\} \leq {}_S(S^n).$$

We assume indirectly $U \neq 0$ and choose $(\lambda_i)_i \in U \setminus \{0\}$ minimal with respect to the standard basis of S^n (Remark III.11.8). Wlog. let $\lambda_1 = 1$. For $f \in GS$ we have

$$0 = \sum_{i=1}^n (\lambda_i s_i^*)(f) = \sum_{i=1}^n \lambda_i f(s_i).$$

We apply $\sigma \in G$ to this:

$$0 = \sum_{i=1}^n \sigma(\lambda_i)\sigma f(s_i) = \sum_{i=1}^n \sigma(\lambda_i) s_i^*(\sigma f).$$

Since σf runs through GS as f does, one obtains $(\sigma(\lambda_i))_i \in U$. From the minimality of $(\lambda_i)_i$ it follows that $\sigma(\lambda_i) = \mu\lambda_i$ for some $\mu \in S$ and $i = 1, \ldots, n$. Here $\mu = \mu\lambda_1 = \sigma(\lambda_1) = 1$ holds. This shows $(\lambda_i)_i \in (S^G)^n = R^n$. For $f = \mathrm{id}$ one finally has

$$0 = \sum_{i=1}^{n} (\lambda_i s_i^*)(f) = \sum_{i=1}^{n} \lambda_i s_i.$$

The linear independence of $s_1, \ldots, s_n$ yields the contradiction $\lambda_1 = \ldots = \lambda_n = 0$.

(2) $\Rightarrow$ (1): Let $r_1, \ldots, r_n \in R$ with $\sum_{i=1}^{n} r_i s_i = 0$. For $\sigma \in G$ we have

$$0 = \sigma\Big(\sum_{i=1}^{n} r_i s_i\Big) = \sum_{i=1}^{n} r_i \sigma(s_i) = \sum_{i=1}^{n} r_i s_i^*(\sigma).$$

Since GS is generated by G, it follows that $\sum_{i=1}^{n} r_i s_i^* = 0$. By assumption $r_1 = \ldots = r_n = 0$. □

Theorem III.11.10. *Let S be a skew field, $G \leq \mathrm{Aut}(S)$ and $R := S^G$. Then $\mathrm{End}({}_R S) = GS$ holds.*

Proof. According to Remark III.11.8, $\dim(\mathrm{End}({}_R S)_S) = \dim({}_R S)$ holds and analogously $\dim({}_S(GS)^*) = \dim((GS)_S)$ (dual basis). From Lemma III.11.9 it therefore follows that $\dim(\mathrm{End}({}_R S)_S) \leq \dim((GS)_S)$. Due to $GS \leq \mathrm{End}({}_R S)$, equality holds. □

Definition III.11.11. Let $R \subseteq S$ be an extension of skew fields.

- As with fields, let
$$G := \mathrm{Gal}(S|R) := \{\gamma \in \mathrm{Aut}(S) : \forall r \in R : \gamma(r) = r\}$$
be the *Galois group* of S over R.
- We call $R \subseteq S$ a *Galois extension*, if $\dim({}_R S) < \infty$ and $S^G = R$ holds.
- For $s \in S^\times$ let $\rho_s \colon S \to S$, $x \mapsto sxs^{-1}$ be the *inner* automorphism of S induced by s. Then $\rho \colon S^\times \to \mathrm{Aut}(S)$, $s \mapsto \rho_s$ is a ring homomorphism. One calls $\mathrm{Inn}(S) := \rho(S^\times)$ the *inner automorphism group* of S. For $\alpha \in \mathrm{Aut}(S)$ and $s \in S^\times$ we have $\alpha\rho_s\alpha^{-1} = \rho_{\alpha(s)}$. This shows $\mathrm{Inn}(S) \trianglelefteq \mathrm{Aut}(S)$.
- A subgroup $H \leq G$ is called *closed*, if $\rho^{-1}(H) \cup \{0\}$ is a skew field.

Remark III.11.12. Since $\mathrm{Z}(S)^\times$ is the kernel of ρ, we have $\mathrm{Inn}(S) \cong S^\times/\mathrm{Z}(S)^\times$.

Example III.11.13. Apparently $\mathbb{R} \subseteq \mathbb{H}$ is a Galois extension, because $\dim_{\mathbb{R}}(\mathbb{H}) = 4$ and $\mathbb{H}^{\mathrm{Inn}(\mathbb{H})} = \mathrm{Z}(\mathbb{H}) = \mathbb{R}$. By Skolem-Noether, $G := \mathrm{Gal}(\mathbb{H}|\mathbb{R}) = \mathrm{Inn}(\mathbb{H})$ holds. In contrast to Galois extensions of fields, G can thus be infinitely large. We will see that the *outer* automorphism group $G\mathrm{Inn}(S)/\mathrm{Inn}(S)$ is always finite (Theorem III.11.16).

Lemma III.11.14. *Let S be a division ring and $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}(S)$ be linearly independent in $\mathrm{Aut}(L, +)_S$. Let $s_1, \ldots, s_n \in S^\times$ with*

$$\gamma := \sum_{i=1}^{n} \sigma_i s_i \in \mathrm{Aut}(S).$$

Then $\gamma = \rho_{s_i}^{-1}\sigma_i$ for $i = 1, \ldots, n$. In the case $\gamma = \rho_s$ for some $s \in S^\times$, then $\sigma_i = \rho_{s_i s}$ for $i = 1, \ldots, n$ holds.

Proof. For $s, t \in S$ we have

$$\gamma(s) = \gamma(st)\gamma(t)^{-1} = \sum_{i=1}^{n} (\sigma_i s_i)(st)\gamma(t)^{-1} = \sum_{i=1}^{n} \sigma_i(s)\big(\sigma_i(t) s_i \gamma(t)^{-1}\big).$$

Since the σ_i are linearly independent, it follows that $s_i = \sigma_i(t) s_i \gamma(t)^{-1}$ and $\gamma(t) = s_i^{-1}\sigma_i(t)s_i$ for all $t \in S$. This shows $\gamma = \rho_{s_i}^{-1}\sigma_i$ for $i = 1, \ldots, n$. The second statement follows by rearranging. □

Lemma III.11.15. *Let S be a division ring, $s, s_1, \ldots, s_n \in S^\times$ and $Z := \mathrm{Z}(S)$. Then the following are equivalent:*

(1) $s_1, \ldots, s_n$ are linearly independent in ${}_Z S$ and $s \in \mathrm{Span}_Z\{s_1, \ldots, s_n\}$

(2) $\rho_{s_1}, \ldots, \rho_{s_n}$ are linearly independent in $\mathrm{End}(S, +)_S$ and $\rho_s \in \mathrm{Span}_S\{\rho_{s_1}, \ldots, \rho_{s_n}\}$.

Proof. We first show only a part of (1)⇒(2): Let $s = \sum_{i=1}^n z_i s_i$ with $z_1, \ldots, z_n \in Z$. For $x \in S$ it holds that

$$\rho_s(x) = sxs^{-1} = \sum_{i=1}^{n} z_i s_i x s^{-1} = \sum_{i=1}^{n} \rho_{s_i}(x)(s_i z_i s^{-1})$$

and $\rho_s \in \mathrm{Span}_S\{\rho_{s_1}, \ldots, \rho_{s_n}\}$.

(2) ⇒ (1): Let $\rho_s = \sum_{i=1} \rho_{s_i}\lambda_i$ with $\lambda_1, \ldots, \lambda_n \in S$. From Lemma III.11.14 it follows that $\lambda_i = 0$ or $\rho_{s_i} = \rho_{\lambda_i s}$ for $i = 1, \ldots, n$. Thus there exist $z_1, \ldots, z_n \in Z$ with $z_i s_i = \lambda_i s$ for $i = 1, \ldots, n$ (in the case $\lambda_i = 0$ we have $z_i = 0$). Now it holds that

$$s = \rho_s(1)s = \sum_{i=1}^{n} \lambda_i s = \sum_{i=1}^{n} z_i s_i \in \mathrm{Span}_Z\{s_1, \ldots, s_n\}.$$

Assume now that $s_1, \ldots, s_n$ are linearly dependent. Wlog. let $s_1 = \sum_{i=2}^n z_i s_i$ with $z_2, \ldots, z_n \in Z$. From the first part of the proof it follows that $\rho_{s_1} \in \mathrm{Span}_L\{\rho_{s_2}, \ldots, \rho_{s_n}\}$ in contradiction to the linear independence of $\rho_{s_1}, \ldots, \rho_{s_n}$.

(1) ⇒ (2): It remains to show that $\rho_{s_1}, \ldots, \rho_{s_n}$ are linearly independent. Wlog. let $\rho_{s_2}, \ldots, \rho_{s_n}$ be linearly independent and $\rho_{s_1} \in \mathrm{Span}_S\{\rho_{s_2}, \ldots, \rho_{s_n}\}$. Because of (2)⇒(1) one obtains the contradiction $s_1 \in \mathrm{Span}_Z\{s_2, \ldots, s_n\}$. □

Theorem III.11.16. *Let $R \subseteq S$ be a Galois extension of skew fields and $G := \mathrm{Gal}(S|R)$. Then*

$$\boxed{\dim({}_R S) = \dim_{\mathrm{Z}(S)}(\mathrm{C}_S(R))|G : G \cap \mathrm{Inn}(S)|,}$$

where $\mathrm{C}_S(R)$ is the centralizer of R in S. In particular, $\boxed{\dim({}_R S) = \dim(S_R).}$

Proof. Let $\mathcal{C}$ be a basis of $C := \mathrm{C}_S(R)$ over $Z := \mathrm{Z}(S)$ and let $\Gamma \subseteq G$ be a system of representatives for $G/(G \cap \mathrm{Inn}(S))$. Let $E := \mathrm{End}({}_R S)$. Because of $\dim({}_R S) = \dim(E_S)$, it suffices to show that

$$B := \{\gamma\rho_c : c \in \mathcal{C},\ \gamma \in \Gamma\} \subseteq E$$

is a basis of E_S. If B is linearly dependent, then one finds a non-trivial linear combination

$$\gamma\rho_c = \sum_{(i,j)\in I} \gamma_j \rho_{c_i} s_{ij} \tag{III.11.1}$$

with $c, c_i \in \mathcal{C}$, $\gamma, \gamma_j \in \Gamma$ and $s_{ij} \in S^\times$ for $(i,j) \in I$. Here we can assume that the automorphisms $\gamma_j \rho_{c_i}$ on the right side are linearly independent in $E_S \subseteq \mathrm{End}(S,+)$. From Lemma III.11.14 it follows that $\gamma\rho_c = \rho_{s_{ij}}^{-1}\gamma_j\rho_{c_i}$ for all $(i,j) \in I$. Thus $\gamma \equiv \gamma_j \pmod{\mathrm{Inn}(S)}$ and $\gamma = \gamma_j$. Multiplying (III.11.1) from the left by γ^{-1}, one obtains $\rho_c \in \mathrm{Span}_S\{\rho_{c_1}, \ldots, \rho_{c_n}\}$, where we have replaced I by $\{1, \ldots, n\}$. From Lemma III.11.15 the contradiction $c \in \mathrm{Span}_Z\{c_1, \ldots, c_n\}$ follows.

Because of $E = GS$ (Theorem III.11.10) it remains to show that every $\sigma \in G$ is generated by B. Let $\gamma \in \Gamma$ with $\sigma \equiv \gamma \pmod{\mathrm{Inn}(S)}$. Then there exists a $c \in C$ with $\sigma = \gamma\rho_c$. Let $c_1, \ldots, c_n \in \mathcal{C}$ with $c \in \mathrm{Span}_Z\{c_1, \ldots, c_n\}$. From Lemma III.11.15 it follows that $\rho_c \in \mathrm{Span}_S\{\rho_{c_1}, \ldots, \rho_{c_n}\}$. Thus σ lies in $\mathrm{Span}_S B$.

For the second assertion, one considers analogously that $B' := \{\rho_c\gamma : c \in \mathcal{C}, \gamma \in \Gamma\}$ is a basis of ${}_S\mathrm{End}(S_R)$. □

Example III.11.17. If $R \subseteq Z := \mathrm{Z}(S)$ in the situation of Theorem III.11.16, then one obtains $\dim_R(Z) = |G : G \cap \mathrm{Inn}(S)|$, because $\dim_R(S) = \dim_Z(S)\dim_R(Z)$.

Theorem III.11.18. *Let $R \subseteq S$ be a Galois extension of skew fields and T a skew field with $R \subseteq T \subseteq S$. Then $T \subseteq S$ is also a Galois extension.*

Proof. Certainly $\dim({}_TS) \leq \dim({}_RS) < \infty$. Let $G := \mathrm{Gal}(S|R)$ and $H := \mathrm{Gal}(S|T) \leq G$. Let $\Gamma \subseteq G$ be a basis of $GS = \mathrm{End}({}_RS)_S$ (Theorem III.11.10). We choose $\varphi \in \mathrm{End}({}_TS) \leq GS$ minimal with respect to Γ (Remark III.11.8). Let $\varphi = \sum_{i=1}^n \gamma_i s_i$ with $\gamma_1, \ldots, \gamma_n \in \Gamma$ and $s_1, \ldots, s_n \in S^\times$. Wlog. let $s_1 := 1$. For $\lambda \in S$, the map $f_\lambda \colon S \to S$, $s \mapsto s\lambda$ lies in $\mathrm{End}({}_TS)$. Thus, $\varphi f_\lambda \in \mathrm{End}({}_TS)$ also holds with

$$(\varphi f_\lambda)(s) = \sum_{i=1}^n (\gamma_i s_i)(s\lambda) = \sum_{i=1}^n \gamma_i(s)\gamma_i(\lambda)s_i = \sum_{i=1}^n (\gamma_i\gamma_i(\lambda)s_i)(s)$$

for $s \in S$. From the minimality of φ, it follows that $\varphi f_\lambda = \varphi\mu$ for some $\mu \in S$. Thus $s_i\mu = \gamma_i(\lambda)s_i$ for $i = 1, \ldots, n$. In particular, $\mu = s_1\mu = \gamma_1(\lambda)$. Now it holds that

$$\varphi(\lambda) = \sum_{i=1}^n \gamma_i(\lambda)s_i = \Big(\sum_{i=1}^n s_i\Big)\gamma_1(\lambda)$$

for all $\lambda \in S$. Because $\varphi \neq 0$, $s := \sum_{i=1}^n s_i \in S^\times$ and

$$\varphi s^{-1} = \rho_s\gamma_1 \in \mathrm{End}({}_TS) \cap \mathrm{Aut}(S) = \mathrm{End}({}_TS) \cap G = H.$$

Since the minimal elements form a generating system of $\mathrm{End}({}_TS)$ (Exercise III.66), one obtains $\mathrm{End}({}_TS) = HS$. Now let $s \in S \setminus T$. Then one can extend $\{1, s\}$ to a basis B of ${}_TS$. We construct $f \in \mathrm{End}({}_TS)$ by $f(s) = 0$ and $f(b) = b$ for all $b \in B \setminus \{s\}$. Then there exist $s_1, \ldots, s_n \in S$ and $\sigma_1, \ldots, \sigma_n \in H$ with $f = \sum_{i=1}^n \sigma_i s_i$. If $\sigma_i(s) = s$ were true for all i, one would have the contradiction

$$f(s) = \sum_{i=1}^n \sigma(s)s_i = s\sum_{i=1}^n s_i = sf(1) = s.$$

This shows $S^H = T$. □

Theorem III.11.19 (Cartan-Jacobson)**.** *Let $R \subseteq S$ be a Galois extension of skew fields and $G := \mathrm{Gal}(S|R)$. Let $\mathcal{T}$ be the set of all skew fields T with $R \subseteq T \subseteq S$. Let $\mathcal{H}$ be the set of all closed subgroups of G. Then the maps $\mathcal{T} \to \mathcal{H}$, $T \mapsto \mathrm{Gal}(S|T)$ and $\mathcal{H} \to \mathcal{T}$, $H \mapsto S^H$ are mutually inverse, inclusion-reversing bijections.*

Proof (KASCH). Let $T \in \mathcal{T}$ and $H := \mathrm{Gal}(S|T) \leq G$. Because of $\rho^{-1}(H) = \mathrm{C}_S(T)^\times$, $H \in \mathcal{H}$ holds. According to Theorem III.11.18, $S^H = T$ holds. Conversely, let $H \in \mathcal{H}$ and $T := S^H \in \mathcal{T}$. According to Theorem III.11.10,

$$H \leq \mathrm{Gal}(S|T) \leq \mathrm{End}({}_T S) = HS.$$

For $c \in \mathrm{C}_S(T)$, $\rho_c \in \mathrm{Gal}(S|T)$ and there exist linearly independent elements $\gamma_1, \ldots, \gamma_n \in H$ and $s_1, \ldots, s_n \in S^\times$ with $\rho_c = \sum_{i=1}^n \gamma_i s_i$. According to Lemma III.11.14, $\gamma_i = \rho_{s_i c}$ with $s_i c \in \rho^{-1}(H)$ for $i = 1, \ldots, n$. According to Lemma III.11.15, $c \in \mathrm{Span}_{\mathrm{Z}(S)}(s_1 c, \ldots, s_n c)$. Because $H \in \mathcal{H}$, $\rho^{-1}(H) \cup \{0\}$ is a division ring. From $\mathrm{Z}(S)^\times \leq \rho^{-1}(H)$ it follows that $c \in \rho^{-1}(H)$ and $\mathrm{C}_S(T)^\times \subseteq \rho^{-1}(H)$.

Finally, let $\sigma \in \mathrm{Gal}(S|T)$. According to Lemma III.11.14, there exist $\gamma \in H$ and $s \in S^\times$ with $\sigma = \rho_s^{-1}\gamma$. Because $\rho_s = \gamma\sigma^{-1} \in \mathrm{Gal}(S|T)$, $s \in \mathrm{C}_S(T)^\times \subseteq \rho^{-1}(H)$ holds and it follows that $\sigma \in H$. Overall, $\mathrm{Gal}(S|S^H) = H$. This shows that the specified maps are inverse bijections to each other. Obviously, they are inclusion-reversing. □

Remark III.11.20.

(i) In the situation of Theorem III.11.19, $\rho^{-1}(H)$ lies between $\mathrm{Z}(S)$ and $\mathrm{C}_S(R)$. If G consists only of inner automorphisms, then ρ induces an isomorphism $\mathrm{C}_S(R)^\times/\mathrm{Z}(S)^\times \to G$. If applicable, the division rings between $\mathrm{Z}(S)$ and $\mathrm{C}_S(R)$ are in bijection with the closed subgroups of G. The map $T \mapsto \mathrm{C}_S(T)$ is then a bijection between $\mathcal{M}$ and the set of division rings C with $\mathrm{Z}(S) \subseteq C \subseteq \mathrm{C}_S(R)$.

(ii) In the case $Z := \mathrm{Z}(S) \subseteq R$, every element in G is an automorphism of the central simple Z-algebra S. According to Skolem-Noether, G then consists only of inner automorphisms and we are in the situation of (i).

(iii) If, on the other hand, $\mathrm{C}_S(R) = \mathrm{Z}(S)$, then every subgroup $H \leq G$ is closed, because $\rho^{-1}(H) = \mathrm{Z}(S)^\times$. This applies in particular if S is a field. In this case, one recovers the fundamental theorem of Galois theory.

Theorem III.11.21 (Extension Theorem)**.** *Let $R \subseteq S$ be a Galois extension of division rings and $G := \mathrm{Gal}(S|R)$. Let T_1, T_2 be division rings with $R \subseteq T_1, T_2 \subseteq S$. Then every R-linear ring isomorphism $\varphi\colon T_1 \to T_2$ can be extended to an element of G. In particular, T_1 and T_2 are R-isomorphic if and only if $\mathrm{Gal}(S|T_1)$ and $\mathrm{Gal}(S|T_2)$ are conjugate in G.*

Proof. Obviously, one can extend φ to $\mathrm{End}({}_R S)$ by extending a basis of ${}_R T$ to a basis of ${}_R S$ and choosing suitable images. However, we choose a basis $\Gamma \subseteq G$ of $\mathrm{End}({}_R S) = GS$. Let $\psi = \sum_{\gamma\in\Gamma} \gamma s_\gamma \in GS$ be an extension of φ such that as many s_γ as possible vanish. For $s, t \in T_1$, it holds that

$$\sum_{\gamma\in\Gamma} \gamma(s)\gamma(t)s_\gamma = \psi(st) = \varphi(st) = \psi(s)\varphi(t) = \sum_{\gamma\in\Gamma} \gamma(s)s_\gamma\varphi(t).$$

If there exists a $\gamma \in G$ with $\gamma(t)s_\gamma = s_\gamma\varphi(t)$ for all $t \in T_1$, then the claim holds with $\sigma = \rho_{s_\gamma}^{-1}\gamma \in G$ (note $s_\gamma \in \mathrm{C}_S(R)$). Let us therefore assume that there exist $\gamma \in G$ and $t \in T_1$ with $d := \gamma(t)s_\gamma - s_\gamma\varphi(t) \neq 0$. Then

$$\tilde{\psi} := \psi - \Big(\sum_{\delta\in\Gamma} \delta\delta(t)s_\delta - \psi\varphi(t)\Big)d^{-1}s_\gamma \in (G \setminus \{\gamma\})S$$

is also an extension of φ with fewer non-zero coefficients with respect to Γ. Contradiction.

Now let $\psi \in G$ be an extension of φ. Let $H_i := \mathrm{Gal}(S|T_i) \leq G$ for $i = 1, 2$. Then $\psi H_1 \psi^{-1} = \mathrm{Gal}(S|\psi(T_1)) = H_2$. Conversely, assume that H_1 and H_2 are conjugate by some $\sigma \in G$. According to Cartan-Jacobson, $\sigma(T_1) = \sigma(S^{H_1}) = S^{\sigma H_1 \sigma^{-1}} = S^{H_2} = T_2$. Thus T_1 and T_2 are R-isomorphic. □

Theorem III.11.22. *Let $R \subseteq S$ be a Galois extension of skew fields and $G := \mathrm{Gal}(S|R)$. Let $H \leq G$ be closed and $T := S^H$. Then $\mathrm{Gal}(T|R) \cong \mathrm{N}_G(H)/H$. $R \subseteq T$ is a Galois extension if and only if $\mathrm{N}_G(H)$ is contained in no closed proper subgroup of G.*

Proof. For $\sigma \in \mathrm{N}_G(H)$, we have $\sigma(T) = \sigma(S^H) = S^{\sigma H \sigma^{-1}} = S^H = T$ (cf. proof of Theorem I.10.11). Thus the restriction map $\Gamma\colon \mathrm{N}_G(H) \to \mathrm{Gal}(T|R)$ is a homomorphism with kernel $\mathrm{Gal}(S|T) = H$ (Theorem III.11.19). According to Theorem III.11.21, every automorphism in $\mathrm{Gal}(T|R)$ can be extended to a $\sigma \in G$. In this case, $\sigma H \sigma^{-1} = \mathrm{Gal}(S|\sigma(T)) = \mathrm{Gal}(S|T) = H$, i.e., $\sigma \in \mathrm{N}_G(H)$. Thus Γ is surjective and $\mathrm{N}_G(H)/H \cong \mathrm{Gal}(T|R)$. Now let $R \subseteq T$ be a Galois extension. Because $H \leq \mathrm{N}_G(H)$, it holds that

$$S^{\mathrm{N}_G(H)} = T^{\mathrm{N}_G(H)} = T^{\mathrm{Gal}(T|R)} = R = S^G.$$

According to Cartan-Jacobson, G is the smallest closed subgroup containing $\mathrm{N}_G(H)$. Conversely, if $R \subseteq T$ is not a Galois extension, then $T_1 := T^{\mathrm{N}_G(H)} \supsetneq R$ and $\mathrm{Gal}(S|T_1) < G$ is a closed subgroup containing $\mathrm{N}_G(H)$. □

Remark III.11.23. According to Theorem II.3.6 and Exercise II.23, a finite field extension $K \subseteq L$ is a Galois extension if and only if it is separable and normal. In this way, we will extend the definition of the Galois extension to infinite field extensions.

Lemma III.11.24. *Let $K \subseteq L \subseteq \overline{K}$ be field extensions, where $\overline{K}$ is the algebraic closure of K. $K \subseteq L$ is normal if and only if $\alpha(L) = L$ holds for all $\alpha \in \mathrm{Gal}(\overline{K}|K)$.*

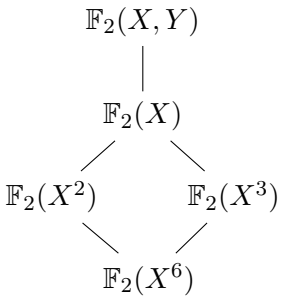
Proof. Let $x \in L$ and $\alpha \in \mathrm{Gal}(\overline{K}|K) =: G$. Then $\alpha(x)$ is a root of the minimal polynomial $\mu_x \in K[X]$. If $K \subseteq L$ is normal, it follows that $\alpha(x) \in L$ and $\alpha(L) \subseteq L$. According to Lemma I.9.11, $\alpha(L) = L$. Now assume that a root $y \in \overline{K}$ of μ_x does not lie in L. According to the extension theorem, there exists a K-isomorphism $K(x) \to K(y)$, which can be extended to an automorphism $\alpha \in G$ with $\alpha(L) \neq L$ using Theorem II.2.10 and Lemma I.9.11. □

Theorem III.11.25. *Let $K \subseteq L$ be an algebraic field extension and M the union of all normal field extensions of K in L. Then $K \subseteq M$ is a normal field extension.*

Proof. Let $x, y \in M$. Then there exist normal extensions $K \subseteq L_1$ and $K \subseteq L_2$ with $x \in L_1$ and $y \in L_2$. We can assume $L \subseteq \overline{K}$. Every element of the compositum L_1L_2 is a rational function in finitely many variables from L_2 and with coefficients from L_1 (Remark II.3.14). From Lemma III.11.24 it follows that $\alpha(L_1L_2) = L_1L_2$ for all $\alpha \in \mathrm{Gal}(\overline{K}|K)$. Thus $K \subseteq L_1L_2$ is a normal field extension. In particular, $x \dotplus y \in L_1L_2 \subseteq M$. This shows that M is a field. Obviously, $K \subseteq M$ is normal. □

Definition III.11.26. In the situation of Theorem III.11.25, M is called the *normal closure* of K in L.

Example III.11.27. Let $K := \mathbb{F}_2(X^6)$ and $L := \mathbb{F}_2(X, Y)$. Then $\mathbb{F}_2(X)$ is the algebraic closure of K in L. According to Exercise II.23, the extension $K \subseteq \mathbb{F}_2(X^3)$ of degree 2 is normal. On the other hand, $K \subseteq \mathbb{F}_2(X^2)$ is not normal, because the minimal polynomial $Y^3 - X^6 \in K[Y]$ of X^2 only splits into linear factors in $\mathbb{F}_4(X^2)$. Thus $\mathbb{F}_2(X^3)$ is the normal closure of K in L. On the other hand, $K \subseteq \mathbb{F}_2(X^2)$ is separable, because $(Y^3 - X^6)' = Y^2 \neq 0$, but $K \subseteq \mathbb{F}_2(X^3)$ is known to be inseparable. Therefore $\mathbb{F}_2(X^2)$ is the separable closure of K in L.



Theorem III.11.28. *For every algebraic field extension $K \subseteq L$, the following statements are equivalent:*

(1) $K \subseteq L$ is separable and normal.

(2) For every $x \in L$, the minimal polynomial $\mu_x \in K[X]$ splits into pairwise distinct linear factors in $L[X]$.

(3) $L^{\mathrm{Gal}(L|K)} = K$.

(4) L is the union of all intermediate fields $M \subseteq L$ such that $K \subseteq M$ is a finite Galois extension.

If applicable, we call $K \subseteq L$ a (possibly infinite) Galois extension.

Proof. Let $L \subseteq \overline{K}$ and $G := \mathrm{Gal}(L|K)$.

(1)⇔(2): Follows from the definition of separable and normal.

(2)⇒(3): Certainly $K \subseteq L^G$ holds. Let $x \in L \setminus K$. Then the minimal polynomial $\mu_x \in K[X]$ has another root $y \in L \setminus \{x\}$. By the extension theorem, there exists a K-isomorphism $K(x) \to K(y)$, which can be extended as usual to $\sigma \in \mathrm{Gal}(\overline{K}|K)$. By Lemma III.11.24, $\sigma_{|L} \in G$ with $\sigma(x) = y \neq x$. This shows $x \notin L^G$ and $L^G = K$.

(3)⇒(4): Let $x \in L$. Since G permutes the roots of μ_x, the set $N := \{\sigma(x) : \sigma \in G\} \subseteq L$ is finite. In particular, $\alpha := \prod_{y \in N}(X - y) \in L^G[X] = K[X]$ is well-defined. From $\mu_x \mid \alpha$ follows (2) and thus (1). By Theorem II.3.4, the finite, separable extension $K \subseteq K(x)$ can be embedded into a (finite) Galois extension.

(4)⇒(2): For $x \in L$ there exists a (finite) Galois extension $K \subseteq M$ with $x \in M$. Therefore μ_x already splits into pairwise distinct linear factors in $M[X]$. □

Theorem III.11.29. *For every infinite Galois extension $K \subseteq L$, $\mathrm{Gal}(L|K)$ is uncountable.*

Proof. According to Theorem III.11.28, there exist finite Galois extensions $K \subseteq L_i$ with $L = \bigcup_{i \in I} L_i$. By forming composita, one constructs an infinite sequence $K := L_0 \subsetneq L_1 \subsetneq \ldots$, such that all $K \subseteq L_i$ are finite Galois extensions. As usual, one shows that $M := \bigcup_{i \in \mathbb{N}} L_i$ is a Galois extension of K. Every K-automorphism $\sigma\colon M \to M$ extends to a K-automorphism $\hat{\sigma}\colon \overline{K} \to \overline{K}$. According to Lemma III.11.24, $\hat{\sigma}_{|L} \in \mathrm{Gal}(L|K) =: G$ is then an extension of σ. We can therefore assume $M = L$. According to the Fundamental Theorem of Galois Theory, $L_{i-1} \subsetneq L_i$ is a Galois extension. We choose $1 \neq \sigma_i \in \mathrm{Gal}(L_i|L_{i-1})$ for $i \in \mathbb{N}$. Let $\hat{\sigma}_i \in G$ be an extension of σ_i. For every infinite sequence $a = (a_i)_i \in \{0,1\}^{\mathbb{N}}$, we define $\sigma_a\colon L \to L$ by

$$\sigma_a(x) = \hat{\sigma}_1^{a_1} \hat{\sigma}_2^{a_2} \ldots \hat{\sigma}_k^{a_k}(x)$$

for $x \in L_k$. One easily sees that σ_a is a well-defined automorphism in G (Lemma I.9.11). Let $b = (b_i)_i \neq a$ be another sequence and $k = \min\{i \in \mathbb{N} : a_i \neq b_i\}$. Then there exists an $x \in L_k$ with $\sigma_k^{a_k}(x) \neq \sigma_k^{b_k}(x)$. It follows that $\sigma_a \neq \sigma_b$. Therefore $|G| \geq |\{0,1\}^{\mathbb{N}}|$ is uncountable. □

Example III.11.30.

(i) Let $\overline{K}$ be the algebraic closure of K and L the separable closure of K in $\overline{K}$. For $x \in L$, every root of the minimal polynomial $\mu_x \in K[X]$ is separable. Therefore, μ_x splits into linear factors in $L[X]$ and $K \subseteq L$ is a Galois extension. One calls $G := \mathrm{Gal}(L|K)$ the *absolute Galois group* of K. Let $\sigma \in G$ with order $k < \infty$. If $\mathrm{char}\, K = 0$, then $L = \overline{K}$ and $k \leq 2$ according to Corollary A.7.12. Now let $p := \mathrm{char}\, K > 0$. As usual, σ can be extended to $\hat{\sigma} \in \mathrm{Gal}(\overline{K}|K)$. According to Theorem II.3.8,

$L \subseteq \overline{K}$ is purely inseparable. For all $x \in \overline{K}$, there exists by Theorem II.3.11 an $n \in \mathbb{N}$ with $x^{p^n} \in L$. This shows

$$(\hat{\sigma}^k(x) - x)^{p^n} = \hat{\sigma}^k(x^{p^n}) - x^{p^n} = 0$$

and $\hat{\sigma}^k(x) = x$. Thus $\hat{\sigma}$ also has order k. From Corollary A.7.12 it follows that $\sigma = 1$, i. e. G is torsion-free.

(ii) Let us specifically consider $K = \mathbb{F}_q$ for a prime power $q \neq 1$. Suppose there exist $\sigma, \tau \in G := \mathrm{Gal}(\overline{K}|K)$ with $\sigma\tau \neq \tau\sigma$. Then there exists an $x \in \mathbb{F}_{q^n} \subseteq K$ with $\sigma\tau(x) \neq \tau\sigma(x)$. Since $\mathrm{Gal}(\mathbb{F}_{q^n}|K) \cong C_n$ is abelian, the restrictions of σ and τ to $\mathbb{F}_{q^n}$ must commute. This contradiction shows that G is a torsion-free abelian group. According to Theorem III.11.29, G is uncountable, while $\overline{K}$ is countable. In contrast to finite Galois extensions, it thus holds that $|G| > |\overline{K} : K|$.

(iii) Let $p \in \mathbb{P}$ and $\zeta_n := e^{2\pi\mathrm{i}/p^n} \in \mathbb{Q}_{p^n}$ for $n \in \mathbb{N}$. According to Theorem III.11.28,

$$\mathbb{Q}_{p^\infty} := \mathbb{Q}(\zeta_n : n \in \mathbb{N}) = \bigcup_{n \in \mathbb{N}} \mathbb{Q}_{p^n}$$

is an infinite Galois extension over $\mathbb{Q}$. For $\sigma \in G := \mathrm{Gal}(\mathbb{Q}_{p^n}|\mathbb{Q})$, there exist $a_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ with $\sigma(\zeta_n) = \zeta_n^{a_n}$ and $a_{n+1} \equiv a_n \pmod{p^n}$ for all $n \in \mathbb{N}$. This shows $G \cong \mathbb{Z}_{[p]}^\times$, where $\mathbb{Z}_{[p]}$ is the ring of p-adic integers (Definition III.10.19). Now let $p > 2$. According to Theorem I.8.34, there exists an $a \in \mathbb{Z}$ with $(\mathbb{Z}/p^2\mathbb{Z})^\times = \langle a + p^2\mathbb{Z} \rangle$. According to Exercise I.52, $(\mathbb{Z}/p^n\mathbb{Z})^\times = \langle a + p^n\mathbb{Z} \rangle$ holds for all $n \in \mathbb{N}$. For $\sigma \in G$ with $\sigma(\zeta_n) = \zeta_n^a$, it is then $\mathbb{Q}_{p^\infty}^\sigma = \mathbb{Q} = \mathbb{Q}_{p^\infty}^G$. The Fundamental Theorem of (finite) Galois theory thus does not transfer directly to infinite extensions.

(iv) For $\pi \subseteq \mathbb{P}$ let $\mathbb{Q}(\sqrt{\pi}) := \mathbb{Q}(\sqrt{p} : p \in \pi)$. Let π be finite at first. We show by induction on $|\pi|$ that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\pi})$ is a Galois extension of degree $2^{|\pi|}$. This is clear for $|\pi| \leq 1$. Let $q \in \pi$ and $\pi' := \pi \setminus \{q\}$. For $\omega \subseteq \pi$ let $p_\omega := \prod_{p \in \omega} p$. By induction, $\{\sqrt{p_\omega} : \omega \subseteq \pi'\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{\pi'})$. Suppose $\sqrt{q} \in \mathbb{Q}(\sqrt{\pi'})$. Then there exist $x_\omega \in \mathbb{Q}$ with $\sqrt{q} = \sum_{\omega \subseteq \pi'} x_\omega \sqrt{p_\omega}$. Let $r \in \omega \subseteq \pi'$ with $x_\omega \neq 0$. Let

$$x_1 := \sum_{\omega \subseteq \pi' \setminus \{r\}} x_{\omega \cup \{r\}} \sqrt{p_\omega}, \qquad x_2 := \sum_{\omega \subseteq \pi' \setminus \{r\}} x_\omega \sqrt{p_\omega}.$$

Then it holds that

$$q = \sqrt{q}^2 = (\sqrt{r}x_1 + x_2)^2 = rx_1^2 + x_2^2 + 2\sqrt{r}x_1x_2$$

with $x_1, x_2 \in \mathbb{Q}(\sqrt{\pi' \setminus \{r\}})$. By induction, $\sqrt{r} \notin \mathbb{Q}(\sqrt{\pi' \setminus \{r\}})$. This implies $x_1x_2 = 0$ and $x_2 = 0$ because $x_1 \neq 0$. Now it follows that $\sqrt{q} = \sqrt{r}x_1$. Since r was arbitrary, it even holds that $\sqrt{q} = x_\omega\sqrt{p_\omega}$ for some $\omega \subseteq \pi'$. Then $q = x_\omega^2 p_\omega$ would have two different prime factorizations. Thus $\sqrt{q} \notin \mathbb{Q}(\sqrt{\pi'})$ and $|\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}| = 2^{|\pi|}$ as claimed. As an (iterated) compositum of the Galois extensions $\mathbb{Q}(\sqrt{p})$ for $p \in \pi$, $\mathbb{Q}(\sqrt{\pi})$ is a Galois extension with $\mathrm{Gal}(\mathbb{Q}(\sqrt{\pi})|\mathbb{Q}) \cong C_2^{|\pi|}$ according to Theorem I.10.15. Therefore, $\mathbb{Q}(\sqrt{\mathbb{P}}) = \bigcup_{|\pi|<\infty} \mathbb{Q}(\sqrt{\pi})$ is also a Galois extension. For every subset $\pi \subseteq \mathbb{P}$ there exists a $\sigma_\pi \in G := \mathrm{Gal}(\mathbb{Q}(\sqrt{\mathbb{P}})|\mathbb{Q})$ with

$$\sigma_\pi(\sqrt{p}) = \begin{cases} \sqrt{p} & \text{if } p \in \pi, \\ -\sqrt{p} & \text{if } p \notin \pi. \end{cases}$$

Conversely, every $\tau \in G$ is uniquely determined by the images $\tau(\sqrt{p})$ for $p \in \mathbb{P}$. Thus $G \cong C_2^{\mathbb{N}}$. For $H := \langle \sigma_\pi : |\pi| < \infty \rangle < G$ it holds that $\mathbb{Q}(\sqrt{\mathbb{P}})^H = \mathbb{Q}$.

Theorem III.11.31. *Let $K \subseteq M \subseteq L$ be field extensions such that $K \subseteq L$ is a Galois extension. Let $G := \mathrm{Gal}(L|K)$ and $H := \mathrm{Gal}(L|M)$. Then:*

(i) $M \subseteq L$ is a Galois extension.

(ii) If $|M : K| < \infty$, then $|G : H| = |M : K|$.

(iii) $K \subseteq M$ is a Galois extension if and only if $H \trianglelefteq G$. In this case, $\mathrm{Gal}(M|K) \cong G/H$.

Proof.

(i) Let $x \in L$. According to Theorem III.11.28, the minimal polynomial $\mu_x \in K[X]$ splits into pairwise distinct linear factors in $L[X]$. The minimal polynomial of x over M divides μ_x and therefore also splits into pairwise distinct linear factors.

(ii) According to Exercise II.18, $|M : K|$ is the number of homomorphisms $\sigma\colon M \to \overline{L}$. Each of these homomorphisms extends to an isomorphism $\overline{L} \to \overline{L}$. According to Lemma III.11.24, these isomorphisms can be restricted to elements of G. Conversely, every $\sigma \in G$ can be restricted to M. For $\sigma, \tau \in G$, it holds that $\sigma H = \tau H$ if and only if σ and τ have the same restriction to M. This proves the claim.

(iii) In any case, $K \subseteq M$ is separable. Suppose that $K \subseteq M$ is normal. According to Lemma III.11.24, $\sigma(M) = M$ for all $\sigma \in G$. The restriction therefore yields a homomorphism $\Gamma\colon G \to \mathrm{Gal}(M|K)$ with kernel $H \trianglelefteq G$. As before, every K-automorphism $M \to M$ can be extended to an element of G. Therefore, Γ is surjective and $G/H \cong \Gamma(G) = \mathrm{Gal}(M|K)$.

Conversely, let $H \trianglelefteq G$. According to (i) and Theorem III.11.28, $M = L^H$ and $\sigma(M) = L^{\sigma H \sigma^{-1}} = L^H = M$ for all $\sigma \in G$ (cf. proof of Theorem I.10.11). According to Lemma III.11.24, $K \subseteq M$ is normal. □

Remark III.11.32. Let $K \subseteq L$ be a Galois extension with $G := \mathrm{Gal}(L|K)$. According to Theorem III.11.28, there exist finite Galois extensions $K \subseteq L_i$ with $L = \bigcup_{i \in I} L_i$. According to Theorem III.11.31, $H_i := \mathrm{Gal}(L|L_i) \trianglelefteq G$ with $|G : H_i| = |L_i : K| < \infty$ and $\bigcap_{i \in I} H_i = \mathrm{Gal}(L|\bigcup L_i) = 1$. Therefore, the homomorphism $G \to \times_{i \in I} G/H_i$, $g \mapsto (gH_i)_i$ is injective and G is isomorphic to a subgroup of $\times_{i \in I} G/H_i$. Groups with this property are called *residually finite*.

Definition III.11.33. Let $K \subseteq L$ be a Galois extension and $G := \mathrm{Gal}(L|K)$. Let

$$\mathcal{N} := \big\{\mathrm{Gal}(L|M) : K \subseteq M \text{ finite Galois extension}\big\}.$$

A subset $U \subseteq G$ is called *open*, if U is a union of (arbitrarily many) cosets gN with $g \in G$ and $N \in \mathcal{N}$. As usual, $A \subseteq G$ is called *closed*, if $G \setminus A$ is open.

Lemma III.11.34. *With the notation from Definition III.11.33, the open subsets form a topology on G, i. e. it holds that*

(i) $\varnothing$ and G are open.

(ii) The union of open sets is open.

(iii) The intersection of two open sets is open.

Proof. Obviously $\varnothing$ is open as an empty union and G is the trivial coset of $G \in \mathcal{N}$. By definition, (ii) holds. Let $g, h \in G$ and $N, M \in \mathcal{N}$ with $gN \cap hM \neq \varnothing$. For $x \in gN \cap hM$ it holds that

$$gN \cap hM = xN \cap xM = x(N \cap M).$$

Let $K \subseteq L_1$ and $K \subseteq L_2$ be finite Galois extensions with $N = \mathrm{Gal}(L|L_1)$ and $M = \mathrm{Gal}(L|L_2)$. According to Theorem I.10.15, $K \subseteq L_1L_2$ is a finite Galois extension with $\mathrm{Gal}(L|L_1L_2) = N \cap M$. From this follows (iii). □

Definition III.11.35. The topology from Lemma III.11.34 is called the *Krull topology* on G.

Example III.11.36. According to Remark III.11.32, there exist $N_i \in \mathcal{N}$ with $\bigcap_{i\in I} N_i = 1$. For $g \in G$

$$G \setminus \{g\} = G \setminus \bigcap_{i\in I} gN_i = \bigcup_{i\in I}(G \setminus gN_i) = \bigcup_{i\in I} \bigcup_{hN_i \neq gN_i} hN_i$$

is open. Therefore, every finite subset of G is closed. If G is finite, then the Krull topology is discrete, i. e. every subset is open and closed.

Theorem III.11.37 (Krull)**.** *Let $K \subseteq L$ be a Galois extension, $G := \mathrm{Gal}(L|K)$, $\mathcal{M} := \{M \text{ field} : K \subseteq M \subseteq L\}$ and $\mathcal{H} := \{H \leq G : H \text{ closed}\}$. Then the maps $M \mapsto \mathrm{Gal}(L|M)$ and $H \mapsto L^H$ are mutually inverse, inclusion-reversing bijections between $\mathcal{M}$ and $\mathcal{H}$.*

Proof. Let $M \in \mathcal{M}$ and $H := \mathrm{Gal}(L|M) \leq G$. According to Theorem III.11.28, there exist finite Galois extensions $K \subseteq L_i$ with $L = \bigcup_{i\in I} L_i$. According to Theorem III.11.31, $N_i := \mathrm{Gal}(L|L_i) \trianglelefteq G$ and $|G : N_i| = |L_i : K| < \infty$. For $\sigma \in G \setminus H$, there exist $i \in I$ and $x \in M \cap L_i$ with $\sigma(x) \neq x$. For $\tau \in N_i$, it holds that $\sigma\tau(x) = \sigma(x) \neq x$. Therefore, $\sigma \in \sigma N_i \subseteq G \setminus H$. Thus, $G \setminus H$ is open and $H \in \mathcal{H}$.

According to Theorem III.11.31, $M \subseteq L$ is a Galois extension and $L^H = M$. Conversely, let $H \in \mathcal{H}$ be given. Then $H \leq \mathrm{Gal}(L|L^H)$. Let $\sigma \in \mathrm{Gal}(L|L^H)$. Since H is closed, there exist finite Galois extensions $K \subseteq L_i$ and $g_i \in G$ with $G \setminus H = \bigcup_{i\in I} g_iN_i$, where $N_i := \mathrm{Gal}(L|L_i)$. Assume indirectly that $\sigma \notin H$. Then there exists $i \in I$ with $\sigma \in g_iN_i$. According to Artin, $L^H \subseteq L_iL^H$ is a finite Galois extension. Therefore, the restriction $\Phi\colon \mathrm{Gal}(L|L^H) \to \mathrm{Gal}(L_iL^H|L^H)$ is a well-defined homomorphism. Obviously, it holds that

$$(L_iL^H)^{\Phi(H)} = L^H = (L_iL^H)^{\mathrm{Gal}(L_iL^H|L^H)}.$$

From the Fundamental Theorem of Galois Theory, it follows that $\Phi(H) = \mathrm{Gal}(L_iL^H|L^H)$. In particular, there exists an $h \in H$ with $\Phi(\sigma) = \Phi(h)$. This shows $\sigma^{-1}h \in \mathrm{Gal}(L|L_i) = N_i$ and $h \in hN_i = \sigma N_i \subseteq G \setminus H$. Contradiction. Thus $H = \mathrm{Gal}(L|L^H)$ holds and the maps are mutually inverse bijections. As usual, they are inclusion-reversing. □

Corollary III.11.38. *Let $K \subseteq L$ be a Galois extension and H_1, H_2 finite subgroups of $\mathrm{Gal}(L|K)$. Then $L^{H_1} = L^{H_2}$ is equivalent to $H_1 = H_2$.*

Proof. According to Example III.11.36, H_1 and H_2 are closed. Therefore, it holds that

$$L^{H_1} = L^{H_2} \iff H_1 = \mathrm{Gal}(L|L^{H_1}) = \mathrm{Gal}(L|L^{H_2}) = H_2.$$ □

Corollary III.11.39. *Let $K \subseteq L$ be a Galois extension and $H \leq \mathrm{Gal}(L|K)$. H is open if and only if H is closed and $|G : H| < \infty$.*

Proof. Let H be open, say $H = \bigcup_{i\in I} g_i N_i$ with $g_i \in G$ and $N_i \in \mathcal{N}$. Then there exists an i with $1 \in g_i N_i = N_i \subseteq H$. It follows that $|G : H| \leq |G : N_i| < \infty$ and $G \setminus H = \bigcup_{x\in G\setminus H} xN_i$ is open, i. e. H is closed. Conversely, let H be closed and $|G : H| < \infty$. According to Krull, $H = \mathrm{Gal}(L|L^H)$ and $|L^H : K| = |G : H| < \infty$. According to Theorem II.3.4, there exists a finite Galois extension $K \subseteq M$ with $L^H \subseteq M$. Now $N := \mathrm{Gal}(L|M) \leq H$ is open and thus also $H = \bigcup_{h\in H} hN$. □

Example III.11.40.

(i) Let $H := \langle \sigma_\pi : |\pi| < \infty\rangle \leq G := \mathrm{Gal}(\mathbb{Q}(\sqrt{\mathbb{P}})|\mathbb{Q}) \cong C_2^{\mathbb{N}}$ from Example III.11.30. We can consider G/H as an $\mathbb{F}_2$-vector space. By choosing a basis, one finds $H \leq N \leq G$ with $|G : N| = 2$. If N were closed, one would have the contradiction

$$\mathbb{Q} = \mathbb{Q}(\sqrt{\mathbb{P}})^G \subsetneq \mathbb{Q}(\sqrt{\mathbb{P}})^N \subseteq \mathbb{Q}(\sqrt{\mathbb{P}})^H = \mathbb{Q}.$$

(ii) The inverse Galois problem mentioned in Remark I.12.18 is equivalent to the question of whether for every finite group G there exists a continuous epimorphism $\Gamma\colon \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to G$, where G is equipped with the discrete topology. The continuity of Γ guarantees that $N := \mathrm{Ker}(\Gamma)$ is closed. According to Krull, then $\mathrm{Gal}(\overline{\mathbb{Q}}|\overline{\mathbb{Q}}^N) = N$ and $G \cong \mathrm{Gal}(\overline{\mathbb{Q}}^N|\mathbb{Q})$ according to Theorem III.11.31.

Theorem III.11.41. *For field extensions $K \subseteq M_i \subseteq L$ with $i = 1, 2$, the following holds:*

(i) If $K \subseteq M_1$ is a Galois extension, then so is $M_2 \subseteq M_1M_2$ and it holds that

$$\boxed{\mathrm{Gal}(M_1M_2|M_2) \cong \mathrm{Gal}(M_1|M_1 \cap M_2).}$$

(ii) If $K \subseteq M_1$ and $K \subseteq M_2$ are Galois extensions, then so is $K \subseteq M_1M_2$ and

$$\boxed{\mathrm{Gal}(M_1M_2|M_1 \cap M_2) \cong \mathrm{Gal}(M_1|M_1 \cap M_2) \times \mathrm{Gal}(M_2|M_1 \cap M_2).}$$

(iii) Let $K \subseteq L$ be a Galois extension with $G := \mathrm{Gal}(L|K)$ and $H_1, H_2 \leq G$ closed. Then $\boxed{L^{H_1}L^{H_2} = L^{H_1\cap H_2}}$ *and* $\boxed{L^{H_1} \cap L^{H_2} = L^{\langle H_1,H_2\rangle}.}$

Proof.

(i) For $x \in M_1M_2$ there exist $y_1, \ldots, y_n \in M_1$ with $x \in M_2(y_1, \ldots, y_n)$. Since $K \subseteq M_1$ is separable, there exists a finite Galois extension $K \subseteq L_1$ with $K(y_1, \ldots, y_n) \subseteq L_1 \subseteq M_1$. We can argue as in Theorem I.10.15: L_1 is the splitting field of a separable polynomial $\alpha \in K[X]$. Since L_1M_2 is the splitting field of $\alpha \in M_2[X]$, $M_2 \subseteq L_1M_2$ is also a Galois extension with $x \in L_1M_2$. As a union of the fields L_1M_2, M_1M_2 is a Galois extension over M_2 according to Theorem III.11.28. According to Lemma III.11.24, the restriction

$$\Gamma\colon \mathrm{Gal}(M_1M_2|M_2) \to \mathrm{Gal}(M_1|M_1 \cap M_2) =: G$$

is well-defined and injective. Let $\sigma \in \mathrm{Gal}(M_1|M_1 \cap M_2)$. According to Theorem I.10.15, there exists exactly one extension $\hat{\sigma}_{L_1} \in \mathrm{Gal}(L_1M_2|M_2)$ of $\sigma_{|L_1} \in \mathrm{Gal}(L_1|L_1 \cap M_2)$. We define

$$\hat{\sigma}\colon M_1M_2 \to M_1M_2, \qquad x \mapsto \hat{\sigma}_{L_1}(x).$$

Let also $K \subseteq L_1'$ be a finite Galois extension with $x \in L_1'$. Then $K \subseteq L_1 \cap L_1'$ is also a Galois extension. Therefore, $\hat{\sigma}_{L_1}$ and $\hat{\sigma}_{L_1'}$ must coincide with σ on $L_1 \cap L_1'$. In particular, $\hat{\sigma}_{L_1}(x) = \hat{\sigma}_{L_1'}(x)$. This shows that $\hat{\sigma}$ is well-defined. As usual, one shows that $\hat{\sigma}$ is an automorphism in $\mathrm{Gal}(M_1M_2|M_2)$. Thus $\Gamma(\hat{\sigma}) = \sigma$ and Γ is surjective.

(ii) According to Theorem III.11.28, there exist finite Galois extensions $K \subseteq M_{ij}$ with $M_i = \bigcup_{j \in J_i} M_{ij}$ for $i = 1, 2$. According to Theorem I.10.15, $K \subseteq M_{1j}M_{2k}$ are finite Galois extensions for all $j \in J_1$ and $k \in J_2$. As in (i), one shows $M_1M_2 = \bigcup_{j \in J_1} \bigcup_{k \in J_2} M_{1j}M_{2k}$. Thus $K \subseteq M_1M_2$ is a Galois extension according to Theorem III.11.28. According to Theorem III.11.31, $M_1 \cap M_2 \subseteq M_1M_2$ is also a Galois extension. As usual, the map

$$\Gamma \colon \mathrm{Gal}(M_1M_2|M_1 \cap M_2) \to \mathrm{Gal}(M_1|M_1 \cap M_2) \times \mathrm{Gal}(M_2|M_1 \cap M_2),\ \sigma \mapsto (\sigma_{|M_1}, \sigma_{|M_2})$$

is a well-defined monomorphism. For $\sigma_i \in \mathrm{Gal}(M_i|M_1 \cap M_2)$, there exist extensions $\hat{\sigma}_i \in \mathrm{Gal}(M_1M_2|M_j)$ according to (i) for $\{i, j\} = \{1, 2\}$. Now $\hat{\sigma}_1\hat{\sigma}_2 \in \mathrm{Gal}(M_1M_2|M_1 \cap M_2)$ is a preimage of (σ_1, σ_2) under Γ. Thus Γ is an isomorphism.

(iii) Certainly $L^{H_1} \cap L^{H_2} = L^{\langle H_1, H_2 \rangle}$ and $L^{H_1}L^{H_2} \subseteq L^{H_1 \cap H_2}$. Since H_1 and H_2 are closed, it holds that

$$H_1 \cap H_2 \subseteq \mathrm{Gal}(L|L^{H_1 \cap H_2}) \subseteq \mathrm{Gal}(L|L^{H_1}L^{H_2}) \subseteq \mathrm{Gal}(L|L^{H_1}) \cap \mathrm{Gal}(L|L^{H_2}) = H_1 \cap H_2.$$

This shows $L^{H_1}L^{H_2} = L^{H_1 \cap H_2}$. □

III.12 Coding Theory

Remark III.12.1. With the DHM key exchange in Example I.2.25 and the RSA procedure in Example I.7.19, we had already encountered applications of algebra in cryptography. *Cryptology* includes, in addition to cryptography, also *cryptanalysis*, i.e., the science of decrypting data (e.g., decryption of the Enigma in the Second World War by Alan Turing). In *coding theory*, on the other hand, one deals with error detection and correction during the transmission of digital data over a noise-prone channel (e.g., mobile communications, WIFI, GPS). Motivated by a wide variety of application scenarios, this theory developed significantly more in breadth than in depth. A highlight is the existence and uniqueness of the so-called Golay codes. In addition to methods of algebra, statistical aspects are also relevant, which we will, however, only touch upon briefly.

Example III.12.2. Anyone who does not understand their conversation partner acoustically asks them to repeat what was said. The most obvious idea for error detection is therefore to send data twice. Instead of `mouse`, `mmoouussee` is sent. Due to a transmission error, this becomes `mhoouussee`. From the sequence `mh`, one can immediately determine that an error has occurred. However, this cannot be uniquely corrected, because besides `mouse`, `house` is also a possibility. If, on the other hand, we send each letter three times and receive `mmh`, one can assume that with higher probability the `h` is wrong. The disadvantage of this method is the linearly growing amount of data. We will get to know better procedures (cf. Exercise III.67).

Definition III.12.3. Let $2 \leq q < \infty$ and A be a set (*alphabet*) with q elements (*symbols*). The elements from the n-fold Cartesian product A^n are called *words*.

(i) A (*block*) *code* of *length* n is a non-empty subset $C \subseteq A^n$. The elements of C are called *codewords*.

(ii) For $x = (x_1, \ldots, x_n) \in A^n$ and $y = (y_1, \ldots, y_n) \in A^n$ let

$$d(x, y) := |\{i : x_i \neq y_i\}|$$

be the (HAMMING) *distance* of x and y.

(iii) One calls

$$d(C) := \inf\{d(x, y) : x, y \in C,\ x \neq y\}$$

the *minimum distance* of C (in the case $|C| = 1$ let $d(C) := \infty$).

(iv) For $x \in A^n$ and $e \geq 0$ let

$$K_e(x) := \{y \in A^n : d(x, y) \leq e\}$$

be the "ball" with radius e around x.

Remark III.12.4.

(i) Let $C \subseteq A^n$ be a code and S a set of data to be sent. The *encoding* is an injective mapping $\gamma\colon S \to C$. Since transmission errors can occur, one defines the *decoding* as a mapping $\gamma'\colon A^n \to S$ with $\gamma' \circ \gamma = \mathrm{id}_S$ (in the case of error-free transmission, γ' is thus the inverse mapping of γ). We

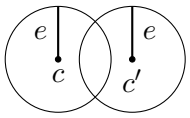
will assume wlog. $S = C$, $\gamma = \mathrm{id}_C$ and $\gamma' \colon A^n \to C$. Besides the construction of C, an efficient calculation of γ' is also one of the main tasks of coding theory.

(ii) For $x, y \in A^n$, $d(x,y) = d(y,x)$ and $d(x,y) = 0 \iff x = y$. If x and y differ at positions $i_1, \ldots, i_k$ and y and z differ at positions $j_1, \ldots, j_l$, then x and z can differ at most at the positions $\{i_1, \ldots, i_k\} \cup \{j_1, \ldots, j_l\}$. This shows the triangle inequality $d(x,z) \leq d(x,y) + d(y,z)$. The Hamming distance is therefore a metric in the sense of analysis.

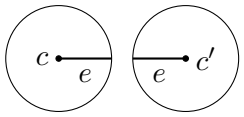
(iii) If exactly e errors occur during transmission, Bob receives a word $x \in A^n$ with $d(c,x) = e$ instead of the codeword $c \in C$. For Bob to be able to detect the occurrence of errors, $x \notin C$ must hold. For distinct $c, c' \in C$, $d(c,c') > e$ should therefore always hold, i. e. $d(C) > e$. For Bob to be able to correct all e errors, c must additionally be the only codeword with $d(c,x) \leq e$. In this case, $d(c,c') > 2e$ must hold for distinct $c, c' \in C$, because otherwise one could construct an $x \in A^n$ with $d(c,x), d(c',x) \leq e$. This justifies the following definition.

Definition III.12.5. A code C

(i) *detects* e errors if $d(C) > e$ holds.



(ii) *corrects* e errors if $d(C) > 2e$ holds.



Remark III.12.6. The correction of errors occurs under the statistical assumption that errors occur "rarely", independently and uniformly distributed (maximum likelihood decoding). In the case of scratches on CDs, this is generally not given, because a single scratch destroys many neighboring bits. In this case, one requires preprocessing, which we will not discuss in detail.

Example III.12.7.

(i) The *trivial* codes C with $|C| = 1$ can indeed correct every error ($d(C) = \infty$), but cannot transmit any information. Likewise, the code $C = A^n$ with minimum distance 1 is called *trivial*. Both are uninteresting in practice.

(ii) The *repetition code* $W_n(A) := \{(a, \ldots, a) \in A^n\}$ of length n has minimum distance n and can therefore detect $n-1$ errors and correct $\lfloor \frac{n-1}{2} \rfloor$ errors. For example, the word (a,a,a,b,b,b) cannot be uniquely corrected. If more than $n/2$ errors occur, it is even "corrected" incorrectly!

Definition III.12.8. One calls $H \in \{\pm 1\}^{n \times n}$ a HADAMARD *matrix*, if $HH^{\mathrm{t}} = n1_n$ holds.

Example III.12.9. Certainly $H_1 := (1)$ and $H_2 := \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ are Hadamard matrices. If H_n and H_m are Hadamard matrices of format $n \times n$ and $m \times m$ respectively, then the Kronecker product $H_n \otimes H_m$ is an $nm \times nm$ Hadamard matrix, because

$$(H_n \otimes H_m)(H_n \otimes H_m)^{\mathrm{t}} = H_n H_n^{\mathrm{t}} \otimes H_m H_m^{\mathrm{t}} = nm1_{nm}.$$

In particular, one obtains through $H_{2^n} := H_2 \otimes \ldots \otimes H_2$ a $2^n \times 2^n$ Hadamard matrix, which coincides with the character table of C_2^n (Example II.14.41).

Lemma III.12.10. *If $H \in \{\pm 1\}^{n \times n}$ is a Hadamard matrix with $n > 2$, then $4 \mid n$.*

Proof. By permuting rows and columns, H remains a Hadamard matrix. We can therefore assume that the first three rows of H have the form

$$\begin{pmatrix} 1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \\ 1 & \cdots & \cdots & \cdots & \cdots & 1 & -1 & \cdots & \cdots & \cdots & \cdots & -1 \\ 1 & \cdots & 1 & -1 & \cdots & -1 & 1 & \cdots & 1 & -1 & \cdots & -1 \end{pmatrix}$$

have. From the orthogonality of the rows, it follows easily that the four sections of the third row are all of equal length. □

Remark III.12.11. An open conjecture states that for every $k \geq 1$ Hadamard matrices of format $4k \times 4k$ exist (so far, no Hadamard matrix of size 668×668 is known).

Theorem III.12.12. *Let H be an $n \times n$ Hadamard matrix. Then the rows of H and $-H$ form a code C with $2n$ elements and minimum distance $\frac{n}{2}$.*

Proof. For distinct rows v and w of H, it holds that $vw^{\mathrm{t}} = 0 = (-v)w^{\mathrm{t}}$. This shows $|C| = 2n$ and $d(v, w) = n/2 = d(C)$. □

Remark III.12.13.

(i) Let H be an $n \times n$ Hadamard matrix and C the corresponding code. According to Theorem III.12.12, C can correct at least $\frac{n}{4} - 1$ errors. We construct a decoding function $\gamma' \colon \{\pm 1\}^n \to C$ as follows: For $x \in \{\pm 1\}^n$, let x_k be an entry of Hx^{t} with the largest absolute value. We define $\gamma(x)$ as the k-th row of $\pm H$, where $\pm$ is the sign of x_k. If x deviates from a codeword c in $e < \frac{n}{4}$ coordinates, then

$$|x_k| \geq xc^{\mathrm{t}} = n - 2e > \frac{n}{2}.$$

Since every other codeword differs from c in $\frac{n}{2}$ coordinates, $|x_l| \leq \frac{n}{2}$ holds for all $l \neq k$. This shows $\gamma'(x) = c$.

(ii) The code constructed in Theorem III.12.12 for $n = 32$ was used for image transmission during the *Mariner 9 mission* to Mars.

(iii) In practice, one seeks codes $C \subseteq A^n$ with the largest possible minimum distance in order to be able to correct many errors. At the same time, one wants to transmit a lot of information with the smallest possible amount of data, i.e., the (*information*) *rate*

$$r(C) := \log_q(|C|)/n$$

should be large. The next theorem shows that one cannot maximize $d(C)$ and $r(C)$ simultaneously, but rather a compromise is required depending on the application. In live transmissions, for example, preference is given to $r(C)$ to avoid delays.

Theorem III.12.14. *For every code $C \subseteq A^n$ with $d := d(C)$ and $e := \lfloor \frac{d-1}{2} \rfloor$, it holds that*

$$|C| \leq q^{n-d+1} \qquad \text{(Singleton bound)},$$

$$|C| \sum_{k=0}^{e} \binom{n}{k} (q-1)^k \leq q^n \qquad \text{(Hamming bound)}.$$

If $d > n\frac{q-1}{q}$, then

$$|C| \leq \frac{d}{d - n\frac{q-1}{q}} \qquad \text{(Plotkin bound)}.$$

Proof.

(i) The projection onto the first $n-d+1$ components is an injective mapping $f\colon C \to A^{n-d+1}$, because from $f(c) = f(c')$ it follows that $d(c,c') \leq d-1$ and $c = c'$. This shows $|C| = |f(C)| \leq |A^{n-d+1}| = q^{n-d+1}$.

(ii) Because $d \geq 2e+1$, it holds that $K_e(c) \cap K_e(c') = \varnothing$ for distinct $c, c' \in C$ by the triangle inequality. Let $x \in K_e(c)$ with $d(c,x) = k$. For the choice of the k positions where c and x differ, there are $\binom{n}{k}$ possibilities. At each of these positions, x can take one of $q-1$ remaining values. This shows

$$|K_e(c)| = \sum_{k=0}^{e} \binom{n}{k} (q-1)^k.$$

Finally,

$$|C| \sum_{k=0}^{e} \binom{n}{k} (q-1)^k = \sum_{c \in C} |K_e(c)| = \Big| \bigcup_{c \in C} K_e(c) \Big| \leq |A^n| = q^n.$$

(iii) Let $A = \{a_1, \ldots, a_q\}$ and $m_{ij} := |\{c \in C : c_i = a_j\}|$ for $1 \leq i \leq n$ and $1 \leq j \leq q$. Obviously, $\sum_{j=1}^{q} m_{ij} = |C|$ for $i = 1, \ldots, n$. We sum the distances of all $|C|^2$ pairs of codewords. The i-th coordinate contributes exactly

$$\sum_{j=1}^{q} m_{ij}(|C| - m_{ij}) = |C|^2 - \sum_{j=1}^{q} m_{ij}^2$$

to this sum. The Cauchy-Schwarz inequality applied to the vectors $(m_{ij} : j = 1, \ldots, q)$ and $(1, \ldots, 1)$ shows

$$|C|^2 = \Big(\sum_{j=1}^{q} m_{ij} \Big)^2 \leq q \sum_{j=1}^{q} m_{ij}^2.$$

Therefore,

$$|C|(|C|-1)d \leq \sum_{c,c' \in C} d(c,c') \leq \sum_{i=1}^{n} \sum_{j=1}^{q} m_{ij}(|C| - m_{ij}) \leq \sum_{i=1}^{n} |C|^2 \Big(1 - \frac{1}{q}\Big) \leq n|C|^2 \frac{q-1}{q}.$$

Rearranging yields

$$|C| \Big(d - n\frac{q-1}{q} \Big) \leq d$$

and the assertion follows from the assumption $d - n\frac{q-1}{q} > 0$. □

Theorem III.12.15. *For all $1 \leq d \leq n$ there exists a code $C \subseteq A^n$ with $d(C) \geq d$ and*

$$|C| \sum_{k=0}^{d-1} \binom{n}{k} (q-1)^k \geq q^n \qquad \text{(Gilbert bound).}$$

Proof. Let $C \subseteq A^n$ with $d(C) \geq d$ and $|C|$ maximal. For every $x \in A^n$ there then exists a $c \in C$ with $d(x,c) < d$, because otherwise x could be added to C in contradiction to the maximality of $|C|$. Thus

$$q^n = \Big| \bigcup_{c \in C} K_{d-1}(c) \Big| \leq \sum_{c \in C} |K_{d-1}(c)| = |C| \sum_{k=0}^{d-1} \binom{n}{k} (q-1)^k. \qquad \square$$

Example III.12.16. For $q = 2$, $n = 10$ one obtains the following estimates for $|C|$:

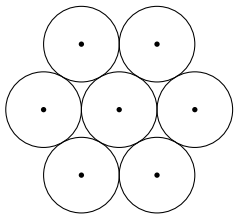
$d(C)$	Gilbert	Singleton	Hamming	Plotkin
1	2^{10}	2^{10}	2^{10}	
2	94	2^9	2^{10}	
3	16	256	93	
4	6	128	93	
5	3	64	15	
6	2	32	15	6
7	2	16	5	3

Let wlog. $A = \{0,1\}$ and $(0,\ldots,0) \in C$. In the case $d(C) \geq 7$, every non-trivial codeword consists of at least seven ones. Two non-trivial codewords would therefore have at least four common ones. This shows $|C| \leq 2$.

Remark III.12.17.

(i) C is called an MDS *code* (maximum distance separable) if equality holds in the Singleton bound. Besides the trivial code $C = A^n$, the repetition code W_n is also an MDS code.

(ii) If equality holds in the Hamming bound, then C is called *perfect*. In this case, $|C|$ is a q-power and A^n is the disjoint union of balls around codewords with radius e.



Thus, *every* error can be uniquely "corrected" (but not always correctly). In particular, $d(C) = 2e+1$ is odd. The trivial code $C = A^n$ is the only perfect code with $e = 0$. For $q = 2$ and $n = 2e+1$, the repetition code W_n is also perfect, because every word $x \in \{0,1\}^n$ has distance $\leq e$ to exactly one of the codewords $(0,\ldots,0)$ or $(1,\ldots,1)$. We will see later that there are only few other perfect codes (cf. Exercise III.69).

(iii) According to Shannon's main theorem from information theory, there exist codes C with "good" rate (but large n), such that the probability of an erroneous decoding is arbitrarily small. The proof uses statistics and is non-constructive.

Example III.12.18. Let $A = \{0, 1\}$ and $p = 10^{-3}$ be the probability that a symbol is transmitted incorrectly (i.e., 0 instead of 1 and vice versa). Let $q := 1 - p$. The probability of an error-free transmission of $n = 100$ symbols without coding is then $q^{100} \approx 0.90$. Using the code W_3, the probability increases to $(q^3 + 3q^2p)^{100} \approx 0.9997$.

Definition III.12.19. Codes $C, D \subseteq A^n$ are called *equivalent* if there exists a permutation $\pi \in S_n$ with

$$(x_1, \ldots, x_n) \in C \iff (x_{\pi(1)}, \ldots, x_{\pi(n)}) \in D.$$

For $C = D$, the corresponding π form the *automorphism group* $\mathrm{Aut}(C)$ of C.

Remark III.12.20. Equivalent codes obviously have the same properties (length, cardinality, minimum distance, rate, ...). One is therefore only interested in "interesting" representatives of equivalence classes.

Definition III.12.21. Let $A = \mathbb{F}_q$ be a finite field. A code $C \subseteq \mathbb{F}_q^n$ is called *linear*, if C is a subspace of $\mathbb{F}_q^n$. If $k := \dim C$ and $d := d(C)$, then C is an (n, k, d)-code (more precisely $(n, k, d)_q$-code). The rate of C is $r(C) = k/n$. Furthermore, $w(x) := d(x, 0)$ is called the *weight* of $x \in \mathbb{F}_q^n$.

Example III.12.22.

(i) The *parity code*

$$P_n := \left\{ x \in \mathbb{F}_q^n : \sum_{i=1}^{n} x_i = 0 \right\}$$

of length n has dimension $k = n - 1$ and minimum distance $d = 2$. It can therefore detect one error, but not correct it. A concrete version is the ASCII *code* with $q = 2$ and $n = 8$. With the first 7 bits, one represents one of $2^7 = 128$ frequently used symbols:

`	´	ˆ	˜	¨	˝	°	ˇ	˘	¯	˙	¸	˛	,	‹	›
“	”	„	«	»	–	—		0	ı	ȷ	ff	fi	fl	ffi	ffl
␣	!	"	#	$	%	&	’	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
‘	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	-

The eighth bit (*check bit*) results from the sum of the seven previous bits (modulo 2). For example, the letter b has position $98 = 2^6 + 2^5 + 2$ and therefore corresponds to the codeword $(1, 1, 0, 0, 0, 1, 0, 1)$ (check bit = 1). The eight bits together form a *byte* and can be processed efficiently on computers.

(ii) The ISBN *code*

$$C := \left\{ x \in \mathbb{F}_{11}^{10} : \sum_{l=1}^{10} l x_l = 0 \right\} \leq \mathbb{F}_{11}^{10}$$

with length $n = 10$, dimension $k = 9$ and minimum distance $d = 2$ has already been introduced in Example I.2.27.

Remark III.12.23.

(i) For $q = 2$ (resp. $q = 3$) one speaks of *binary* (resp. *ternary*) codes.

(ii) Obviously, the Hamming distance on $\mathbb{F}_q^n$ is *translation-invariant*, i. e. for $x, y, z \in \mathbb{F}_q^n$ it holds that $d(x, y) = d(x - z, y - z)$. For a linear code $C \leq \mathbb{F}_q^n$ it is therefore

$$\begin{aligned} d(C) &= \min\{d(x, y) : x, y \in C,\ x \neq y\} = \min\{d(x - y, 0) : x, y \in C,\ x \neq y\} \\ &= \min\{w(c) : c \in C \setminus \{0\}\}. \end{aligned}$$

One therefore also calls $d(C)$ the *minimum weight* of C.

(iii) Equivalent codes are isomorphic as vector spaces, but not vice versa. Often it is more appropriate to consider codes $C, C' \leq \mathbb{F}_q^n$ as equivalent if they are transformed into each other under a generalized permutation matrix $P \in \mathbb{F}_q^{n \times n}$. Here P has exactly one non-zero entry in each row and each column. Thus there exist $\pi \in S_n$ and $a_1, \ldots, a_n \in \mathbb{F}_q^\times$ with

$$(c_1, \ldots, c_n) \in C \iff (a_1 c_{\pi(1)}, \ldots, a_n c_{\pi(n)}) \in C'$$

for all $c \in \mathbb{F}_q^n$. Obviously C and C' still have the same properties.

(iv) The Singleton bound for (n, k, d)-codes has the form $d \leq n - k + 1$ (independent of q). The Hamming bound can be written in the form

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i \leq q^{n-k}.$$

The Gilbert bound essentially also holds for linear codes: Let $1 \leq d \leq n$ be given and C be an (n, k, d)-code with k maximal. Suppose there exists $x \in \mathbb{F}_q^n$ with $d(x, c) \geq d$ for all $c \in C$. For $\alpha \in \mathbb{F}_q^\times$ and $c \in C$ it then holds that

$$w(c + \alpha x) = d(c + \alpha x, 0) = d(c, -\alpha x) = d(-\alpha^{-1} c, x) \geq d.$$

Therefore $C + \mathbb{F}_q x$ would be an $(n, k + 1, d)$-code in contradiction to the maximality of k. Thus it holds that

$$\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i \geq q^{n-k}.$$

Example III.12.24.

(i) Let C be a perfect $(n, k, 7)$-code with $k \geq 1$ over $\mathbb{F}_2$. Then $n \geq 7$ and

$$1 + n + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)}{6} = \sum_{i=0}^{e} \binom{n}{i} = 2^{n-k}.$$

Multiplication by 6 yields

$$(n + 1)(6 + n(n - 1)) = 3 \cdot 2^{n-k+1}.$$

The substitution $N := n + 1 \geq 8$ leads to

$$N(N^2 - 3N + 8) = 3 \cdot 2^{n-k+1}.$$

If N is divisible by 16, then $N^2 - 3N + 8 \equiv 8 \pmod{16}$ and it follows that $N^2 - 3N + 8 \in \{8, 24\}$. This contradicts $N(N - 3) + 8 \geq 8 \cdot 5 + 8 > 24$. Thus N is not divisible by 16 and one obtains $N \mid 24$. Due to $N \geq 8$, the following cases arise:

- $(n, k) = (7, 1)$: These are the parameters of the repetition code W_7.

- $n = 11$: Here the equation does not work out: $N^2 - 3N + 8 = 12 \cdot 9 + 8 = 116 = 4 \cdot 29$.
- $(n, k) = (23, 12)$: Such a code is defined in Example III.12.42.

(ii) For the parameters $(n, k, d)_q = (90, 78, 5)_2$ one also obtains $\sum_{i=0}^{2} \binom{n}{i} = 2^{n-k}$. The following lemma with $s = 2$ shows that no such code can exist.

Lemma III.12.25. *Let C be a perfect $(n, k, 2e+1)$-code over $\mathbb{F}_q$ and $0 \leq s \leq e$. Then*

$$\binom{2e-s+1}{e} \;\Big|\; \binom{n-s}{e-s+1}(q-1)^{e-s+1}.$$

Proof. Let $V_s := \{x \in \mathbb{F}_q^n : \forall i = 1, \ldots, s : x_i = 1\}$ and

$$C_s := \{c \in C \cap V_s : w(c) = 2e+1\}.$$

Each of the $\binom{n-s}{e-s+1}(q-1)^{e-s+1}$ vectors $x \in V_s$ with $w(x) = e+1$ lies in exactly one ball $B_e(c)$ with $c \in C$. Because $w(c) \geq 2e+1$, it holds that $x_i \neq 0 \Rightarrow x_i = c_i$ and $c \in C_s$. On the other hand, $B_e(c)$ contains exactly $\binom{2e-s+1}{e}$ vectors $x \in V_s$ with $w(x) = e+1$. This shows

$$|C_s| = \frac{\binom{n-s}{e-s+1}}{\binom{2e-s+1}{e}}(q-1)^{e-s+1} \in \mathbb{N}. \qquad \square$$

Theorem III.12.26. *For every (n, k, d)-code $0 \neq C \leq \mathbb{F}_q^n$ it holds that*

$$\sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \leq n \qquad \text{(Griesmer bound).}$$

Proof. Induction on k: For $k = 1$ the claim is trivial. So let $k \geq 2$. Let $b_1, \ldots, b_k \in C$ be a basis of C. After passing to an equivalent code as in Remark III.12.23(iii), we can assume $b_1 = (1, \ldots, 1, 0, \ldots, 0)$ with $w(b_1) = d$. Let $b_i' \in \mathbb{F}_q^{n-d}$ be the vector formed from the last $n-d$ coordinates of b_i $(i = 2, \ldots, k)$.

Assume there exists a non-trivial linear combination c' of $b_2', \ldots, b_k'$ with $w(c') < d/q$. Let $c = (c_1, c') \in C$ be the corresponding linear combination of $b_2, \ldots, b_k$. Because $w(c) \geq d$, at most $w(c')$ coordinates of c_1 vanish. Because $(q-1)w(c') < d - w(c')$, some $\lambda \in \mathbb{F}_q^\times$ occurs more than $w(c')$-times in c_1. We replace c by $\lambda^{-1}c$. Then

$$d(c, b_1) < d - w(c') + w(c') = d$$

holds and it follows that $c = b_1$. This contradicts the linear independence of $b_1, \ldots, b_k$. Thus $w(c') \geq d/q$. Overall, $C' := \langle b_2', \ldots, b_k' \rangle \leq \mathbb{F}_q^{n-d}$ is a $(k-1)$-dimensional code with $d' := d(C') \geq d/q$. By induction,

$$\sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil = d + \sum_{i=1}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \leq d + \sum_{i=0}^{k-2} \left\lceil \frac{d'}{q^i} \right\rceil \leq d + n - d = n. \qquad \square$$

Definition III.12.27. Let $C \leq \mathbb{F}_q^n$ be an (n, k, d)-code.

(i) One calls $G \in \mathbb{F}_q^{k \times n}$ a *generator matrix* of C if $C = \{xG : x \in \mathbb{F}_q^k\}$ holds. Furthermore, one calls $H \in \mathbb{F}_q^{(n-k) \times n}$ a *parity-check matrix* of C if $C = \{x \in \mathbb{F}_q^n : Hx^{\mathrm{t}} = 0\}$ holds.

(ii) As usual,

$$xy^{\mathrm{t}} = \sum_{i=1}^{n} x_i y_i \qquad (x, y \in \mathbb{F}_q^n)$$

defines a bilinear form on $\mathbb{F}_q^n$. One calls

$$C^\perp := \{x \in \mathbb{F}_q^n : \forall c \in C : xc^{\mathrm{t}} = 0\} \leq \mathbb{F}_q^n$$

the *dual* code to C. In the case $C = C^\perp$, C is called *self-dual*.

Remark III.12.28.

(i) $G \in \mathbb{F}_q^{k\times n}$ is a generator matrix of C if and only if the rows of G form a basis of C. $H \in \mathbb{F}_q^{(n-k)\times n}$ is a parity-check matrix if and only if the rows of H form a basis for the solution space of the homogeneous system of equations $Gx = 0$. In particular, both matrices always exist (but not uniquely) and have full rank.

(ii) By passing to an equivalent code, one can assume that the first k columns of G are linearly independent. Through a basis transformation, one achieves that G has the form $G = (1_k|L)$. Every codeword is thus already uniquely determined by the first k components. Now $H = (-L^{\mathrm{t}}|1_{n-k})$ is a parity-check matrix of C.

(iii) The minimum distance is evidently the minimum number of linearly dependent columns of a parity-check matrix.

(iv) If G is a generator matrix of C, then $C^\perp$ lies in the solution space of $Gx = 0$ and it follows that $\dim(C^\perp) \leq n - k$. If H is a parity-check matrix of C, then the rows of H lie in $C^\perp$ and it follows that $\dim(C^\perp) \geq n - k$. Thus $\dim(C^\perp) = n - k$ and G (resp. H) is a parity-check matrix (resp. generator matrix) of $C^\perp$. Self-dual codes therefore have even length $n = 2k$ and dimension k.

(v) It holds that $(C^\perp)^\perp = C$. In contrast to the Euclidean space $\mathbb{R}^n$, it is quite possible over $\mathbb{F}_q^n$ for $C = C^\perp \neq 0$ to occur. For example for $C = W_2 = \langle(1, 1)\rangle \leq \mathbb{F}_2^2$.

Example III.12.29. The repetition code W_n has the following generator and parity-check matrices:

$$G = \begin{pmatrix} 1 & \cdots & 1 \end{pmatrix}, \qquad H = \begin{pmatrix} 1 & & 0 & -1 \\ & \ddots & & \vdots \\ 0 & & 1 & -1 \end{pmatrix}.$$

Evidently $W_n^\perp = P_n$ is the parity-check code.

Theorem III.12.30. *With the notation from Remark III.12.23*(iii)*, there are exactly* $\binom{Q+n-k-1}{n-k}$ *non-equivalent linear* $(n, k)_q$*-codes, where* $Q := 1 + \frac{q^k-1}{q-1}$.

Proof. Using the Gaussian algorithm, the generator matrix G can be transformed into exactly one reduced row echelon form. By multiplication with a generalized permutation matrix from the right, the equivalence class does not change. Since G has full rank, one can achieve by coordinate permutation that the first k columns form an identity matrix. The remaining $n - k$ columns form a multiset of $\mathbb{F}_q^k$. By scaling, one can assume that the non-zero columns begin with a 1. One thus has an $(n - k)$-element multiset from $Q = 1 + \frac{q^k-1}{q-1}$ possible vectors. The number of these multisets is $\binom{Q+n-k-1}{n-k}$.[1] □

[1] See lecture notes Discrete Mathematics

Remark III.12.31. For $k = 1$, one obtains $Q = 2$ and exactly n non-equivalent codes. These are generated by the vectors of the form $(1, \dots, 1, 0, \dots, 0)$.

Theorem III.12.32 (Syndrome Decoding)**.** *Let $C \leq \mathbb{F}_q^n$ be a linear code. From each coset $x+C \in \mathbb{F}_q^n/C$ we choose a representative $e_x \in x + C$ such that $w(e_x)$ is minimal. Then $c := x - e_x \in C$ is a codeword with minimal distance to x. Thus, one can decode x to c.*

Proof. Let $c' \in C$ with $d(x, c') < d(x, c)$. Then $e := x - c' \in x + C$ with $w(e) = d(x, c') < d(x, c) = w(e_x)$ in contradiction to the choice of e_x. □

Remark III.12.33. Let $k := \dim C$. In practice, one first determines for each of the q^{n-k} cosets $x + C$ an e_x as in Theorem III.12.32. To decide whether a $y \in \mathbb{F}_q^n$ lies in the same coset as e_x, one uses the parity-check matrix H of C. It holds that

$$x + C = y + C \iff x - y \in C \iff H(x - y) = 0 \iff Hx = Hy.$$

One calls Hx the *syndrome* of x w.r.t. C. In contrast to non-linear codes, one thus has an "efficient" decoding algorithm.

Definition III.12.34. Let $m \geq 2$. Let $\langle v_1 \rangle, \dots, \langle v_n \rangle$ be the one-dimensional subspaces of $\mathbb{F}_q^m$. The code H_n with parity-check matrix $\begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} \in \mathbb{F}_2^{m \times n}$ is called the *Hamming code* of length n.

Example III.12.35. Let $q = 2$, $m = 3$ and $n = 2^3 - 1 = 7$. A parity-check matrix of H_7 is

$$\begin{pmatrix} 1 & . & . & . & 1 & 1 & 1 \\ . & 1 & . & 1 & . & 1 & 1 \\ . & . & 1 & 1 & 1 & . & 1 \end{pmatrix}.$$

This yields the generator matrix

$$\begin{pmatrix} . & 1 & 1 & 1 & . & . & . \\ 1 & . & 1 & . & 1 & . & . \\ 1 & 1 & . & . & . & 1 & . \\ 1 & 1 & 1 & . & . & . & 1 \end{pmatrix}.$$

Theorem III.12.36. *The Hamming code H_n has length $n = \frac{q^m-1}{q-1}$, dimension $n - m$ and minimum distance 3. Furthermore, H_n is perfect.*

Proof. Every $v \in \mathbb{F}_q^n \setminus \{0\}$ spans a one-dimensional subspace. Every such subspace contains q vectors and any two different subspaces have trivial intersection. This shows $n = \frac{q^m-1}{q-1}$. Since the standard basis vectors $\{(1, 0, \dots, 0), \dots, (0, \dots, 0, 1)\}$ appear up to scaling as columns of the parity-check matrix H, H has full rank and it follows that $k := \dim H_n = n - m$. Since any two different columns of H are linearly independent, $d(H_n) \geq 3$ holds. On the other hand, the linearly dependent vectors $(1, 0, \dots, 0)$, $(0, 1, 0, \dots, 0)$ and $(1, 1, 0, \dots, 0)$ appear up to scaling as columns of H. Thus $d(H_n) = 3$.

The Hamming bound with $e = 1$ yields

$$\sum_{i=0}^{1} \binom{n}{i} (q-1)^i = 1 + n(q-1) = q^m = q^{n-k}.$$

Thus H_n is perfect. □

Remark III.12.37.

(i) The Hamming code depends on the choice of the v_i. Different choices of the v_i yield, however, equivalent codes in the sense of Remark III.12.23(iii).

(ii) The correction of one error can be performed particularly efficiently in the Hamming code. Let H be the parity-check matrix, $c \in H_n$ and $x = c + e$ with $w(e) = 1$. Then $Hx = H(c + e) = He$. The position of the occurred error is the position of the column Hx in H.

(iii) A disadvantage of Hamming codes is that they only exist for certain n (especially when q is small).

Theorem III.12.38. *Every linear perfect $(n, k, 3)$-code C is equivalent to H_n.*

Proof. The Hamming bound yields $1 + n(q-1) = q^{n-k}$, i. e. $n = \frac{q^{n-k}-1}{q-1}$. Because of $d(C) = 3$, any two columns of a parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ of C are linearly independent. On the other hand, the number of 1-dimensional subspaces of $\mathbb{F}_q^{n-k}$ is $\frac{q^{n-k}-1}{q-1} = n$. Therefore, H is, up to equivalence, the parity-check matrix of H_n. □

Example III.12.39. For $q = 2$, W_3 is equivalent to H_3.

Definition III.12.40. For a linear code $C \leq \mathbb{F}_q^n$ let

$$\widehat{C} := \left\{(x_1, \ldots, x_{n+1}) \in \mathbb{F}_q^{n+1} : (x_1, \ldots, x_n) \in C,\ \sum_{i=1}^{n+1} x_i = 0\right\} \leq \mathbb{F}_q^{n+1}$$

be the *extended* code.

Remark III.12.41. Certainly $\dim \widehat{C} = \dim C$ and $d(\widehat{C}) \geq 2$. If C is a binary code with odd weight d, then $d(\widehat{C}) = d + 1$. In this way, the number of detectable (but not correctable) errors can be easily increased. At the same time, the rate decreases from $\frac{k}{n}$ to $\frac{k}{n+1}$.

Example III.12.42.

(i) The parity code P_n is the extension of the trivial code $\mathbb{F}_q^{n-1}$.

(ii) The extended Hamming code $\widehat{H_7}$ over $\mathbb{F}_2$ is an $(8, 4, 4)$-code with generator matrix

$$G = \begin{pmatrix} . & 1 & 1 & 1 & . & . & . & 1 \\ 1 & . & 1 & . & 1 & . & . & 1 \\ 1 & 1 & . & . & . & 1 & . & 1 \\ 1 & 1 & 1 & . & . & . & 1 & . \end{pmatrix}$$

according to Example III.12.35. Because of $GG^{\mathrm{t}} = 0$, $\widehat{H_7}$ is self-dual.

(iii) According to Exercise III.70, $\widehat{H_7}$ is equivalent to the codes C and $\widetilde{C}$ with generator matrices

$$G = \begin{pmatrix} 1 & 1 & . & 1 & . & . & . & 1 \\ . & 1 & 1 & . & 1 & . & . & 1 \\ . & . & 1 & 1 & . & 1 & . & 1 \\ . & . & . & 1 & 1 & . & 1 & 1 \end{pmatrix}, \qquad \widetilde{G} = \begin{pmatrix} . & . & . & 1 & . & 1 & 1 & 1 \\ . & . & 1 & . & 1 & 1 & . & 1 \\ . & 1 & . & 1 & 1 & . & . & 1 \\ 1 & . & 1 & 1 & . & . & . & 1 \end{pmatrix}.$$

With their help, we define the *extended binary* GOLAY *code* by

$$G_{24} := \left\{(c+e, d+e, c+d+e) : c, d \in C,\ e \in \widetilde{C}\right\} \leq \mathbb{F}_2^{24}.$$

The *binary Golay code* $G_{23} \leq \mathbb{F}_2^{23}$ is formed from G_{24} by deleting the last coordinate of all codewords.

Theorem III.12.43. *It holds that*

(i) G_{24} *is a self-dual* $(24, 12, 8)$*-code.*

(ii) G_{23} *is a perfect* $(23, 12, 7)$*-code.*

Proof (TURYN).

(i) We use the notation from Example III.12.42. Adding the 1st, 3rd and 4th row of G or $\widetilde{G}$, respectively, yields $\mathbb{F}_2(1, \ldots, 1) \subseteq C \cap \widetilde{C}$. We show that $C \cap \widetilde{C}$ is not larger. For this, let $x, y \in \mathbb{F}_2^4$ with $xG = y\widetilde{G}$. Then $(x, y)\binom{G}{\widetilde{G}} = 0$. The Gaussian algorithm leads to

$$\binom{G}{\widetilde{G}} \sim \left(\begin{array}{cccccccc} 1&1&.&1&.&.&.&1\\ .&1&1&.&1&.&.&1\\ .&.&1&1&.&1&.&1\\ .&.&.&1&1&.&1&1\\ \hline .&.&.&.&1&1&.&.\\ .&.&.&1&1&.&.&.\\ .&.&1&1&.&.&.&.\\ .&1&1&.&.&.&.&. \end{array}\right) \sim \left(\begin{array}{cccccccc} 1&1&.&1&.&.&.&1\\ .&1&1&.&1&.&.&1\\ .&.&1&1&.&1&.&1\\ .&.&.&1&1&.&1&1\\ \hline .&.&.&.&1&1&.&.\\ .&.&.&.&.&.&1&1\\ .&.&.&.&.&1&.&1\\ .&.&.&.&1&.&.&1 \end{array}\right) \sim \left(\begin{array}{cccccccc} 1&1&.&1&.&.&.&1\\ .&1&1&.&1&.&.&1\\ .&.&1&1&.&1&.&1\\ .&.&.&1&1&.&1&1\\ \hline .&.&.&.&1&1&.&.\\ .&.&.&.&.&1&.&1\\ .&.&.&.&.&.&1&1\\ .&.&.&.&.&.&.&. \end{array}\right)$$

Thus $\binom{G}{\widetilde{G}}$ has rank 7 and it follows that $C \cap \widetilde{C} = \mathbb{F}_2(1, \ldots, 1)$. The codewords of the form $(c, 0, c)$, $(0, d, d)$ and (e, e, e) with $c, d \in C$ and $e \in \widetilde{C}$ form a generating system of G_{24}. In the case $(c, 0, c) + (0, d, d) = (e, e, e)$, we have $c = e = d = c + d = 0$. This shows

$$\dim G_{24} = \dim C + \dim C + \dim \widetilde{C} = 4 + 4 + 4 = 12.$$

Since C and $\widetilde{C}$ are self-dual with $\widehat{H_7}$, the vectors $(c, 0, c)$, $(0, d, d)$ and (e, e, e) are pairwise orthogonal. Thus G_{24} is also self-dual.

Any two rows c and d of G (or $\widetilde{G}$) have weight 4. Because of $cd^{\mathrm{t}} = 0$, c and d have an even number of ones in common. In the sum $c + d$, the common ones cancel each other out. It follows that $w(c + d)$ is divisible by 4. For another row e of G, $w(c + d + e)$ is now also divisible by 4 etc. Overall, $4 \mid w(c)$ for all $c \in C \cup \widetilde{C}$. By the same argument, $4 \mid w(x)$ for all $x \in G_{24}$, since G_{24} is also self-dual. In particular, $d(G_{24}) \geq 4$. Suppose there exists $x = (c + e, d + e, c + d + e) \in G_{24}$ with $d(x) = 4$. Since each of the three components has even weight, one of the three components must be 0. Then $e \in C \cap \widetilde{C} = \mathbb{F}_2(1, \ldots, 1)$ and one easily obtains a contradiction. Therefore $d(G_{24}) \geq 8$. Conversely, for $c \in C$ with $w(c) = 4$, $w((c, 0, c)) = 8 \leq d(G_{24})$.

(ii) Because of $d(G_{24}) = 8$, the projection $G_{24} \to G_{23}$ is injective. Thus G_{23} is a $(23, 12, d)$-code with $d \geq 7$. Deleting the last coordinate from $(c, 0, c) \in G_{24}$ with $c = (1, 1, 0, 1, 0, 0, 0, 1) \in C$, one obtains a codeword with weight 7. This shows $d = 7$. The Hamming bound now has the form

$$\sum_{i=0}^{3} \binom{23}{i} = 1 + 23 + 23 \cdot 11 + 23 \cdot 11 \cdot 7 = 1 + 23 \cdot 89 = 2048 = 2^{23-12},$$

i. e. G_{23} is perfect. □

Definition III.12.44. The linear code $G_{12} \leq \mathbb{F}_3^{12}$ with generator matrix

$$\begin{pmatrix} 1 & . & . & . & . & . & 1 & 1 & 1 & 1 & 1 & . \\ . & 1 & . & . & . & . & . & 1 & -1 & -1 & 1 & -1 \\ . & . & 1 & . & . & . & 1 & . & 1 & -1 & -1 & -1 \\ . & . & . & 1 & . & . & -1 & 1 & . & 1 & -1 & -1 \\ . & . & . & . & 1 & . & -1 & -1 & 1 & . & 1 & -1 \\ . & . & . & . & . & 1 & 1 & -1 & -1 & 1 & . & -1 \end{pmatrix}$$

is called the *extended ternary Golay code* G_{12}. By puncturing the last coordinate, one obtains the *ternary Golay code* G_{11}.

Theorem III.12.45. *The following holds:*

(i) G_{12} *is a self-dual* $(12, 6, 6)$*-code.*

(ii) G_{11} *is a perfect* $(11, 6, 5)$*-code.*

Proof.

(i) Let M be the generator matrix of G_{12} given in Definition III.12.44. Since M has rank 6, G_{12} is a $(12, 6)$-code. Obviously, every row of M has weight 6. One also checks that the rows of M are pairwise orthogonal. Therefore, G_{12} is self-dual. For $c = (x_1, \ldots, x_{12}) \in C$, it thus holds that $w(c) = x_1^2 + \ldots + x_{12}^2 = cc^{\mathrm{t}} \equiv 0 \pmod 3$. Two different rows c and d of M differ in exactly two positions in the first six coordinates. In the last six coordinates, c and d differ at least in the two positions of the zeros. Every linear combination x of c and d therefore has weight $w(x) = 6$ because of $3 \mid w(x)$. Thus, x has exactly two zeros in the last six coordinates. A linear combination of three different rows of M consequently has at least weight 6. Every linear combination of more than three rows already has at least four non-zero entries in the first six coordinates. This shows $d(G_{12}) = 6$.

(ii) Because of $d(G_{12}) = 6$, the projection $G_{12} \to G_{11}$ is injective. Thus, G_{11} is an $(11, 6, 5)$-code. The Hamming bound has the form

$$1 + \binom{11}{1} 2 + \binom{11}{2} 4 = 1 + 22 + 220 = 243 = 3^5 = 3^{11-6},$$

i. e. G_{11} is perfect. □

Remark III.12.46.

(i) van Lint and Tietäväinen have proven that every linear perfect code is equivalent to one of the following codes:

- the trivial $(n, n, 0)$-code $\mathbb{F}_q^n$.
- the trivial $(n, 0, n)$-code $\{0\}$.
- the binary $(2n + 1, 1, 2n + 1)$-repetition code $W_{2n+1} = \mathbb{F}_2(1, \ldots, 1)$.
- the $(n, n - m, 3)$-Hamming code H_n, where $n = \frac{q^m - 1}{q - 1}$.
- the binary Golay code G_{23}.
- the ternary Golay code G_{11}.

The classification of non-linear codes over arbitrary alphabets is, however, still open (cf. Exercise III.69).

(ii) The code G_{24} was used by the Voyager space probes to send images of Jupiter to Earth. The automorphism group $\mathrm{Aut}(G_{24})$ is isomorphic to the sporadic simple *Mathieu group* M_{24} of order $244,823,040$. John Conway, who passed away from Covid in 2020, referred to M_{24} as "the most remarkable of all finite groups".

(iii) Codes with given parameters can be looked up in the database `https://codetables.de/`. For example, one finds a $(32,14,8)_2$-code there, while the existence of a $(32,14,9)_2$-code is still open.

Definition III.12.47. Let $C \subseteq \mathbb{F}_q^n$ be a code and $w_i := |\{c \in C : w(c) = i\}|$ for $i = 0, \ldots, n$. One calls

$$W_C(X) := \sum_{c \in C} X^{w(c)} = w_0 + w_1 X + \ldots + W_n X^n \in \mathbb{Z}[X]$$

the *generating function* of C.

Remark III.12.48. From $W_C(X)$, one can obviously read off $|C| = w_0 + \ldots + w_n$, as well as $d(C) = \min\{i \geq 1 : w_i \neq 0\}$.

Theorem III.12.49 (MacWilliams Identity)**.** *Let $C \leq \mathbb{F}_q^n$ be a linear code of dimension k. Then*

$$W_{C^\perp}(X) = q^{-k}\big(1 + (q-1)X\big)^n W_C\Big(\frac{1-X}{1+(q-1)X}\Big).$$

Proof. Let $V := \mathbb{F}_q^n$. Since $(\mathbb{F}_q, +)$ is abelian, there exists a non-trivial homomorphism $\chi\colon \mathbb{F}_q \to \mathbb{C}^\times$. For $v \in V$, $C \to \mathbb{C}^\times$, $c \mapsto \chi(cv^{\mathrm{t}})$ is a character of C. For $c \in C$ let

$$\alpha(c) := \sum_{v \in V} \chi(cv^{\mathrm{t}}) X^{w(v)} \in \mathbb{C}[X].$$

According to the first orthogonality relation (Theorem II.14.22), it holds that

$$\sum_{c \in C} \alpha(c) = \sum_{v \in V} X^{w(v)} \sum_{c \in C} \chi(cv^{\mathrm{t}}) = \sum_{v \in C^\perp} |C| X^{w(v)} = q^k W_{C^\perp}(X).$$

We now write $v = (v_1, \ldots, v_n)$ and $w(v_i) = 1$ if $v_i \neq 0$ and $w(v_i) = 0$. Then

$$\begin{aligned}\alpha(c) &= \sum_{v \in V} \chi(c_1 v_1) \ldots \chi(c_n v_n) X^{w(v_1)+\ldots+w(v_n)} = \prod_{i=1}^{n} \sum_{a \in \mathbb{F}_q} \chi(a c_i) X^{w(a)} \\ &= (1-X)^{w(c)}(1+(q-1)X)^{n-w(c)} = \big(1-(q-1)X\big)^n \Big(\frac{1-X}{1+(q-1)X}\Big)^{w(c)}.\end{aligned}$$

Overall, one obtains

$$q^k W_{C^\perp}(X) = \sum_{c \in C} \alpha(c) = \big(1-(q-1)X\big)^n W_C\Big(\frac{1-X}{1+(q-1)X}\Big). \qquad \square$$

Example III.12.50. According to Example III.12.35, the code $C = H_7^\perp$ consists of the following codewords:

0000000	1000111	0101011	1101100
0011101	1011010	0110110	1110001

Therefore $W_C(X) = 1 + 7X^4$. The MacWilliams identity yields

$$\begin{aligned} W_{H_7}(X) &= \frac{1}{8}(1+X)^7\Big(1 + 7\frac{(1-X)^4}{(1+X)^4}\Big) = \frac{1}{8}(1+X)^3\big((1+X)^4 + 7(1-X)^4\big) \\ &= (1 + 3X + 3X^2 + X^3)(1 - 3X + 6X^2 - 3X^3 + X^4) \\ &= 1 + 7X^3 + 7X^4 + X^7. \end{aligned}$$

Definition III.12.51. A code $C \subseteq A^n$ is called *cyclic*, if $(c_2, c_3, \ldots, c_n, c_1) \in C$ holds for all $(c_1, \ldots, c_n) \in C$.

Theorem III.12.52. *Let $\mathcal{C}$ be the set of linear cyclic codes $C \leq \mathbb{F}_q^n$. Let $\mathcal{D}$ be the set of monic divisors of $X^n - 1 \in \mathbb{F}_q[X]$. For $c = (c_0, \ldots, c_{n-1}) \in C \in \mathcal{C}$ let $c(X) := \sum_{i=0}^{n-1} c_i X^i \in \mathbb{F}_q[X]$. Then there exists an $\alpha \in \mathcal{D}$ with*

$$(\alpha)/(X^n - 1) = \{c(X) + (X^n - 1) : c \in C\}$$

and $\dim C = n - \deg \alpha$. The map $\mathcal{C} \to \mathcal{D}$, $C \to \alpha$ is a bijection.

Proof. Let $I := (X^n - 1) \trianglelefteq \mathbb{F}_q[X]$. For $c, d \in C \in \mathcal{C}$ we have

$$\begin{aligned} c(X) + d(X) &= \sum_{i=0}^{n-1} (c_i + d_i) X^i = (c + d)(X), \\ X(c(X) + I) &= \sum_{i=0}^{n-1} c_i X^{i+1} + I = c_{n-1} + c_0 X + \ldots + c_{n-2} X^{n-2} + I \\ &= (c_{n-1}, c_0, \ldots, c_{n-2})(X). \end{aligned}$$

This shows $C(X) := \{c(X) + I : c \in C\} \trianglelefteq \mathbb{F}_q[X]/I$. According to the correspondence theorem, there exists exactly one ideal $J \trianglelefteq \mathbb{F}_q[X]$ with $C(X) = J/I$. Since $\mathbb{F}_q[X]$ is a principal ideal domain, there exists exactly one monic polynomial $\alpha \in \mathbb{F}_q[X]$ with $J = (\alpha)$. Since the map $c \mapsto c(X)$ is injective, we have

$$\dim C = \dim(J/I) = \dim(\mathbb{F}_q[X]/I) - \dim(\mathbb{F}_q[X]/(\alpha)) = n - \deg \alpha.$$

Because of $X^n - 1 \in J$, it holds that $\alpha \mid X^n - 1$, i. e. $\alpha \in \mathcal{D}$. The map $\mathcal{C} \to \mathcal{D}$ is thus injective. Conversely, if $\alpha \in \mathcal{D}$ is given, then $(\alpha)/I$ can be interpreted as a cyclic code as above. Therefore $\mathcal{C} \to \mathcal{D}$ is also surjective. □

Definition III.12.53. In the situation of Theorem III.12.52, α is called the *generator polynomial* and $\beta := \frac{X^n - 1}{\alpha}$ the *check polynomial* of C. It holds that $\dim C = \deg \beta$.

Remark III.12.54. Let $\alpha = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_0$ be the generator polynomial of C, where $a_d = 1$. Then $\alpha, X\alpha, \ldots, X^{n-d-1}\alpha$ is a basis of $(\alpha)/(X^n - 1)$. Thus

$$\begin{pmatrix} a_0 & \cdots & a_d & & 0 \\ & \ddots & & \ddots & \\ 0 & & a_0 & \cdots & a_d \end{pmatrix} \in \mathbb{F}_q^{(n-d)\times n}$$

is a generator matrix of C. Now let $\beta = b_{n-d}X^{n-d} + \ldots + b_0$ be the check polynomial of C. Because of $\alpha\beta = X^n - 1$, we have $\sum_i a_i b_{k-i} = 0$ for $k = 1, \ldots, n-1$. Therefore

$$\begin{pmatrix} b_{n-d} & \cdots & b_0 & & 0 \\ & \ddots & & \ddots & \\ 0 & & b_{n-d} & \cdots & b_0 \end{pmatrix} \in \mathbb{F}_q^{d \times n}$$

is a parity-check matrix of C. Therefore $C^\perp$ is cyclic with generator polynomial $X^{n-d} + b_0^{-1}b_1X^{n-d-1} + \ldots + b_0^{-1} = b_0^{-1}X^{n-d}\beta(X^{-1})$ (up to normalization, the order of the coefficients is reversed).

Example III.12.55. The generator polynomials $\alpha = 1$ and $\alpha = X^n - 1$ lead to the trivial codes $\mathbb{F}_q^n$ and 0. For $\alpha = X - 1$ one obtains the parity-check code P_n. The complementary factor $\frac{X^n-1}{X-1} = 1 + X + \ldots + X^{n-1}$ belongs to the repetition code W_n. For more interesting examples, the prime factorization of $X^n - 1$ is useful.

Definition III.12.56. For coprime numbers $a, d \in \mathbb{N}$, let $\mathrm{ord}_d(a)$ be the order of $a + d\mathbb{Z}$ in $(\mathbb{Z}/d\mathbb{Z})^\times$.

Theorem III.12.57. *Let $q \neq 1$ be a power of the prime number p and $n = p^k m \in \mathbb{N}$ with $p \nmid m$. Then*

$$X^n - 1 = \prod_{d \mid m} \Phi_d^{p^k} = \prod_{d \mid m} \prod_{i=1}^{\varphi(d)/\mathrm{ord}_d(q)} \Phi_{d,i}^{p^k},$$

where $\Phi_{d,i} \in \mathbb{F}_q[X]$ are pairwise distinct irreducible polynomials of degree $\mathrm{ord}_d(q)$.

Proof. Since $X^n - 1 = (X^m - 1)^{p^k}$ holds in $\mathbb{F}_q[X]$, we can assume $n = m$. The cyclotomic polynomials $\Phi_d \in \mathbb{Z}[X]$ lie in $\mathbb{F}_p[X] \subseteq \mathbb{F}_q[X]$ after reduction modulo p. Thus the first equation is proven. Let $N := \mathrm{ord}_n(q)$. Because of $q^N = 1 \pmod n$, there exists a primitive n-th root of unity $\zeta \in \mathbb{F}_{q^N}^\times$. Obviously $\zeta, \zeta^2, \ldots, \zeta^n$ are the roots of $X^n - 1$. By induction on n it follows that

$$\Phi_n = \prod_{\gcd(s,n)=1} (X - \zeta^s)$$

as in $\mathbb{Q}[X]$. The irreducible factors of Φ_n in $\mathbb{F}_q[X]$ correspond to the orbits of $\mathrm{Gal}(\mathbb{F}_{q^N}|\mathbb{F}_q) = \langle F \rangle$ on $\{\zeta^s : \gcd(s,n) = 1\}$, where $F(x) = x^q$ is the Frobenius automorphism. We therefore look for the orbits of the multiplication action of $\langle q + n\mathbb{Z} \rangle$ on $(\mathbb{Z}/n\mathbb{Z})^\times$. These are exactly the cosets of $\langle q + n\mathbb{Z} \rangle$; they thus have length N. In this way, the $\varphi(n)/N$ irreducible polynomials $\Phi_{n,i}$ of degree N arise. □

Theorem III.12.58. *Let q be a prime power, $n \in \mathbb{N}$ coprime to q and $d := \mathrm{ord}_n(q)$, such that $n = q^d - 1$ holds. Then there exists a cyclic $(n, d, q^{d-1}(q-1))$-code C with $W_C(X) = 1 + nX^{d(C)}$.*

Proof. According to Theorem III.12.57, there exists an irreducible divisor β of Φ_n of degree d. Let C be the cyclic code with check polynomial β and generator polynomial $\alpha := \frac{X^n-1}{\beta}$. Because of $\gcd(n, q) = 1$, the prime factors of $X^n - 1$ are pairwise distinct. In particular, α and β are coprime. Assume there exist $0 \leq i < j < n$ with $X^i\alpha \equiv X^j\alpha \pmod I$, where $I := (X^n - 1)$. Then β is a divisor of $X^k - 1$ with $k := j - i < n$. Consequently, β also divides $\gcd(X^k - 1, X^n - 1) = X^{\gcd(k,n)} - 1$. But then β would have to appear twice in the prime factorization of $X^n - 1$. This contradiction shows $X^i\alpha \not\equiv X^j\alpha \pmod I$. Because of $|C| = q^d = n + 1$, it follows that

$$C(X) = (\alpha)/I = \{0, X^i\alpha + I : i = 0, \ldots, n-1\}.$$

In particular, all non-trivial codewords have the same weight. Let $c \in C$ with $c_i \neq 0$. Write $C = \langle c \rangle \oplus D$ as a direct sum of vector spaces. For each $c' \in D$, there exist exactly $q-1$ elements $\lambda \in \mathbb{F}_q$ such that $\lambda c + c'$ does not vanish at coordinate i. Thus, there are exactly $|D|(q-1) = q^{d-1}(q-1)$ codewords c with $c_i \neq 0$. This shows

$$d(C) = \frac{1}{|C|-1} \sum_{c \in C \setminus \{0\}} w(c) = \frac{1}{n} \sum_{i=1}^{n} q^{d-1}(q-1) = q^{d-1}(q-1).$$

This also yields the generating function $W_C(X)$. □

Example III.12.59. For $n = 7$, $q = 2$ and $d = 3$, the condition $n = q^d - 1$ from Theorem III.12.58 is satisfied. Thus, there exists a cyclic $(7, 3, 4)$-code C. Because of $\Phi_7 = (X^3 + X + 1)(X^3 + X^2 + 1)$ in $\mathbb{F}_2[X]$, we can choose $\beta = X^3 + X^2 + 1$ as the check polynomial. The corresponding check matrix is

$$\begin{pmatrix} 1 & 1 & . & 1 & . & . & . \\ . & 1 & 1 & . & 1 & . & . \\ . & . & 1 & 1 & . & 1 & . \\ . & . & . & 1 & 1 & . & 1 \end{pmatrix}$$

according to Remark III.12.54. According to Exercise III.70, this is a generator matrix of H_7 (cf. Example III.12.50). Therefore, C is equivalent to $H_7^{\perp}$.

Theorem III.12.60. *Let $k \leq n \leq q$ and $A \subseteq \mathbb{F}_q$ with $|A| = n$. Then*

$$C := \big\{ (\gamma(a) : a \in A) : \gamma \in \mathbb{F}_q[X],\ \deg \gamma < k \big\} \subseteq \mathbb{F}_q^n$$

is an $(n, k, n-k+1)$-code; thus an MDS code. In the case $A = \langle a \rangle$, C is cyclic.

Proof. Let P be the k-dimensional $\mathbb{F}_q$-vector space of all $\gamma \in \mathbb{F}_q[X]$ with $\deg \gamma < k$. Each such $\gamma \neq 0$ has at most $k-1$ roots. Because of $k \leq n$, the map $P \to C$, $\gamma \mapsto (\gamma(a) : a \in A)$ is a monomorphism of vector spaces. In particular, C is an (n, k)-code with $d(C) \geq n-(k-1) = n-k+1$. From the Singleton bound, it follows that $d(C) = n-k+1$, i.e., C is an MDS code. Now let $A = \langle a \rangle$ and $(\gamma(1), \ldots, \gamma(a^{n-1})) \in C$. Set $\rho(X) := \gamma(aX) \in \mathbb{F}_q[X]$. Then $\deg \rho = \deg \gamma < k$ and $(\gamma(a), \gamma(a^2), \ldots, \gamma(1)) = (\rho(1), \ldots, \rho(a^{n-1})) \in C$. Therefore, C is cyclic. □

Remark III.12.61. The codes constructed in Theorem III.12.60 for $A = \langle a \rangle$ are named after Reed and Solomon. They are used, among other things, for Compact Discs (CD) and QR codes (two-dimensional barcodes). In contrast to the codes treated so far, they require large alphabets (for CDs, one uses $q = 2^8$).

Exercises

Varieties

Exercise III.1 (2 points)**.** Let K be an arbitrary field (not necessarily algebraically closed) and $I \lhd K[X_1, \ldots, X_n]$. Show that there exists a point $(x_1, \ldots, x_n) \in \overline{K}^n$ with $\alpha(x_1, \ldots, x_n) = 0$ for all $\alpha \in I$.

Exercise III.2 $(2 + 2 + 2$ points)**.** Let $A \in \mathrm{A}(K^n)$ and $B \in \mathrm{A}(K^m)$. Show:

(a) $A \times B \in \mathrm{A}(K^{n+m})$.

(b) If A and B are irreducible, then so is $A \times B$.

(c) $\dim(A \times B) = \dim(A) + \dim(B)$.

Exercise III.3 (2 points)**.** Let $R \subseteq S$ be integral domains such that S is a finitely generated R-module. Show that R is a field if and only if S is a field.

Exercise III.4 (2 points)**.** Give a new proof for Zariski's Lemma using Noether normalization and Exercise III.3.

Exercise III.5 (2 points)**.** Show that every open subset of K^n with respect to the Zariski topology is empty or infinite.

Exercise III.6 (2 points)**.** Let $\leq_l$ be the lexicographical monomial order on $R := K[X_1, \ldots, X_n]$. Show that

$$\alpha < \beta \ :\Longleftrightarrow\ \deg \alpha < \deg \beta \vee (\deg \alpha = \deg \beta \wedge \alpha <_l \beta).$$

also defines a monomial order on R.

Exercise III.7 (3 points)**.** Let $\beta_1, \ldots, \beta_k \in K[X_1, \ldots, X_n] \setminus \{0\}$ and $I = (\beta_1, \ldots, \beta_k)$. For all $\alpha \in K[X_1, \ldots, X_n]$, let $\alpha \in I$ hold if and only if every remainder in the division of α by $\beta_1, \ldots, \beta_k$ vanishes. Show that $\beta_1, \ldots, \beta_k$ is a Gröbner basis of I.
Remark: This is the converse of Theorem III.2.57.

Exercise III.8 (2 points)**.** Let B be a Gröbner basis of $I \trianglelefteq K[X_1, \ldots, X_n]$ with respect to the lexicographical monomial order and $1 \leq i \leq n$. Then $B \cap K[X_i, \ldots, X_n]$ is a Gröbner basis of the elimination ideal $I \cap K[X_i, \ldots, X_n]$.

Exercise III.9 (2 points)**.** Let $I = (\beta_1, \ldots, \beta_k)$ and $J = (\gamma_1, \ldots, \gamma_l)$ be ideals in $R := K[X_1, \ldots, X_n]$. Let Y be a new variable. Show that

$$I \cap J = (\beta_1 Y, \ldots, \beta_k Y, \gamma_1(Y-1), \ldots, \gamma_l(Y-1)) \cap R.$$

Remark: The intersection $I \cap J$ is thus reduced to an elimination ideal, which can be calculated using Exercise III.8.

Exercise III.10 $(2+2$ points)**.** Construct a Gröbner basis of

$$I = (2XY^2 + 3X + 4Y^2, Y^2 - 2Y - 2) \trianglelefteq \mathbb{C}[X, Y].$$

Decide whether $2X^3Y^3 + 4Y^2 \in I$ holds.

Exercise III.11 (2 points)**.** Construct the reduced Gröbner basis of $(XY - Y^2, X^2 - 1) \trianglelefteq \mathbb{C}[X, Y]$.

Exercise III.12 (2 points)**.** Let B be the reduced Gröbner basis of $I \trianglelefteq K[X_1, \ldots, X_n]$. Show that $1 \in I \iff B = \{1\}$.

Modular Representations

Exercise III.13 $(2+2$ points)**.** Let A be a K-algebra and V an A-module. We define $\mathrm{J}^0(V) := V$, $\mathrm{Soc}(V)^0 := 0$ and

$$\mathrm{J}^{n+1}(V) := \mathrm{J}(\mathrm{J}^n(V)), \qquad \mathrm{Soc}^n(V)/\mathrm{Soc}^{n-1}(V) := \mathrm{Soc}(V/\mathrm{Soc}^{n-1}(V))$$

for $n \geq 0$. Let $0 = V_0 \leq \ldots \leq V_k = V$, such that V_i/V_{i-1} is semisimple for $i = 1, \ldots, k$. Show:

(a) $V_i \leq \mathrm{Soc}^i(V)$ and $\mathrm{J}^i(V) \leq V_{k-i}$ for $i = 0, \ldots, k$.

(b) $\mathrm{J}^i(V) = 0 \iff \mathrm{Soc}^i(V) = V$.

Remark: The smallest $l \in \mathbb{N}_0$ with $\mathrm{J}^l(V) = 0$ is called the *Loewy length* of V. It measures how far a module is from being a semisimple module.

Exercise III.14 (2 points)**.** Let K be a field and V a finite-dimensional K-vector space. Show that $V^{\otimes n} := V \otimes \ldots \otimes V$ (n factors) becomes a KS_n-module via

$$\sigma(v_1 \otimes \ldots \otimes v_n) := v_{\sigma^{-1}(1)} \otimes \ldots \otimes v_{\sigma^{-1}(n)}.$$

Exercise III.15 (3 points)**.** Let K be an arbitrary field and $G \cong C_n$. Show that KG has at most n indecomposable modules up to isomorphism.
Hint: One can use the Weierstrass normal form.

Exercise III.16 (3 points)**.** Let K be an infinite field of characteristic $p > 0$ and $G \cong C_p^2$. Show that KG has infinitely many non-isomorphic indecomposable modules of dimension 2.

Exercise III.17 (2 + 2 points)**.** Let $H \leq G$ and U, V be KH-modules. Construct a vector space monomorphism $\mathrm{Hom}_{KH}(U,V) \to \mathrm{Hom}_{KG}(U^G, V^G)$. Show that the vector spaces are not isomorphic in general.

Exercise III.18 (3 points)**.** Let K be an algebraically closed field of characteristic $p > 0$. Let $N \trianglelefteq G$ with $p \nmid |G:N|$. Let V be a simple KG-module and $U \leq V_N$ a simple KN-module. Show that U^G is semisimple and the multiplicity of V as a composition factor of U^G coincides with the ramification index.
Hint: One can use Exercise II.65.

Exercise III.19 (3 + 3 points)**.** Let P be a projective-indecomposable KG-module and $S := \mathrm{Soc}(P)$. Let $N \trianglelefteq G$ and T be a simple submodule of S_N. Let Q be a projective-indecomposable KN-module with $\mathrm{Soc}(Q) \simeq T$. Show:

(a) There exists an $e \leq |G_T : N|$ with

$$P_N \simeq \bigtimes_{gG_T \in G/G_T} (g \otimes Q)^e.$$

(b) Let $W \in \Gamma(G_U, U)$ and R be a projective-indecomposable KG_U-module with $\mathrm{Soc}(R) \simeq W$. Then R^G is projective-indecomposable with $\mathrm{Soc}(R^G) \simeq W^G$.

Exercise III.20 (4 points)**.** Let K be a field and A be the algebra of all matrices of the form

$$\begin{pmatrix} a & b & . & . \\ . & c & . & . \\ . & . & c & d \\ . & . & . & a \end{pmatrix} \in K^{4\times 4}.$$

Show that $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ is the Cartan matrix of A.

Categories

Exercise III.21 (2 + 2 points)**.** Let G be a group and $\mathcal{C}$ be the category associated to G as in Example III.5.4(iv).

(a) Show that the congruences of $\mathcal{C}$ correspond to the normal subgroups of G.

(b) Derive the isomorphism theorem for groups from Theorem III.5.12.

Exercise III.22 (2 points)**.** Show that a functor of the form $\mathbf{Rng} \to \mathbf{Cat}$, $R \mapsto {}_R\mathbf{mod}$ exists.

Exercise III.23 (2 points)**.** Let $\mathcal{C}$, $\mathcal{D}$ be categories and $\Phi\colon \mathcal{C} \to \mathcal{D}$ be a functor. Show that Φ is an isomorphism if and only if Φ is full and faithful and $\Phi\colon \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ is surjective.

Exercise III.24 (3 points)**.** Decide which of the following functors is full or faithful:

(a) $\mathrm{Hom}(A, .)\colon \mathbf{Grp} \to \mathbf{Set}$.

(b) $\mathrm{GL}(n,.)\colon \mathbf{Rng} \to \mathbf{Grp}$.

(c) $\Phi_K\colon \mathbf{grp} \to \mathbf{Rng}$, $G \mapsto KG$ for a field K.

Exercise III.25 (3 points)**.** Let K be a field. Construct an equivalence ${}_K\mathbf{mod} \approx {}_K\mathbf{mod}^o$.

Exercise III.26 $(2+2+2$ points$)$**.**

(a) Construct a functor $\Phi\colon \mathbf{Grp} \to \mathbf{Ab}$, $G \mapsto G/G'$ (cf. Exercise I.31).

(b) Show that Φ is left-adjoint to the forgetful functor $\mathbf{Ab} \to \mathbf{Grp}$.

(c) Show that *no* functor of the form $\mathbf{Grp} \to \mathbf{Ab}$, $G \mapsto \mathrm{Z}(G)$ exists.

Morita Theory

Exercise III.27 (2 points)**.** Let M and N be left modules over a commutative ring R. Show that $M \otimes_{\mathbb{Z}} N$ coincides with the tensor product defined in Exercise II.53.

Exercise III.28 $(2+2$ points$)$**.** Let $(M_i)_{i\in I}$ and $(N_j)_{j\in J}$ be families of R-S-bimodules and R-T-bimodules, respectively. Show:

(a) There exists an S-T-isomorphism

$$\mathrm{Hom}_R\Big(\coprod_{i\in I} M_i, \bigtimes_{j\in J} N_j\Big) \simeq \bigtimes_{i\in I}\bigtimes_{j\in J} \mathrm{Hom}(M_i, N_j).$$

(b) If M is a finitely generated R-S-bimodule, then there exists an S-T-isomorphism

$$\mathrm{Hom}_R\Big(M, \coprod_{j\in J} N_j\Big) \simeq \coprod_{j\in J} \mathrm{Hom}_R(M, N_j).$$

Exercise III.29 $(1+3+3$ points$)$**.** Let R and S be rings. A sequence

$$\ldots \to A_{-1} \xrightarrow{f_{-1}} A_0 \xrightarrow{f_0} A_1 \to \ldots$$

of R-S-homomorphisms is called *exact* at position i if $f_{i-1}(A_{i-1}) = \mathrm{Ker}(f_i)$ holds. Let

$$\sigma\colon 0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

be any sequence of R-S-homomorphisms. Show:

(a) σ is exact at position A (resp. C) if and only if f is injective (resp. g is surjective).

(b) Let M be an R-S-module. If σ is exact at position A and B, then

$$0 \to \mathrm{Hom}_R(M, A) \xrightarrow{f\circ .} \mathrm{Hom}_R(M, B) \xrightarrow{g\circ .} \mathrm{Hom}_R(M, C)$$

is exact at $\mathrm{Hom}_R(M, A)$ and $\mathrm{Hom}_R(M, B)$.

(c) Let M be an S-R-module. If σ is exact at position B and C, then

$$A \otimes_S N \xrightarrow{f \otimes \mathrm{id}_N} B \otimes_S N \xrightarrow{g \otimes \mathrm{id}_N} C \otimes_S N \to 0$$

is exact at $B \otimes_S N$ and $C \otimes_S N$.

Exercise III.30 ($3 + 3$ points)**.** Let R and S be rings.

(a) (*Five Lemma*) Let the following diagram of R-S-homomorphisms be commutative and let the rows be exact (wherever it makes sense).

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{j} & E \\ \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle t} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{j'} & E' \end{array}$$

Furthermore, let r be surjective, v injective, and s and u bijective. Show that t is bijective.

(b) (*Nine Lemma*) Let the following diagram of R-S-homomorphisms be commutative, let the columns be exact, and let the last two rows be exact (wherever it makes sense).

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & A_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle g_2} & & \downarrow{\scriptstyle g_3} & & \\ 0 & \longrightarrow & B_1 & \xrightarrow{f_3} & B_2 & \xrightarrow{f_4} & B_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g_4} & & \downarrow{\scriptstyle g_5} & & \downarrow{\scriptstyle g_6} & & \\ 0 & \longrightarrow & C_1 & \xrightarrow{f_5} & C_2 & \xrightarrow{f_6} & C_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

Show that the first row is also exact.

Exercise III.31 (2 points)**.** Let $(R, S, M, N, \mathfrak{R}, \mathfrak{S})$ be a Morita context with surjective $\mathfrak{R}$. Construct an S-R-isomorphism $N \to \mathrm{Hom}_S(M, S)$.
Remark: One is therefore in the situation of Example III.6.33.

Central-simple algebras

Exercise III.32 (2 points)**.** Let A, B and C be K-algebras and $q_A \colon A \to C$, $q_B \colon B \to C$ homomorphisms with $q_A(a)q_B(b) = q_B(b)q_A(a)$ for all $a \in A$, $b \in B$ and the following universal property:
For algebra homomorphisms $f_A \colon A \to D$, $f_B \colon B \to D$ with $f_A(a)f_B(b) = f_B(b)f_A(a)$ for all $a \in A$, $b \in B$ there exists exactly one homomorphism $f \colon C \to D$ with $f \circ q_A = f_A$ and $f \circ q_B = f_B$. Show $C \cong A \otimes B$.
Remark: The tensor product is thus a commutative variant of the coproduct in the category K-**alg** of finite-dimensional K-algebras.

Exercise III.33 (2 points)**.** Let $K \subseteq M_i \subseteq L$ be finite field extensions with $M_1 \cap M_2 = K$. Let $K \subseteq M_1$ be a Galois extension. Show that the K-algebra $M_1 \otimes_K M_2$ is isomorphic to the compositum M_1M_2.

Exercise III.34 (2+2 points)**.** Let G be a finite group, K a field and $\gamma \in Z^2(G, K^\times)$. On the K-vector space $K_\gamma G := KG$ we define a multiplication

$$x \cdot y := \gamma(x, y)xy \qquad (x, y \in G).$$

Show:

(a) $K_\gamma G$ is a K-algebra.

(b) The isomorphism type of $K_\gamma G$ depends only on $\overline{\gamma} \in H^2(G, K^\times)$.

Exercise III.35 (1 + 2 + 2 + 2 + 2 + 2 points)**.** Let $K \subseteq L$ be a Galois extension with cyclic Galois group $G = \mathrm{Gal}(L|K) = \langle x \rangle \cong C_n$. Show:

(a) The *norm map* $N\colon L^\times \to K^\times$, $a \mapsto \prod_{\sigma \in G} \sigma(a)$ is a homomorphism.

(b) For $\lambda \in K^\times$ there exists $\gamma_\lambda \in Z^2(G, L^\times)$ with

$$\gamma_\lambda(x^i, x^j) = \begin{cases} 1 & \text{if } i + j < n, \\ \lambda & \text{if } i + j \geq n, \end{cases}$$

where $0 \leq i, j < n$.

(c) $\gamma_\lambda \in B^2(G, L^\times) \iff \lambda \in N(L^\times)$.

(d) $H^2(G, L^\times) \cong K^\times / N(L^\times)$.

(e) If K is finite, then $H^2(G, L^\times) = 1$ holds.

(f) Theorem II.8.7 follows from (e).

Remark: The corresponding algebras $L_\gamma G$ are called *cyclic*.

Exercise III.36 (2 points)**.** Let $n \in \mathbb{N}$ be odd and $N\colon \mathbb{Q}_n^\times \to \mathbb{Q}^\times$ be the norm map as in Exercise III.35. Show $N(x) > 0$ for all $x \in \mathbb{Q}_n^\times$.
Hint: $\zeta^{-1} = \overline{\zeta}$.

Exercise III.37 (1 + 3 + 3 + 2 points)**.** Let $\zeta := e^{2\pi \mathrm{i}/7} \in \mathbb{C}$, $\omega_1 := \zeta + \zeta^{-1}$, $\omega_2 := \zeta^2 + \zeta^{-2}$ and $\omega_3 := \zeta^3 + \zeta^{-3}$. Show:

(a) $\omega_1, \omega_2, \omega_3$ is a normal basis of $K := \mathbb{Q}(\omega) = \mathbb{Q}_7 \cap \mathbb{R}$ over $\mathbb{Q}$.

(b) $N(a\omega_1 + b\omega_2 + c\omega_3) = (a^3 + b^3 + c^3) + 3(a^2b + ac^2 + b^2c) - 4(a^2c + ab^2 + bc^2) - abc$ for $a, b, c \in \mathbb{Q}$ with the norm map from Exercise III.35.

(c) $2 \notin N(K^\times)$.
Hint: Write $x = \frac{1}{d}(a\omega_1 + b\omega_2 + c\omega_3)$ with $d \in \mathbb{N}$ minimal. Consider $N(x)$ modulo 2.

(d) There exists a 9-dimensional $\mathbb{Q}$-division algebra D with $D \not\equiv D^o$.
Hint: Exercise III.35.
Remark: Compare Exercise II.39.

Path Algebras

Exercise III.38 (2 points)**.** Let K be a field and Q a connected quiver. Show that KQ is commutative if and only if $|Q_0| = 1$ and $|Q_1| \leq 1$ holds.

Exercise III.39 (2 points)**.** Let K be a field and $Q = (Q_0, Q_1, s, t)$ a quiver. Let $Q^o := (Q_0, Q_1, t, s)$. Show $KQ^o \cong (KQ)^o$.

Exercise III.40 (4 points)**.** Let K be a field and

$$A := \left\{ \begin{pmatrix} a & 0 & 0 \\ b & c & 0 \\ d & 0 & c \end{pmatrix} : a, b, c, d \in K \right\}.$$

Construct $Q(A)$ and an admissible ideal $I \trianglelefteq KQ(A)$ with $A \cong KQ(A)/I$.

Exercise III.41 (3 points)**.** Let K be a field, Q a quiver and $I \trianglelefteq KQ$ admissible. Let $A := KQ/I$ and M an A-module. Let Δ be the corresponding representation of Q from Theorem III.8.32. Show that M is semisimple if and only if $\Delta(\alpha) = 0$ for all $\alpha \in Q_1$ holds.

Lie Algebras

Exercise III.42 (2 points)**.** Let L be a Lie algebra and $x, y \in L$. Show $[x, y, x, y] = [y, x, x, y]$.

Exercise III.43 (2 points)**.** Let L be a Lie algebra. Show that the Lie bracket is associative (i. e. $[x, [y, z]] = [[x, y], z]$ for all $x, y, z \in L$) if and only if $[L, L] \subseteq \mathrm{Z}(L)$ holds.

Exercise III.44 (2 points)**.** Calculate $\mathrm{Z}(\mathfrak{sl}(n, K))$ for every field K.

Exercise III.45 (2 + 2 points)**.**

(a) Show that there is, up to isomorphism, only one 2-dimensional non-abelian Lie algebra.

(b) Classify all Lie algebras L with $\dim L' = 1$.

Exercise III.46 (2 + 2 points)**.** Let V be a finite-dimensional vector space, $x, y \in \mathfrak{gl}(V)$ and $n \in \mathbb{N}_0$. Prove the *Leibniz rules*

$$\mathrm{ad}_x(y^n) = [x, y^n] = \sum_{k=1}^{n} y^{k-1}[x, y]y^{n-k},$$

$$\mathrm{ad}_x^n(y) = \sum_{k=0}^{n} \binom{n}{k} (-1)^k x^{n-k} y x^k.$$

Exercise III.47 (2 points)**.** Let L be a non-abelian Lie algebra. Show $\dim L/\mathrm{Z}(L) \geq 2$.

Exercise III.48 (2 points)**.** Show that a complex Lie algebra L is nilpotent if and only if every 2-dimensional subalgebra is abelian.

Exercise III.49 (4 points)**.** State and prove the Jordan-Hölder theorem for Lie algebras.

Exercise III.50 (3 points)**.** Let L be the Lie subalgebra of $\mathfrak{gl}(3,2)$ generated by the matrices E_{13}, $E_{12}+E_{21}$ and $E_{11}+E_{33}$. Show that L is solvable, but L' is not nilpotent.

Exercise III.51 ($2+2+2$ points)**.** Let L be a Lie algebra. A linear map $\delta\colon L \to L$ with $\delta([x,y]) = [\delta(x),y]+[x,\delta(y)]$ for $x,y \in L$ is called a *derivation* (cf. product rule). Show:

(a) The derivations of L form a Lie subalgebra $\mathrm{Der}(L)$ of $\mathfrak{gl}(V)$.

(b) $\mathrm{ad}(L) \trianglelefteq \mathrm{Der}(L)$. The elements in $\mathrm{ad}(L)$ are called *inner* derivations.

(c) Let $\operatorname{char} K = 0$ and $\delta \in \mathrm{Der}(L)$ be nilpotent. Then $\exp(\delta) := \sum_{k=0}^{\infty} \frac{1}{k!}\delta^k \in \mathrm{Aut}(L)$.

Exercise III.52 ($2+2+3$ points)**.** Let $p := \operatorname{char} K > 0$. We define a Lie algebra W_p over K with basis $b_{-1}, b_0, \ldots, b_{p-2}$ and

$$[b_i, b_j] := \begin{cases} (j-i)e_{i+j} & \text{if } -1 \le i+j \le p-2, \\ 0 & \text{otherwise.} \end{cases}$$

Show:

(a) W_p is a Lie algebra.

(b) $W_3 \cong \mathfrak{sl}(2,K)$.

(c) For $p > 2$, W_p is simple.

Remark: W_p is called the *Witt algebra* over K. For dimension reasons, W_p for $p > 3$ does not correspond to any of the Lie algebras from Remark III.9.57.

Exercise III.53 ($2+2+3+3+4+3$ points)**.** Let G be a p-group with exponent p, i. e. $x^p = 1$ for all $x \in G$. For $x,y \in G$ let $[x,y] := xyx^{-1}y^{-1}$ be the commutator of x,y (Exercise I.31). As for Lie algebras, we define $G^{[1]} := G$ and

$$G^{[k+1]} := [G, G^{[k]}] = \langle [g,x] : g \in G,\ x \in G^{[k]} \rangle$$

for $k \ge 1$. Show:

(a) There exists a $c \in \mathbb{N}_0$ with $G^{[c+1]} = 1$. The smallest c with this property is called the *nilpotency class* of G.

(b) For $k \in \mathbb{N}$, $G^{[k]}/G^{[k+1]}$ is an $\mathbb{F}_p$-vector space with $xG^{[k+1]} + yG^{[k+1]} := xyG^{[k+1]}$ for $x,y \in G^{[k]}$.

(c) The minimal number of generators of G is $d := \log_p |G/G'| = \dim_{\mathbb{F}_p}(G/G^{[2]})$.

(d) For $k,l \in \mathbb{N}$, the relation $[G^{[k]}, G^{[l]}] \subseteq G^{[k+l]}$ holds.

(e) For $x \in G^{[k]}$ and $y \in G^{[l]}$ let $[xG^{[k+1]}, yG^{[l+1]}] := [x,y]G^{[k+l+1]} \in G^{[k+l]}/G^{[k+l+1]}$. Then

$$L(G) := \bigtimes_{k=1}^{c} G^{[k]}/G^{[k+1]}$$

is a Lie algebra over $\mathbb{F}_p$, where $[.,.]$ is extended bilinearly.

(f) $L(G)$ is generated by d elements and $L(G)^{[n]} \cong \bigtimes_{k=n}^{c} G^{[k]}/G^{[k+1]}$ for $n = 1, \ldots, c$. In particular, $L(G)$ is nilpotent with class c. Thus, one can apply Example III.9.90.

Remark: For $p = 2$, G is abelian, i. e. $c \leq 1$. According to the solution of the restricted Burnside problem, $|G|$ (and thus c) is in general bounded by a function in p and d.[1] For $p > c$, there exists exactly one group G with exponent p, nilpotency class c and $L(G) \cong \mathfrak{L}_d/\mathfrak{L}_d^{[c+1]}$, where $\mathfrak{L}_d$ is the free Lie algebra of rank d over $\mathbb{F}_p$ (without proof).

Valuation Rings

Exercise III.54 (2 points)**.** Show that every local principal ideal domain R is a valuation ring of an ultrametric valuation on $Q(R)$.

Exercise III.55 (2 points)**.** Let K be a field with ultrametric valuation ν. Let $\alpha = \sum_{k=0}^{n} a_k X^k \in K[X]$ be monic with root $x \in K$. Show $\nu(x) \leq \max_{0 \leq k \leq n} \nu(a_k)$.
Remark: Comparison with Theorem A.2.2.

Exercise III.56 ($2+2+2$ points)**.** Let K be a field with a complete ultrametric valuation. Show that a series $\sum_{n=1}^{\infty} x_n$ converges in K if and only if $(x_n)_n$ is a null sequence. If applicable,

$$\nu\Big(\sum_{n=1}^{\infty} x_n\Big) \leq \max_{n \in \mathbb{N}} \nu(x_n), \qquad \sum_{n=1}^{\infty} x_n = \sum_{n=1}^{\infty} x_{\pi(n)}$$

holds for all $\pi \in \mathrm{Sym}(\mathbb{N})$.

Exercise III.57 (3 points)**.** Let $\epsilon = \frac{1}{7}$. Construct $x \in \mathbb{Q}$ with $|x-1| < \epsilon$, $\nu_5(x-3) < \epsilon$ and $\mu_7(x-4) < \epsilon$.

Exercise III.58 (3 points)**.** (Eisenstein) Let K be a field with a discrete valuation and valuation ring R. Let $\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X]$ with $a_0, \ldots, a_{n-1} \in \mathrm{J}(R)$ and $a_0 \notin \mathrm{J}(R)^2$. Show that α is irreducible.

Exercise III.59 (3 points)**.** Let K be a field and ν the valuation of $K(X)$ from Example III.10.3. Show that the completion of $K(X)$ is isomorphic to the field of formal Laurent series $K((X))$.

Exercise III.60 (3 points)**.** Investigate for which $x \in \mathbb{Q}_{[p]}$ the series $\sum_{n=0}^{\infty} \frac{x^n}{n!}$ converges.

[1] See lecture notes combinatorial group theory

Exercise III.61 $(2 + 2 + 3$ points$)$**.**

(a) Determine the p-adic expansion of $-1 \in \mathbb{Z}_{[p]}$.

(b) Construct a primitive fourth root of unity in $\mathbb{Z}_{[5]}$ up to four "digits before the decimal point".
Note: $\zeta^2 = -1$.

(c) Verify $\sum_{n=1}^{\infty} \frac{2^n}{n} = 0$ in $\mathbb{Q}_{[2]}$.

Exercise III.62 (2 points)**.** Let $p \in \mathbb{P}$ and $p \nmid n \in \mathbb{N}$. Show that $a, k \in \mathbb{N}$ with $an = p^k - 1$ and

$$\frac{1}{n} = -a \sum_{i=0}^{\infty} p^{ki} \in \mathbb{Z}_{[p]}$$

exist.

Exercise III.63 (3 points)**.** Show that every automorphism on $\mathbb{Q}_{[p]}$ is continuous and conclude $\mathrm{Aut}(\mathbb{Q}_{[p]}) = 1$.
Note: Compare Exercise I.53.

Exercise III.64 $(3 + 3$ points$)$**.**

(a) Show that the p-adic expansion of $\alpha \in \mathbb{Z}_{[p]}$ is finite if and only if $\alpha \in \mathbb{N}_0$ holds.

(b) Show that the p-adic expansion of $\alpha \in \mathbb{Q}_{[p]}$ is finite or periodic if and only if $\alpha \in \mathbb{Q}$ holds.

Exercise III.65 $(2 + 1 + 3$ points$)$**.** Let $p \in \mathbb{P}$, $K = \mathbb{Q}_{[p]}$ and $\overline{K}$ the algebraic closure of K with valuation $\tilde{\nu}_p$. Assume that $\overline{K}$ is complete. Show:

(a) $|\overline{K} : K| = \infty$.
Note: Remark III.10.42.

(b) Let $x_1, \ldots \in \overline{K}$ be linearly independent over K and $q_1, \ldots \in \mathbb{Q}$ with the following properties:

- $\tilde{\nu}_p(q_1 x_n) > \tilde{\nu}_p(q_2 x_2) > \ldots$ and $\lim_{n\to\infty} \tilde{\nu}_p(q_n x_n) = 0$.
- $\tilde{\nu}_p(q_{n+1} x_{n+1}) < \tilde{\nu}_p(s_n - y)$, where $s_n := \sum_{k=1}^{n} q_k x_k$ and y runs through the remaining roots of the minimal polynomial μ_{s_n}.

Then s_n is a Cauchy sequence and $s := \lim_{n\to\infty} s_n = \sum_{n=1}^{\infty} q_n x_n \in \overline{K}$ exists.

(c) For $n \in \mathbb{N}$, $s_n \in K(s)$ holds. This yields the contradiction $|K(s) : K| = \infty$. Thus $\overline{K}$ is not complete.
Note: Corollary III.10.44.

Galois Theory

Exercise III.66 (2 points)**.** Let V be a module over a division ring R with basis B. For $U \leq V$ define minimal elements $u \in U$ w.r.t. B as in Remark III.11.8. Show that U is generated by minimal elements.

Coding Theory

Exercise III.67 (1 + 2 + 2 points)**.** We consider the (linear) encoding function $\gamma\colon \mathbb{F}_2^2 \to \mathbb{F}_2^5$ with the following values

$$(0,0) \mapsto (0,0,0,0,0), \qquad (0,1) \mapsto (0,1,1,0,1),$$
$$(1,0) \mapsto (1,0,1,1,0), \qquad (1,1) \mapsto (1,1,0,1,1).$$

(a) Show that this code can correct one error.

(b) Decode the following message with it:

11110 10100 01101 00110 10010 11101 00001 11011 10110 11001 01000 01001

and decode the result further with the ASCII code.

(c) Suppose the probability of a incorrectly transmitted bit is $p = 0{,}01$. How high is the probability that you have correctly decoded the message in (b)?

Exercise III.68 (3 + 3 points)**.** Let $H = H_{2^n}$ be the $2^n \times 2^n$ Hadamard matrix constructed in Example III.12.9 and C the code from Theorem III.12.12. Show:

(a) If one replaces all -1 by 0, then C becomes a binary linear code.
Hint: Induction on n.

(b) In the case $n = 3$, C from (a) is equivalent to the extended Hamming code $\widehat{H_7}$.

Exercise III.69 (3 points)**.** Let C be a non-trivial perfect code of length $n \leq 1000$ with minimum distance d over an alphabet with $q \leq 1000$ elements. Show (with computer) that one of the following statements holds:

(i) $n = d$ is odd and $|C| = q = 2$ (parameters of W_n).

(ii) $n = \frac{q^m-1}{q-1}$, $|C| = q^{n-m}$ and $d = 3$ with $m \geq 2$ (parameters of H_n).

(iii) $n = 11$, $|C| = q^6 = 3^6$ and $d = 5$ (parameters of G_{11}).

(iv) $n = 23$, $|C| = q^{12} = 2^{12}$ and $d = 7$ (parameters of G_{23}).

Hint: Example III.12.24 and proof of Theorem III.12.38.

Exercise III.70 (3 points)**.** Show that the code with generator matrix

$$\begin{pmatrix} 1 & 1 & . & 1 & . & . & . \\ . & 1 & 1 & . & 1 & . & . \\ . & . & 1 & 1 & . & 1 & . \\ . & . & . & 1 & 1 & . & 1 \end{pmatrix}$$

is equivalent to H_7.
Hint: Calculate a check matrix.

Exercise III.71 (1 + 2 + 3 points)**.** Let $C = G_{24}$ be the extended binary Golay code. Show:

(a) $(1, \ldots, 1) \in C$.

(b) There exist $a, b \in \mathbb{N}_0$ with $W_C(X) = 1 + aX^8 + bX^{12} + aX^{16} + X^{24}$ and $2a + b = 4094$.
Hint: Proof of Theorem III.12.43 and (a).

(c) $W_C(X) = 1 + 759X^8 + 2576X^{12} + 758X^{16} + X^{24}$.
Hint: MacWilliams identity.

Exercise III.72 (2 points)**.** Determine the prime factorization of $X^{60} - 1$ in $\mathbb{F}_3[X]$.

Appendix

A.1 Quadratic Residues

Definition A.1.1.

(i) Let p be a prime number and $n \in \mathbb{Z} \setminus p\mathbb{Z}$. One calls n a *quadratic residue* modulo p, if there exists a $k \in \mathbb{Z}$ with $n \equiv k^2 \pmod{p}$. Otherwise, one calls n a *quadratic non-residue* modulo p. For $n \in \mathbb{Z}$, one defines the *Legendre symbol*

$$\left(\frac{n}{p}\right) := \begin{cases} 1 & \text{if } n \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } n \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } p \mid n \end{cases}$$

of n *modulo* p.

(ii) Let $n \in \mathbb{Z}$ and $a \in \mathbb{N}$ odd with prime factorization $a = p_1 \dots p_k$ (the case $a = 1$ with $k = 0$ is allowed). One calls

$$\left(\frac{n}{a}\right) := \left(\frac{n}{p_1}\right) \dots \left(\frac{n}{p_k}\right)$$

the *Jacobi symbol* of n *modulo* a.

Remark A.1.2. For odd $a, b \in \mathbb{N}$, one proves in number theory[1] the so-called *quadratic reciprocity law*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$

with the two *supplementary laws*

$$\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}, \qquad \left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}}.$$

In the following, we give some applications.

Theorem A.1.3 (Zolotarev)**.** *Let $n \in \mathbb{N}$ odd and $k \in \mathbb{Z}$ coprime to n. Let $\sigma \in \mathrm{Sym}(\mathbb{Z}/n\mathbb{Z})$ with $\sigma(a + n\mathbb{Z}) = ka + n\mathbb{Z}$ for all $a \in \mathbb{Z}$. Then $\mathrm{sgn}(\sigma) = \left(\frac{k}{n}\right)$ holds.*

Proof. Let $n = p_1^{m_1} \dots p_s^{m_s}$ be the prime factorization of n. According to the Chinese Remainder Theorem,

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{m_s}\mathbb{Z} =: R, \\ a + n\mathbb{Z} &\mapsto (a + p_1^{m_1}\mathbb{Z}, \dots, a + p_s^{m_s}\mathbb{Z}) \end{aligned}$$

is a ring isomorphism. Let $\sigma_i \in \mathrm{Sym}(\mathbb{Z}/p_i^{m_i}\mathbb{Z})$ with $\sigma_i(a+p_i^{m_i}\mathbb{Z}) = ka+p_i^{m_i}\mathbb{Z}$ for $a \in \mathbb{Z}$. Let $\hat{\sigma}_i \in \mathrm{Sym}(R)$ with $\hat{\sigma}_i(a_1, \dots, a_s) = (a_1, \dots, \sigma_i(a_i), \dots, a_s)$ for all $(a_1, \dots, a_s) \in R$. If one identifies $\mathbb{Z}/n\mathbb{Z}$ with R, then

[1] See lecture notes Number Theory

$\sigma = \hat{\sigma}_1 \dots \hat{\sigma}_s$ and $\operatorname{sgn}(\hat{\sigma}_i) = \operatorname{sgn}(\sigma_i)^{n/p_i^{m_i}} = \operatorname{sgn}(\sigma_i)$, since n is odd. According to the definition of the Jacobi symbol, we can assume $n = p_1^{m_1} = p^m$.

According to Theorem I.8.34, $(\mathbb{Z}/n\mathbb{Z})^\times \cong C_{p^{m-1}(p-1)}$. Since p is odd, we can replace k by k^{p^m} without changing $\operatorname{sgn}(\sigma)$ or $\left(\frac{k}{n}\right)$. Subsequently, $q := |\langle\sigma\rangle|$ is a divisor of $p-1$. k is a square in $\mathbb{Z}/p\mathbb{Z}$ if and only if q also divides $\frac{p-1}{2}$. Thus

$$\left(\frac{k}{n}\right) = \left(\frac{k}{p}\right)^m = (-1)^{\frac{m(p-1)}{q}}.$$

For $a \in \mathbb{Z} \setminus n\mathbb{Z}$, $ka \not\equiv a \pmod{n}$. Therefore, σ is a disjoint product of $\frac{n-1}{q}$ cycles of length q. This shows $\operatorname{sgn}(\sigma) = (-1)^{\frac{n-1}{q}}$. The claim now follows from

$$\frac{n-1}{q} = (p^{m-1} + \dots + p + 1)\frac{p-1}{q} \equiv m\frac{p-1}{q} \pmod{2}. \qquad \square$$

Remark A.1.4. In the proof that quadratic number fields lie in cyclotomic fields (Theorem I.12.23), a strange sum of roots of unity appeared, whose sign was irrelevant. In fact, Gauss needed several years to determine this sign. We give a modern proof.

Definition A.1.5. For an odd prime p, let $\zeta := e^{2\pi \mathrm{i}/p} \in \mathbb{C}$ and

$$G_p := \sum_{k=1}^{p} \zeta^{k^2} \in \mathbb{C}.$$

G_p is called the (*quadratic*) *Gauss sum* with respect to p.

Remark A.1.6.

(i) For every quadratic residue q modulo p, the equation $k^2 = q$ has exactly two solutions in $\mathbb{F}_p^\times$. With the Jacobi symbol, it therefore holds that

$$G_p = 1 + 2 \sum_{\substack{1 \le q \le p-1 \\ \text{QR}}} \zeta^q = \sum_{k=1}^{p} \left(\left(\frac{k}{p}\right) + 1 \right) \zeta^k = \sum_{k=1}^{p} \left(\frac{k}{p}\right)\zeta^k + \sum_{k=1}^{p} \zeta^k = \sum_{k=1}^{p} \left(\frac{k}{p}\right)\zeta^k.$$

(ii) If one replaces ζ by another primitive p-th root of unity, say ζ^a, one obtains

$$\sum_{k=1}^{p} \left(\frac{k}{p}\right)\zeta^{ak} = \left(\frac{a}{p}\right) \sum_{k=1}^{p} \left(\frac{ak}{p}\right)\zeta^{ak} = \left(\frac{a}{p}\right) G_p$$

from the multiplicativity of the Jacobi symbol. The Gauss sum thus depends on the choice of ζ.

Theorem A.1.7 (Gauss)**.** *For every odd prime p, it holds that*

$$G_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod{4}, \\ \sqrt{-p} & \text{if } p \equiv -1 \pmod{4}, \end{cases}$$

where $\sqrt{-p}$ denotes the root with positive imaginary part.

Proof. According to Remark A.1.6, it holds that

$$G_p^2 = \left(\sum_{k=1}^{p} \left(\frac{k}{p}\right)\zeta^k\right)^2 = \sum_{k,l=1}^{p} \left(\frac{kl}{p}\right)\zeta^{k+l} = \sum_{k=1}^{p}\zeta^k \sum_{l=1}^{p-1}\left(\frac{l(k-l)}{p}\right) = \sum_{k=1}^{p}\zeta^k \sum_{l=1}^{p-1}\left(\frac{kl^{-1}-1}{p}\right),$$

where l^{-1} denotes the inverse of l modulo p. For $k < p$, $kl^{-1} - 1 \pmod p$ runs through all residue classes except $-1 + p\mathbb{Z}$. With $q := \frac{p-1}{2}$ and the first supplement it follows that

$$G_p^2 = -\left(\frac{-1}{p}\right)\sum_{k=1}^{p-1}\zeta^k + (p-1)\left(\frac{-1}{p}\right) = (-1)^q p =: p^*.$$

For $H_p := \prod_{k=1}^{q}(\zeta^k - \zeta^{-k})$, it holds that

$$\begin{aligned} H_p^2 &= (-1)^q \prod_{k=1}^{q}(\zeta^k - \zeta^{-k})(\zeta^{-k} - \zeta^k) = (-1)^q \prod_{k=1}^{q}(1-\zeta^{2k})(1-\zeta^{-2k}) \\ &= (-1)^q \prod_{k=1}^{p-1}(1-\zeta^k) = (-1)^q \Phi_p(1) = p^* \end{aligned}$$

(cf. proof of Theorem I.12.23). Thus there exists a sign $\epsilon = \pm 1$ with $G_p = \epsilon H_p$. Each factor $\zeta^k - \zeta^{-k}$ of H_p is purely imaginary with positive imaginary part.[2] This shows $H_p = \sqrt{p^*}$ for $q \equiv 0, 1 \pmod 4$ and $H_p = -\sqrt{p^*}$ for $q \equiv 2, 3 \pmod 4$. A case distinction with the supplements yields $H_p = \left(\frac{-2}{p}\right)\sqrt{p^*}$ in all cases. It remains to show $\epsilon = \left(\frac{-2}{p}\right)$.

Let us consider the polynomial

$$\alpha := \prod_{k=1}^{q}(X^k - X^{p-k}) - \epsilon \sum_{k=1}^{p}\left(\frac{k}{p}\right)X^k \in \mathbb{Z}[X].$$

Because of $\alpha(1) = 0 - 0 = 0$, $\alpha(\zeta) = H_p - \epsilon G_p = 0$ and $\alpha \in \mathbb{Z}[X]$, all p-th roots of unity are zeros of α. Division by the monic polynomial $X^p - 1$ yields $\beta \in \mathbb{Z}[X]$ with

$$\alpha = (X^p - 1)\beta \equiv (X-1)^p \beta \equiv 0 \pmod{(X-1)^p} \tag{A.1.1}$$

in $\mathbb{F}_p[X]$. We substitute $Y := X - 1$ and calculate using the binomial formula $X^k - X^{p-k} = (1+Y)^k - (1+Y)^{p-k} \equiv 2kY \pmod{Y^2}$ in $\mathbb{F}_p[X]$ for $k = 1, \ldots, q$. According to Euler's criterion[3] it therefore holds that

$$\prod_{k=1}^{q}(X^k - X^{p-k}) \equiv 2^q q! Y^q \equiv \left(\frac{2}{p}\right) q! \pmod{Y^{q+1}}. \tag{A.1.2}$$

For the second summand of α it holds that

$$\sum_{k=1}^{p}\left(\frac{k}{p}\right)X^k = \sum_{k=1}^{p}\left(\frac{k}{p}\right)\sum_{l=0}^{k}\binom{k}{l}Y^l \equiv \sum_{l=0}^{q}\sum_{k=1}^{p}\binom{k}{l}\left(\frac{k}{p}\right)Y^l \pmod{Y^{q+1}},$$

since $\binom{k}{l} = 0$ for $k < l$. Clearly $\binom{k}{l} = \frac{k(k-1)\ldots(k-l+1)}{l!}$ is a polynomial in k of degree $l \leq q$ with coefficients in $\mathbb{F}_p$. For $\mathbb{F}_p^\times = \langle t \rangle$ and $d \in \mathbb{N}_0$ it holds that

$$\sum_{k=1}^{p} k^d \left(\frac{k}{p}\right) \equiv \sum_{k=1}^{p} k^{d+q} \equiv \sum_{k=1}^{p}(tk)^{d+q} \equiv t^{d+q}\sum_{k=1}^{p} k^d\left(\frac{k}{p}\right) \pmod p.$$

[2] This distinguishes ζ from an arbitrary primitive root of unity.

[3] See lecture notes number theory

In the case $d < q$, $t^{d+q} \neq 1$ and one obtains $\sum_{k=1}^{p} k^d \left(\frac{k}{p}\right) \equiv 0 \pmod{p}$. For $d = q$ on the other hand,

$$\sum_{k=1}^{p} k^q \left(\frac{k}{p}\right) \equiv \sum_{k=1}^{p} k^{p-1} \equiv -1 \pmod{p}.$$

Thus there remains

$$\sum_{k=1}^{p} \left(\frac{k}{p}\right) X^k \equiv \sum_{k=1}^{p} \binom{k}{q} \left(\frac{k}{p}\right) Y^q \equiv -\frac{1}{q!} Y^q \pmod{Y^{q+1}}. \tag{A.1.3}$$

Now we combine (A.1.1), (A.1.2) and (A.1.3) to

$$\left(\left(\frac{2}{p}\right) q! + \frac{\epsilon}{q!}\right) Y^q \equiv \alpha \equiv 0 \pmod{Y^{q+1}}.$$

According to Wilson (Exercise I.9), it holds that $(q!)^2 \equiv 1 \cdot \ldots \cdot q \cdot (-q)(-q-1)\ldots(-1) \equiv (-1)^q (p-1)! \equiv -(-1)^q \equiv -\left(\frac{-1}{p}\right) \pmod{p}$. We obtain

$$\epsilon \equiv -(q!)^2 \left(\frac{2}{p}\right) \equiv \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) \equiv \left(\frac{-2}{p}\right) \pmod{p}$$

as claimed. □

A.2 Zero regions and eigenvalues

Remark A.2.1. To investigate the Galois group of a polynomial, it is useful to localize the position of the zeros in the complex plane. We prove some geometric statements of this kind and give applications for matrices.

Theorem A.2.2. *For every zero $x \in \mathbb{C}$ of $\alpha = X^n + a_1 X^{n-1} + \ldots + a_n \in \mathbb{C}[X]$, it holds that*

$$|x| < \max\{|a_i| : i = 1, \ldots, n\} + 1.$$

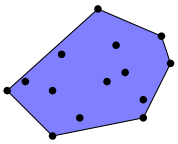
Proof. For $x \in \mathbb{C}$ with $|x| \geq r := \max\{|a_i| : i = 1, \ldots, n\} + 1$, it holds that

$$\begin{aligned} |\alpha(x)| &\geq |x|^n - |a_1||x|^{n-1} - \ldots - |a_n| \geq r|x|^{n-1} - |a_1||x|^{n-1} - \ldots - |a_n| \\ &\geq |x|^{n-1} - |a_2||x|^{n-2} - \ldots - |a_n| \geq \ldots \geq |x| - |a_n| \geq 1 \end{aligned}$$

according to the reverse triangle inequality. □

Definition A.2.3. A set $C \subseteq \mathbb{C}$ is called *convex*, if for $x, y \in C$ the connecting segment $\{x + \lambda(y - x) : \lambda \in [0, 1]\}$ also lies in C. The *convex hull* $\operatorname{conv}(S)$ of a set $S \subseteq \mathbb{C}$ is the intersection of all convex sets containing S. For $S = \{s_1, \ldots, s_n\}$, it holds that

$$\operatorname{conv}(S) = \{\lambda_1 s_1 + \ldots + \lambda_n s_n : \lambda_1, \ldots, \lambda_n \in [0, 1],\ \lambda_1 + \ldots + \lambda_n = 1\}.$$



Theorem A.2.4 (Gauss-Lucas)**.** *Let $\alpha \in \mathbb{C}[X] \setminus \mathbb{C}$. Then the zeros of α' lie in the convex hull of the zeros of α.*

Proof. Wlog. let α be monic and $\alpha = (X - x_1) \ldots (X - x_n)$. According to the product rule, it holds that

$$\frac{\alpha'}{\alpha} = \frac{1}{X - x_1} + \ldots + \frac{1}{X - x_n} \in \mathbb{C}(X).$$

Let $y \in \mathbb{C}$ be a zero of α' that does not lie in $C := \operatorname{conv}(x_1, \ldots, x_n)$. The vectors $y - x_1, \ldots, y - x_n$ then lie in a circular sector with angle $< \pi$. The same holds for the vectors $\frac{1}{y - x_i} = \frac{\overline{y - x_i}}{|y - x_i|^2}$. This yields the contradiction

$$0 = \frac{\alpha'(y)}{\alpha(y)} = \frac{1}{y - x_1} + \ldots + \frac{1}{y - x_n} \neq 0.$$

□

Corollary A.2.5. *If all zeros of $\alpha \in \mathbb{C}[X]$ are real, then all zeros of α' are also real.*

Remark A.2.6. For real polynomials, Corollary A.2.5 can be justified using the intermediate value theorem from analysis (according to Lemma I.11.8, one can assume that only simple zeros are present).

Theorem A.2.7 (SYLVESTER). *Let $\alpha \in \mathbb{R}[X]$ with roots $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ (with multiplicities). Let $\rho_k := \lambda_1^k + \ldots + \lambda_n^k$ for $k \in \mathbb{N}_0$ (cf. Example I.14.20). All λ_i are real if and only if the symmetric matrix*

$$A := (\rho_{i+j-2})_{i,j=1}^n = \begin{pmatrix} \rho_0 & \rho_1 & \cdots & \rho_{n-1} \\ \rho_1 & \rho_2 & \cdots & \rho_n \\ \vdots & \vdots & & \vdots \\ \rho_{n-1} & \rho_n & \cdots & \rho_{2n-2} \end{pmatrix} \in \mathbb{R}^{n \times n}$$

is positive semidefinite.

Proof (NATHANSON). For $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ let $\beta := \sum_{i=1}^n x_i Y^{i-1} \in \mathbb{R}[Y]$. Then

$$xAx^{\mathrm{t}} = \sum_{i,j=1}^n \rho_{i+j-2} x_i x_j = \sum_{i,j,k=1}^n \lambda_k^{i+j-2} x_i x_j = \sum_{k=1}^n \beta(\lambda_k)^2.$$

If all λ_k are real, it follows that $\beta(\lambda_k) \in \mathbb{R}$ and $xAx^{\mathrm{t}} \geq 0$, i. e. A is positive semidefinite. Now let wlog. $\lambda_1 \notin \mathbb{R}$. Because of $\alpha \in \mathbb{R}[X]$ we can assume $\lambda_2 = \overline{\lambda_1}$. Let $\lambda_1, \ldots, \lambda_s$ be pairwise distinct with $\{\lambda_1, \ldots, \lambda_n\} = \{\lambda_1, \ldots, \lambda_s\}$. By interpolation one obtains a uniquely determined polynomial $\beta = \sum_{i=1}^s x_i Y^{i-1} \in \mathbb{C}[Y]$ with

$$\beta(\lambda_1) = \mathrm{i} = -\beta(\lambda_2) = \overline{\beta(\overline{\lambda_1})}$$

and $\beta(\lambda_k) = 0$ for $k = 3, \ldots, s$. Because of

$$(\beta - \overline{\beta})(\lambda_k) = \beta(\lambda_k) - \overline{\beta(\overline{\lambda_k})} = 0$$

for $k = 1, \ldots, s$ it holds that $\beta = \overline{\beta} \in \mathbb{R}[Y]$, i. e. $x_1, \ldots, x_s \in \mathbb{R}$. Let $m \in \mathbb{N}$ be the multiplicity of the root λ_1 (resp. λ_2). For $x = (x_1, \ldots, x_s, 0, \ldots, 0)$ it then follows that

$$xAx^{\mathrm{t}} = \sum_{k=1}^n \beta(\lambda_k)^2 = m(\mathrm{i}^2 + (-\mathrm{i})^2) = -2m < 0.$$

Thus A is not positive semidefinite. □

Remark A.2.8. The equation $xAx^{\mathrm{t}} = \sum \beta(\lambda_k)^2$ in the proof shows that A is invertible (resp. positive definite) if and only if the roots are pairwise distinct (and real).

Theorem A.2.9 (DESCARTES' Rule of Signs). *Let $\alpha = X^n + a_1 X^{n-1} + \ldots + a_n \in \mathbb{R}[X]$ with only real roots. These roots are positive if and only if the coefficients $a_1, \ldots, a_n$ are alternating, i. e. $a_i(-1)^i > 0$ for $i = 1, \ldots, n$.*

Proof. Let $a_i(-1)^i > 0$ for $i = 1, \ldots, n$. For $x < 0$ it then holds that

$$\alpha(x) = (-1)^n \big(|x|^n + |a_1||x|^{n-1} + \ldots + |a_n|\big) \neq 0.$$

Conversely, let $x_1, \ldots, x_n > 0$ be the roots of α. According to Vieta

$$a_k(-1)^k = \sigma_k(x_1, \ldots, x_n) > 0.$$ □

Corollary A.2.10. *A symmetric matrix $A \in \mathbb{R}^{n \times n}$ with characteristic polynomial $\chi_A = X^n + a_1 X^{n-1} + \ldots + a_n$ is positive definite if and only if $a_i(-1)^i > 0$ for $i = 1, \ldots, n$ holds.*

Proof. As a symmetric matrix, A has only real eigenvalues. It is well known that A is positive definite if and only if all eigenvalues are positive. □

Theorem A.2.11 (Sturm). *Let $\alpha = \alpha_0 \in \mathbb{R}[X] \setminus \mathbb{R}$, $\alpha_1 := \alpha_0'$ and*

$$\alpha_{k-1} = \alpha_k \beta_k - \alpha_{k+1} \qquad (\textit{Euclidean division})$$

for $k = 1, \ldots, n+1$ with $\beta_k \in \mathbb{R}[X]$, $\deg \alpha_{k+1} < \deg \alpha_k$ and $\alpha_n \neq 0 \neq \alpha_{n+1}$. For $x \in \mathbb{R}$, let $v(x)$ be the number of sign changes in the sequence $\alpha_0(x), \ldots, \alpha_n(x)$ without considering zeros. For $a < b$ with $\alpha(a)\alpha(b) \neq 0$, then $v(a) - v(b)$ is the number of distinct real zeros of α in the interval $[a, b]$.

Proof. According to the Euclidean algorithm, α_n is, up to normalization, the gcd of α_0 and α_1. By assumption, $\alpha_n(a)\alpha_n(b) \neq 0$. One can therefore work with the sequence $\widetilde{\alpha}_k := \alpha_k/\alpha_n$ without changing $v(a)$ or $v(b)$. We mentally let x run from a to b and observe how $v(x)$ changes in the process. As long as none of the $\widetilde{\alpha}_k$ vanish at x, the sign changes do not change. Now let $x \in \mathbb{R}$ be a zero of α_0 with multiplicity m. By construction, $\widetilde{\alpha}_k(x) \neq 0$ for $k \geq 1$. Furthermore, there exists $\gamma \in \mathbb{R}[X]$ with $\alpha_0 = (X - x)^m \gamma$ and $\gamma(x) \neq 0$. Because of $\alpha_1 = \alpha_0' = m(X - x)^{m-1}\gamma + (X - x)^m \gamma'$, there exist $\sigma, \tau \in \mathbb{R}[X]$ with

$$\widetilde{\alpha}_0 = (X - x)\sigma, \qquad \widetilde{\alpha}_1 = m\sigma + (X - x)\tau, \qquad \sigma(x) \neq 0.$$

For $y = x - \epsilon$ with $\epsilon > 0$, it then holds that

$$\widetilde{\alpha}_0(y)\widetilde{\alpha}_1(y) = -\epsilon\sigma(y)(m\sigma(y) - \epsilon\tau(y)) = -\epsilon m\sigma(y)^2 + \epsilon^2\sigma(y)\tau(y).$$

Because of $\lim_{\epsilon \to 0} \sigma(y)^2 = \sigma(x)^2 > 0$ and $\lim_{\epsilon \to 0} \epsilon\sigma(y)\tau(y) = 0$, one can choose ϵ so small that $\widetilde{\alpha}_0(y)\widetilde{\alpha}_1(y) < 0$ holds. Analogously, $\widetilde{\alpha}_0(y)\widetilde{\alpha}_1(y) > 0$ for $y = x + \epsilon$ with ϵ small enough. The number of sign changes in the sequence $\widetilde{\alpha}_k(x)$ therefore reduces by 1.

Now let $\widetilde{\alpha}_k(x)$ with $k \geq 1$. Because of $\widetilde{\alpha}_n = 1$, it follows that $k < n$. By construction, $\widetilde{\alpha}_{k-1}$, $\widetilde{\alpha}_k$ and $\widetilde{\alpha}_{k+1}$ are pairwise coprime and

$$\widetilde{\alpha}_{k-1} = \widetilde{\alpha}_k \beta_k - \widetilde{\alpha}_{k+1}.$$

From this it follows that $\widetilde{\alpha}_{k-1}(x) = -\widetilde{\alpha}_{k+1}(x) \neq 0$. Thus, both to the left and to the right of x, there is exactly one sign change in the sequence $(\widetilde{\alpha}_{k-1}(x), \widetilde{\alpha}_k(x), \widetilde{\alpha}_{k+1}(x))$. Consequently, $v(x)$ remains unchanged at this point. □

Example A.2.12. One can combine Theorems A.2.2 and A.2.11 to determine all real roots of a real polynomial. We consider $\alpha = X^3 - X^2 + 1$. According to Theorem A.2.2, all roots lie in the unit disk with radius 2. In particular, the real roots lie in the interval $[-2, 2]$. Using the Euclidean algorithm, we calculate the sequence from Sturm's Theorem:

$$\alpha_0 = X^3 - X^2 + 1, \qquad \alpha_1 = 3X^2 - 2X, \qquad \alpha_2 = \alpha_1\Big(\frac{1}{3}X - \frac{1}{9}\Big) - \alpha_0 = -\frac{7}{9}.$$

It follows that $(\alpha_0(-2), \alpha_1(-2), \alpha_2(-2)) = (-11, 16, -\frac{7}{9})$ and $(\alpha_0(2), \alpha_1(2), \alpha_2(2)) = (5, 8, -\frac{7}{9})$. Therefore, α has exactly $v(-2) - v(2) = 2 - 1 = 1$ real root.

Theorem A.2.13 (Murty). *Let $\alpha = X^n + a_1 X^{n-1} + \ldots + a_n \in \mathbb{Z}[X]$ and $\alpha(k) \in \mathbb{P}$ for a natural number $k \geq \max\{|a_i| : i = 1, \ldots, n\} + 2$. Then α is irreducible in $\mathbb{Q}[X]$.*

Proof. Let $m := \max\{|a_i| : i = 1, \ldots, n\}$. For every root $x \in \mathbb{C}$ of α, it holds that $|x| < m+1$ according to Theorem A.2.2. By Gauss's Lemma, we can assume $\alpha = \beta\gamma$ with monic $\beta, \gamma \in \mathbb{Z}[X] \setminus \mathbb{Z}$. Because of $\beta(k)\gamma(k) = \alpha(k) \in \mathbb{P}$, we may assume $\beta(k) = \pm 1$. According to the Fundamental Theorem of Algebra, $\beta = (X - x_1) \ldots (X - x_s)$ for certain roots $x_1, \ldots, x_s \in \mathbb{C}$ of α. The above estimate now yields the contradiction

$$|\beta(k)| = \prod_{i=1}^{s} |k - x_i| \geq \prod_{i=1}^{s} (k - |x_i|) > \prod_{i=1}^{s} (k - (m+1)) \geq 1. \qquad \square$$

Theorem A.2.14 (Gershgorin)**.** *For every eigenvalue $\lambda \in \mathbb{C}$ of $(a_{ij}) \in \mathbb{C}^{n \times n}$, there exists an $i \in \{1, \ldots, n\}$ with $|\lambda - a_{ii}| \leq \sum_{j \neq i} |a_{ij}|$.*

Proof. Let $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$ be an eigenvector for the eigenvalue λ. Let $|x_i| = \max\{|x_j| : j = 1, \ldots, n\} > 0$. After normalization, we can assume $x_i = 1$ and $|x_j| \leq 1$ for $j \neq i$. By the triangle inequality, it then holds that

$$|\lambda - a_{ii}| = |\lambda x_i - a_{ii} x_i| = \Big|\sum_{j=1}^{n} a_{ij} x_j - a_{ii} x_i\Big| = \Big|\sum_{j \neq i} a_{ij} x_j\Big| \leq \sum_{j \neq i} |a_{ij}|. \qquad \square$$

Remark A.2.15.

(i) Since A^{t} has the same eigenvalues as A, one can also apply Theorem A.2.14 to the columns of A.

(ii) Applying Theorem A.2.14 to the companion matrix of $\alpha = X^n + a_1 X^{n-1} + \ldots + a_n \in \mathbb{C}[X]$, one obtains

$$|x| \leq \max\big\{|a_n|, |a_{n-1}| + 1, \ldots, |a_1| + 1\big\}$$

for every root $x \in \mathbb{C}$ of α (note $|x + a_1| \leq 1 \Rightarrow |x| \leq |a_1| + 1$). This improves Theorem A.2.2.

A.3 Cyclotomic Polynomials

Remark A.3.1. In this section, we give four applications of cyclotomic polynomials: special cases of Dirichlet's prime number theorem, integral bases of $\mathbb{Q}_n$, the Peirce decomposition of $\mathbb{F}_q C_n$, and the existence of so-called Zsigmondy primes.

Definition A.3.2. A *prime divisor* of $\alpha \in \mathbb{Z}[X]$ is a prime number p that divides $\alpha(n)$ for some $n \in \mathbb{Z}$. Let the set of prime divisors of α be $\Pi(\alpha)$.

Theorem A.3.3. *For $\alpha \in \mathbb{Z}[X] \setminus \mathbb{Z}$, the following hold:*

(i) For infinitely many $n \in \mathbb{N}$, $\alpha(n)$ is not a prime number.

(ii) α possesses infinitely many prime divisors.

Proof.

(i) Wlog. let the leading coefficient of α be positive (otherwise replace α by $-\alpha$). Because of $\alpha \notin \mathbb{Z}$, we have $\lim_{x\to\infty} \alpha(x) = \infty$. Let p be a prime divisor of $\alpha(n)$. For $k \in \mathbb{N}$, we have $\alpha(n+pk) \equiv \alpha(n) \equiv 0 \pmod{p}$. Therefore, infinitely many values of the form $\alpha(n + pk)$ are not prime numbers.

(ii) Let $\alpha = a_d X^d + \ldots + a_0$. In the case $a_0 = 0$, $p \mid \alpha(p)$ for every prime number p. So let $a_0 \neq 0$. Because of $\alpha(a_0 X) = a_0(a_0^{d-1} a_d X^{d-1} + \ldots + 1)$, we may assume $a_0 = 1$. Because of $d \geq 1$, α has at least one prime divisor. Suppose $p_1, \ldots, p_s$ are the only prime divisors of α. Then there exists $\beta \in \mathbb{Z}[X] \setminus \mathbb{Z}$ with $\alpha(p_1 \ldots p_s X) = p_1 \ldots p_s \beta(X) + 1$. Obviously, there exists $n \in \mathbb{N}$ with $p_1 \ldots p_s \beta(n) + 1 \neq \pm 1$. Every prime divisor of this number would be a new prime divisor of α. □

Remark A.3.4. In Lemma I.12.15, we have seen that almost all prime divisors of Φ_n are congruent to 1 modulo n. With Theorem A.3.3, Theorem I.12.17 now follows. The next theorems generalize this principle.

Theorem A.3.5. *For $n \geq 1$, there exist infinitely many prime numbers $p \equiv 1 + 2^{n-1} \pmod{2^n}$.*

Proof. Wlog. let $n \geq 2$. According to Lemma I.12.15, all odd prime divisors of

$$\alpha := \Phi_{2^{n-1}} \overset{\text{I.12.10}}{=} X^{2^{n-2}} + 1$$

are congruent to 1 modulo 2^{n-1}. Suppose α possesses only finitely many prime divisors $p \equiv 1 + 2^{n-1} \pmod{2^n}$. Let q be their product ($q = 1$ allowed). According to the Chinese Remainder Theorem, there exists an $m \in \mathbb{N}$ with $m \equiv 0 \pmod{q}$ and $m \equiv 5 \pmod{2^{n+1}}$. Because of $\alpha(m) \equiv \alpha(0) \equiv 1 \pmod{q}$, all odd prime divisors of $\alpha(m)$ are congruent to 1 modulo 2^n. On the other hand,

$$\alpha(m) \equiv \alpha(5) = 5^{2^{n-2}} + 1 = (1+4)^{2^{n-2}} + 1 \equiv 2 + 2^n \pmod{2^{n+1}}.$$

But then $\frac{1}{2}\alpha(m) \equiv 1 + 2^{n-1} \pmod{2^n}$ would be the product of prime numbers $p \equiv 1 \pmod{2^n}$. □

Theorem A.3.6 (SCHUR)**.** *Let $a, n \in \mathbb{N}$ with $a^2 \equiv 1 \pmod{n}$. If there exists a prime $p \geq \frac{1}{2}\varphi(n)$ with $p \equiv a \pmod{n}$, then there are infinitely many such primes.*

Proof. Wlog. let $n \geq 3$ and $k := \varphi(n)/2$. According to Theorem I.12.17 we can assume $a \not\equiv 1 \pmod{n}$. Let $\zeta \in \mathbb{C}$ be a primitive n-th root of unity and $\sigma \in G := \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ with $\sigma(\zeta) = \zeta^a$. By assumption $\sigma^2 = 1$. For $\tau \in G \setminus \langle\sigma\rangle$ the polynomials $(X-\zeta)(X-\zeta^a)$ and $(X-\tau(\zeta))(X-\tau(\zeta)^a)$ can coincide at at most finitely many points. Therefore there exists a $z \in \mathbb{Z}$ ("large enough"), such that $\eta := (z-\zeta)(z-\zeta^a)$ is a primitive element of $\mathbb{Q}_n^\sigma$. Let $1 = \tau_1, \ldots, \tau_k \in G$ be a system of representatives for the cosets of $\langle\sigma\rangle$ in G. Then

$$\alpha := (-1)^k \prod_{i=1}^{k} (X - \tau_i(\eta)) \in \mathbb{Q}_n^G[X] = \mathbb{Q}[X].$$

Since ζ and η are algebraic integers, it even holds that $\alpha \in \mathbb{Z}[X]$. Let $D := \prod_{i<j}(\tau_j(\eta) - \tau_i(\eta))^2 \in \mathbb{Z}$ be the discriminant of α.

Step 1: For $p \in \Pi(\alpha)$ it holds that $p \mid n$, $p \mid D$ or $p \equiv a^i \pmod{n}$ with $i \in \{0,1\}$.
Let $m \in \mathbb{N}$ and p be a prime divisor of $\alpha(m)$ with $p \nmid n$ and $p \nmid D$. Let R be the ring of integers of $\mathbb{Q}_n$. Because $1/p \notin R$ there exists a maximal ideal $P \trianglelefteq R$ with $p \in P$ (Theorem II.2.7). Then $K := R/P$ is a field of characteristic p and $P \cap \mathbb{Z} = p\mathbb{Z}$. In K it holds that $(m - \tau_1(\eta)) \ldots (m - \tau_k(\eta)) = 0$. Let therefore $m \equiv \tau_l(\eta) \pmod{P}$ for some $1 \leq l \leq k$. Because $p \nmid n$, ζ^p is also a primitive n-th root of unity. Therefore there exists $1 \leq j \leq k$ with $(z - \tau_l(\zeta^p))(z - \tau_l(\zeta^p)^a) = \tau_j(\eta)$. With the Frobenius homomorphism and Fermat-Euler one obtains

$$\tau_j(\eta) \equiv \big(z^p - \tau_l(\zeta)^p\big)\big(z^p - \tau_l(\zeta^a)^p\big) \equiv \tau_l(\eta)^p \equiv m^p \equiv m \equiv \tau_l(\eta) \pmod{P}.$$

In the case $j \neq l$, $\tau_j(\eta) - \tau_l(\eta)$ is a factor of D and one obtains $D \in P \cap \mathbb{Z} = p\mathbb{Z}$. But then $p \mid D$. Thus $j = l$ and $(z - \zeta^p)(z - \zeta^{ap}) = \eta$. This shows $p \equiv a^i \pmod{n}$ for $i \in \{0,1\}$.

Step 2: Every prime $p \equiv a^i \pmod{n}$ is a prime divisor of α.
As in Step 1 it holds that

$$\eta^p \equiv (z - \zeta^p)(z - \zeta^{ap}) \equiv (z - \zeta^{a^i})(z - \zeta^{a^{i+1}}) \equiv \eta \pmod{P}.$$

Therefore η is a root of $X^p - X$ in K. On the other hand $X^p - X$ has only the p roots in the prime field $\mathbb{F}_p \subseteq K$. Thus there exists $m \in \mathbb{Z}$ with $\eta \equiv m \pmod{P}$. It follows $\alpha(m) \in P \cap \mathbb{Z} = p\mathbb{Z}$.

Step 3: There exist $m \in \mathbb{N}$, $p \in \mathbb{P}$ with $p \equiv a \pmod{n}$, $p \mid \alpha(m)$ and $p^2 \nmid \alpha(m)$.
By assumption there exists a prime $p \equiv a \pmod{n}$ with $p > k$. According to Step 2 there exists $m \in \mathbb{N}$ with $p \mid \alpha(m)$. We assume $p^2 \mid \alpha(m)$. Write $\alpha = \sum a_i X^i$. Then it holds that

$$\alpha(m+p) = \sum a_i (m+p)^i \equiv \sum a_i (m^i + i m^{i-1} p) \equiv \alpha(m) + p\alpha'(m) \equiv p\alpha'(m) \pmod{p^2}.$$

In the case $p \nmid \alpha'(m)$ we can replace m by $m + p$ and are done. So let $p \mid \alpha'(m)$. According to Lemma I.11.8 m is a multiple root of α in K. Therefore there exist $1 \leq s < t \leq k$ with $\tau_s(\eta) \equiv \tau_t(\eta) \pmod{P}$. By replacing P with $\tau_t^{-1}(P) \trianglelefteq R$, we can assume $t = 1$. This means

$$z\big(\tau_s(\zeta) + \tau_s(\zeta)^a - \zeta - \zeta^a\big) \equiv \tau_s(\zeta)^{1+a} - \zeta^{1+a} \pmod{P}.$$

Let us assume $\tau_s(\zeta) + \tau_s(\zeta)^a \equiv \zeta + \zeta^a \pmod{P}$. Then it follows $\tau_s(\zeta)^{1+a} \equiv \zeta^{1+a} \pmod{P}$ and

$$\tau_s((X-\zeta)(X-\zeta^a)) \equiv (X-\zeta)(X-\zeta^a) \pmod{P}.$$

This shows $\tau_s(\zeta) \equiv \zeta^{a^i} \pmod{P}$ for some $i \in \{0,1\}$. Because $\tau_s \notin \langle\sigma\rangle$, on the other hand $\tau_s(\zeta) \neq \zeta^{a^i}$. Consequently $X^n - 1$ also has a multiple root in K. On the other hand $(X^n - 1)' = nX^{n-1}$ is coprime

to $X^n - 1$ (note $p \nmid n$). This contradiction shows $\tau_s(\zeta) + \tau_s(\zeta)^a \not\equiv \zeta + \zeta^a \pmod{P}$. Thus z modulo P and also modulo p is uniquely determined by l. For l there are at most $k-1$ possibilities. Because $p > k-1$ there exists a residue class $r + p\mathbb{Z}$, such that for $z \in r + p\mathbb{Z}$ it always holds that $p^2 \nmid \alpha(m)$ or $p^2 \nmid \alpha(m+p)$.

Step 4: Every prime divisor of $\alpha(0)$ is congruent to 1 modulo n.
With the Chinese Remainder Theorem we can achieve that z is divisible by n without leaving the residue class $r + p\mathbb{Z}$. By definition of α it holds that $\alpha(0) = \Phi_n(z)$. Because $n \geq 3$ the primitive n-th roots of unity occur in pairs of the form ζ^i, ζ^{-i}. Therefore Φ_n has constant term 1 and it follows $\Phi_n(z) = \Phi_n(0) \equiv 1 \pmod{n}$. According to Lemma I.12.15 every prime divisor of $\alpha(0)$ is now congruent to 1 modulo n.

Step 5: Contradiction.
Let m and p be as in Step 3. Assume there are only finitely many primes in $a + n\mathbb{Z}$. Then there are also only finitely many prime divisors of α that do not lie in $1 + n\mathbb{Z}$ (Step 1). Let q be the product of these prime divisors excluding p. By the Chinese Remainder Theorem there exists $c \in \mathbb{Z}$ with $c \equiv m \pmod{p^2}$ and $c \equiv 0 \pmod{nq}$. It follows $\alpha(c) \equiv \alpha(m) \pmod{p^2}$ and $\alpha(c) \equiv \alpha(0) \pmod{nq}$. Thus p is a prime divisor of $\alpha(c)$ with multiplicity 1. All other prime divisors of $\alpha(c)$ lie in $1 + n\mathbb{Z}$, because $\alpha(0)$ has only such prime divisors (Step 4). This yields the contradiction $a \equiv p \equiv \alpha(c) \equiv \alpha(0) \equiv 1 \pmod{n}$. □

Corollary A.3.7. *In every prime residue class modulo* 24 *there are infinitely many prime numbers.*

Proof. For $a + 24\mathbb{Z} \in (\mathbb{Z}/24\mathbb{Z})^\times \cong C_2^3$ it holds that $a^2 \equiv 1 \pmod{24}$. According to Theorem I.12.17 we can assume $a \not\equiv 1 \pmod{24}$. According to Theorem A.3.6 it suffices to provide one prime number $p \geq \frac{1}{2}\varphi(24) = 4$ from each such residue class. In fact, the smallest representatives $a \in \{5, 7, 11, 13, 17, 19, 23\}$ are already prime numbers. □

Remark A.3.8. Because of $11 + 24\mathbb{Z} \subseteq 3 + 8\mathbb{Z}$, $5 + 24\mathbb{Z} \subseteq 5 + 8\mathbb{Z}$ and $7 + 24\mathbb{Z} \subseteq 7 + 8\mathbb{Z}$, every prime residue class modulo 8 also contains infinitely many prime numbers.

Theorem A.3.9 (Bauer)**.** *For every $n \in \mathbb{N}$ there exist infinitely many prime numbers $p \equiv -1 \pmod{n}$.*

Proof. Wlog. let $n \geq 3$ and $k := \varphi(n)/2$. We argue as in the proof of Theorem A.3.6 with $a = -1$. Then $\eta = (z - \zeta)(z - \bar{\zeta}) \in \mathbb{R}$ is a simple root of $\alpha \in \mathbb{Z}[X]$. Consequently, α must change sign at η. Thus there exist $x, y \in \mathbb{Z}$ with $\alpha(x/y) < 0$ and $y > 0$. We define $\beta := y^k \alpha(X/y) \in \mathbb{Z}[X]$. Like α, β is also monic. Furthermore, $\beta(x) < 0$. Finally, let

$$\gamma := -\frac{1}{\beta(x)} \beta(x - \beta(x)X).$$

The constant term of γ is $\gamma(0) = -1$. In all other coefficients $\beta(x)$ can be canceled, so that $\gamma \in \mathbb{Z}[X]$ follows. The leading coefficient is $(-\beta(x))^{k-1} > 0$. In particular, $\gamma(m) > 1$ for m "large enough". Assume that γ has only finitely many prime divisors $p \not\equiv 1 \pmod{n}$. Let q be their product ($q = 1$ allowed). Every prime divisor p of $\gamma(mnq) > 0$ then satisfies $p \equiv 1 \pmod{n}$, because $\gamma(mnq) \equiv \gamma(0) \equiv -1 \pmod{q}$. On the other hand, however, $\gamma(mnq) \equiv -1 \pmod{n}$. This contradiction shows that γ has infinitely many prime divisors $p \not\equiv 1 \pmod{n}$. Because of $\gamma(m) \mid \beta(x - \beta(x)m)$, we have $\Pi(\gamma) \subseteq \Pi(\beta)$.

Now let p be a prime divisor of $\beta(m)$ with $p \nmid y$. Then there exists an $m' \in \mathbb{N}$ with $ym' \equiv m \pmod{p}$. It follows

$$y^k \alpha(m') = \beta(ym') \equiv \beta(m) \equiv 0 \pmod{p}.$$

This implies $p \mid \alpha(m')$. Thus α also has infinitely many prime divisors $p \not\equiv 1 \pmod{n}$. From step 1 in the proof of Theorem A.3.6 we know on the other hand that almost all (up to finitely many) prime divisors of α satisfy the congruence $p \equiv \pm 1 \pmod{n}$. There must therefore be infinitely many prime divisors $p \equiv -1 \pmod{n}$. □

Definition A.3.10. Let $K \subseteq L$ be a Galois extension with $\mathrm{Gal}(L|K) = \{\sigma_1, \ldots, \sigma_n\}$. Let $x_1, \ldots, x_n$ be a K-basis of L and $M := (\sigma_i(x_j))_{1 \le i,j \le n}$. The *discriminant* of $x_1, \ldots, x_n$ with respect to K is

$$D(x_1, \ldots, x_n) := \det(M)^2.$$

Remark A.3.11.

(i) Due to the squaring, $D := D(x_1, \ldots, x_n)$ depends neither on the order of the x_i nor on the order of the σ_i. In particular, $\sigma_i(D) = D$ for $i = 1, \ldots, n$ and it follows that $D \in L^{\mathrm{Gal}(L|K)} = K$.

(ii) For all $\lambda = (\lambda_1, \ldots, \lambda_n) \in K^n \setminus \{0\}$, it holds that $M\lambda = (\sigma_i(\lambda_1 x_1 + \ldots + \lambda_n x_n))_i \neq 0$. Therefore M is invertible and $D(x_1, \ldots, x_n) \neq 0$.

(iii) If $K = \mathbb{Q}$ and $x_1, \ldots, x_n$ is an integral basis of L, then D is algebraic-integral, thus $D \in \mathbb{Z}$. If $y_1, \ldots, y_n$ is another integral basis of L, then there exists an $S = (s_{ij}) \in \mathrm{GL}(n, \mathbb{Z})$ with $Sx = y$. With $M := (\sigma_i(x_j))_{i,j}$ it follows that

$$\begin{aligned} D(y_1, \ldots, y_n) &= \det\big((\sigma_i(y_j))_{i,j}\big)^2 = \det\Big(\Big(\sum_{k=1}^{n} s_{jk}\sigma_i(x_k)\Big)_{i,j}\Big)^2 \\ &= \det(MS^{\mathrm{t}})^2 = \det(M)^2 \det(S)^2 = D(x_1, \ldots, x_n). \end{aligned}$$

The discriminant is therefore an invariant of the ring of integers $\mathbb{Z}_L$.

Example A.3.12. According to the primitive element theorem, every Galois extension $K \subseteq L$ has a basis of the form $1, x, \ldots, x^{n-1}$. Now $(\sigma_i(x^{j-1}))_{1 \le i,j \le n}$ is a Vandermonde matrix with determinant $\prod_{i<j}(\sigma_j(x) - \sigma_i(x))$. Therefore $D(1, x, \ldots, x^{n-1}) = D_\mu$ is the discriminant of the minimal polynomial μ of x. The next theorem is therefore related to Exercise I.69.

Theorem A.3.13 (Stickelberger)**.** *For every integral basis $x_1, \ldots, x_n$ of a number field, $D(x_1, \ldots, x_n)$ is congruent to 0 or 1 modulo 4.*

Proof. Let K be the said number field and $\mathrm{Gal}(K|\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$ as well as $M = (\sigma_i(x_j))_{i,j}$. For a permutation $\tau \in S_n$ let $s_\tau := \sigma_1(x_{\tau(1)}) \ldots \sigma_n(x_{\tau(n)}) \in K$. Let $S_+ := \sum_{\tau \in A_n} s_\tau$ and $S_- := \sum_{\tau \in S_n \setminus A_n} s_\tau$. According to the Leibniz formula, $\det M = S_+ - S_-$ and

$$D(x_1, \ldots, x_n) = \det(M)^2 = (S_+ - S_-)^2 = (S_+ + S_-)^2 - 4S_+S_- \in \mathbb{Z}.$$

Since each σ_i permutes the s_τ, it holds that $S_+ + S_- \in \mathbb{Z}$. Therefore $S_+S_- \in \mathbb{Q} \cap \mathbb{Z}_K = \mathbb{Z}$ and it follows that $D(x_1, \ldots, x_n) \equiv (S_+ + S_-)^2 \equiv 0, 1 \pmod{4}$. □

Lemma A.3.14. *Let $p \in \mathbb{P}$, $n \in \mathbb{N}$ and ζ be a primitive p^n-th root of unity. Let $k := \varphi(p^n)$. Then*

$$D(1, \zeta, \ldots, \zeta^{k-1}) = (-1)^{\binom{k}{2}} p^{p^{n-1}(np-n-1)}.$$

Proof. Let $m := p^n$ and $G := \mathrm{Gal}(\mathbb{Q}_m|\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_k\}$. As is well known, $1, \zeta, \ldots, \zeta^{k-1}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta) = \mathbb{Q}_m$. According to Example A.3.12, $D := D(1, \zeta, \ldots, \zeta^{k-1}) = D_{\Phi_m}$. With the norm map $N\colon \mathbb{Q}_m \to \mathbb{Q}$, $x \mapsto \prod_{l=1}^{k} \sigma_l(x)$, it follows that

$$D = (-1)^{\binom{k}{2}} \prod_{l=1}^{k} \sigma_l(\Phi'_m(\zeta)) = (-1)^{\binom{k}{2}} N(\Phi'_m(\zeta))$$

from Lemma I.14.22. According to Example I.12.10, $(1 - X^{p^{n-1}})\Phi_m = 1 - X^m$. Differentiating and substituting ζ yields

$$(1 - \gamma)\Phi'_m(\zeta) = -m\zeta^{m-1} = -m\zeta^{-1}$$

with the primitive p-th root of unity $\gamma := \zeta^{p^{n-1}}$. Now $N(-\zeta^{-1}) = N(-\zeta)^{-1} = \Phi_m(0) = 1$ and $N(1 - \gamma) = \Phi_p(1)^{p^{n-1}} = p^{p^{n-1}}$, since the restriction $G \to \mathrm{Gal}(\mathbb{Q}_p|\mathbb{Q})$ is surjective. Because $N(xy) = N(x)N(y)$ for $x, y \in \mathbb{Q}_m$, we obtain overall

$$\begin{aligned} D &= (-1)^{\binom{k}{2}} N\Big(\frac{-m\zeta^{-1}}{1-\gamma}\Big) = (-1)^{\binom{k}{2}} m^k p^{-p^{n-1}} \\ &= (-1)^{\binom{k}{2}} p^{np^{n-1}(p-1)-p^{n-1}} = (-1)^{\binom{k}{2}} p^{p^{n-1}(np-n-1)}. \end{aligned}$$

□

Remark A.3.15. In the situation of Lemma A.3.14, $k = p^{n-1}(p-1) \equiv 0 \pmod 2$ holds except in the case $p^n = 2$. This shows

$$\begin{aligned} (-1)^{\binom{k}{2}} = (-1)^{\frac{k^2-k}{2}} = -1 &\iff k^2 - k \equiv 2 \pmod 4 \iff k \equiv 2 \pmod 4 \\ &\iff p \equiv 3 \pmod 4,\ n \equiv 1 \pmod 2. \end{aligned}$$

Lemma A.3.16. *Let $\mathbb{Q} \subseteq K$ and $\mathbb{Q} \subseteq L$ be Galois extensions with $K \cap L = \mathbb{Q}$. Let $x_1, \ldots, x_n \in K$ and $y_1, \ldots, y_m \in L$ be integral bases of K and L respectively with coprime discriminants D_K and D_L. Then $\{x_i y_j : i = 1, \ldots, n,\ j = 1, \ldots, m\}$ is an integral basis of KL with discriminant $D_K^m D_L^n$.*

Proof. According to Theorem I.10.15, $\mathbb{Q} \subseteq KL$ is a Galois extension with

$$G := \mathrm{Gal}(KL|\mathbb{Q}) = \mathrm{Gal}(KL|L) \times \mathrm{Gal}(KL|K) \cong \mathrm{Gal}(K|\mathbb{Q}) \times \mathrm{Gal}(L|\mathbb{Q}).$$

With $\mathrm{Gal}(KL|L) = \{\sigma_1, \ldots, \sigma_n\}$ and $\mathrm{Gal}(KL|K) = \{\tau_1, \ldots, \tau_m\}$, it holds that $G = \{\sigma_i\tau_j : 1 \le i \le n, 1 \le j \le m\}$. According to the proof of the degree theorem, $B := \{x_i y_j : 1 \le i \le n, 1 \le j \le m\}$ is also a basis of KL. For $M_K := (\sigma_i(x_j))_{i,j}$ and $M_L := (\tau_i(y_j))_{i,j}$, the Kronecker product $M_K \otimes M_L$ is the matrix for the discriminant of B. According to Exercise II.72, it holds that

$$\det(M_K \otimes M_L)^2 = \det(M_K)^{2m} \det(M_L)^{2n} = D_K^m D_L^n.$$

It remains to show that B is an integral basis. Certainly B lies in the ring of integers $\mathbb{Z}_{KL}$. Conversely, let $\alpha = \sum a_{ij} x_i y_j \in \mathbb{Z}_{KL}$ with $a_{ij} \in \mathbb{Q}$ for all i, j. We must show $a_{ij} \in \mathbb{Z}$. For $j = 1, \ldots, m$ let $\beta_j := \sum_i a_{ij} x_i \in K$. Then

$$M_L(\beta_j)_j = \Big(\sum_{j=1}^{m} \tau_i(y_j)\beta_j\Big)_i = \Big(\tau_i\Big(\sum_{j=1}^{m} \beta_j y_j\Big)\Big)_i = (\tau_1(\alpha), \ldots, \tau_m(\alpha)) \in \mathbb{Z}_{KL}^m.$$

For the adjugate matrix $\widetilde{M_L} \in \mathbb{Z}_{KL}^{m \times m}$ to M_L, it holds that $\widetilde{M_L} M_L = \det(M_L) 1_m$ and $\det(M_L)\beta_i \in \mathbb{Z}_{KL}$. Because of $\det(M_L)^2 = D_L$, it also holds that $D_L \beta_i \in \mathbb{Z}_{KL} \cap K = \mathbb{Z}_K = \mathbb{Z}[x_1, \ldots, x_n]$ for $i = 1, \ldots, n$. This shows $D_L a_{ij} \in \mathbb{Z}$ for all i, j. Analogously, $D_K a_{ij} \in \mathbb{Z}$ holds. From $\gcd(D_K, D_L) = 1$, one obtains $a_{ij} \in \mathbb{Z}$ as desired. □

Theorem A.3.17. *Let $n \in \mathbb{N}$ and $\zeta \in \mathbb{C}$ be a primitive n-th root of unity. Then $1, \zeta, \dots, \zeta^{\varphi(n)-1}$ is an integral basis of $\mathbb{Q}_n$.*

Proof. Let $R := \mathbb{Z}_{\mathbb{Q}_n}$ and $k := \varphi(n)$.

Case 1: $n = p^s$ with $p \in \mathbb{P}$.
Certainly $\mathbb{Z}[\zeta] \subseteq R$. Conversely, let $a := \sum_{i=0}^{k-1} a_i \zeta^i \in R$ with $a_i \in \mathbb{Q}$. Let $\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) = \{\sigma_1, \dots, \sigma_k\}$ and $S\colon \mathbb{Q}_n \to \mathbb{Q}$, $x \mapsto \sum_{i=1}^{k} \sigma_i(x)$ be the trace map (Example II.3.20). For $M := (\sigma_i(\zeta^{j-1}))_{1 \le i,j \le k}$, it holds that

$$T := M^{\mathrm{t}} M = \Big(\sum_{l=1}^{k} \sigma_l(\zeta^{i-1}) \sigma_l(\zeta^{j-1}) \Big)_{i,j} = \big(S(\zeta^{i+j-2}) \big)_{i,j}$$

and

$$T(a_i)_i = \Big(\sum_{l=0}^{k-1} S(\zeta^{i+l-1}) a_l \Big)_i = (S(\zeta^{i-1} a))_i \in \mathbb{Q}^k \cap R^k = \mathbb{Z}^k.$$

By multiplication with the complementary matrix, one obtains $\det(T) a_i \in \mathbb{Z}$ for $i = 0, \dots, k-1$ as in the proof of Lemma A.3.16. On the other hand, $\det T = \det(M)^2 = D(1, \zeta, \dots, \zeta^{k-1})$ is, up to sign, a p-power according to Lemma A.3.14. It therefore suffices to prove $pR \cap \mathbb{Z}[\zeta] \subseteq p\mathbb{Z}[\zeta]$.

For $i \in \mathbb{Z}$ with $p \nmid i$, let $\epsilon_i := \frac{1-\zeta^i}{1-\zeta} = \sum_{j=0}^{i-1} \zeta^j \in R$. Then

$$p \overset{\text{I.12.10}}{=} \Phi_n(1) = \prod_{\substack{1 \le i \le n \\ p \nmid i}} (1 - \zeta^i) = (1-\zeta)^k \prod_{\substack{1 \le i \le n \\ p \nmid i}} \epsilon_i.$$

For $j \in \mathbb{N}$ with $ij \equiv 1 \pmod{n}$, we have

$$\epsilon_i^{-1} = \frac{1-\zeta^{ij}}{1-\zeta^i} = \sum_{l=0}^{j-1} \zeta^{il} \in R.$$

This shows $\epsilon := \prod \epsilon_i \in R^\times$ and $p = \epsilon \lambda^k$ with $\lambda := 1 - \zeta$. Obviously $\mathbb{Z}[\lambda] \subseteq \mathbb{Z}[\zeta]$ and one shows inductively that $\mathbb{Z}[\zeta] \subseteq \mathbb{Z}[\lambda]$ (for example, $\zeta^2 = \lambda^2 - 2\lambda + 1$). Let $a := \sum_{i=0}^{k-1} a_i \lambda^i \in pR \cap \mathbb{Z}[\lambda]$. We show $p \mid a_i$ by induction on i. Because $\lambda \mid p \mid a$, it follows that $\lambda \mid a_0$ and $a_0 \in \lambda R \cap \mathbb{Z}$. Obviously $p \in \lambda R \cap \mathbb{Z} \trianglelefteq \mathbb{Z}$. In the case $\mathbb{Z} \subseteq \lambda R$, we would have $R = \lambda R = \lambda^k R = pR$ and $1/p \in R$. This contradiction shows $a_0 \in \lambda R \cap \mathbb{Z} = p\mathbb{Z}$. If the claim is already proven for all $i < k-1$, then λ is a divisor of $\epsilon \lambda^{k-i-1} = p/\lambda^{i+1}$ and thus also of

$$\frac{1}{\lambda^{i+1}} \Big(a - \sum_{j=0}^{i} a_j \lambda^j \Big) = \sum_{j=i+1}^{k-1} a_j \lambda^{j-i-1}.$$

It follows that $\lambda \mid a_{i+1}$ and $p \mid a_{i+1}$ as above. Overall, $a \in p\mathbb{Z}[\lambda] = p\mathbb{Z}[\zeta]$ as claimed.

Case 2: $n \in \mathbb{N}$ arbitrary.
Let $n = p_1^{a_1} \dots p_l^{a_l}$ be the prime factorization of n. As is well known, $\zeta_i := \zeta^{n/p_i^{a_i}}$ is a primitive $p_i^{a_i}$-th root of unity and $\mathbb{Q}_n = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1) \dots \mathbb{Q}(\zeta_l) = \mathbb{Q}_{p_1^{a_1}} \dots \mathbb{Q}_{p_l^{a_l}}$. According to Theorem I.12.14, it also holds that $\mathbb{Q}(\zeta_1) \dots \mathbb{Q}(\zeta_{l-1}) \cap \mathbb{Q}(\zeta_l) = \mathbb{Q}$. According to Case 1, $1, \zeta_i, \dots, \zeta_i^{\varphi(p_i^{a_i})}$ is an integral basis of $\mathbb{Q}_{p_i^{a_i}}$. According to Lemma A.3.14, the corresponding discriminants for different p_i are coprime. By induction on l, one obtains from Lemma A.3.16 an integral basis of $\mathbb{Q}_n$ consisting of powers of ζ. For $s \ge k$, $\zeta^s = \zeta^s - \zeta^{s-k} \Phi_n(\zeta)$ can be expressed as a $\mathbb{Z}$-linear combination of smaller ζ-powers. Therefore, $1, \zeta, \dots, \zeta^{k-1}$ is already an integral basis. □

Remark A.3.18. From Lemma A.3.14 and Lemma A.3.16 one can obtain an explicit (but extremely confusing) formula for D_{Φ_n}. In particular, n and D_{Φ_n} have the same prime divisors.

Theorem A.3.19 (KRONECKER)**.** *Let $\alpha \in \mathbb{Z}[X] \setminus \{X\}$ be irreducible. Suppose that for all roots $x \in \mathbb{C}$ of α, $|x| \leq 1$ holds. Then α is a cyclotomic polynomial.*

Proof (GREITER). The roots $x_1, \ldots, x_n \in \mathbb{C}$ of α are pairwise distinct, since α is irreducible (Theorem I.11.20) and not equal to 0 because of $\alpha \neq X$. The companion matrix $A \in \mathbb{Z}^{n \times n}$ of α has eigenvalues $x_1, \ldots, x_n$ (Lemma II.10.4) and is therefore diagonalizable. So let $S = (s_{ij}) \in \mathrm{GL}(n, \mathbb{C})$ with $SAS^{-1} = D = \mathrm{diag}(x_1, \ldots, x_n)$ and $S^{-1} = (s'_{ij})$. For $k \in \mathbb{N}$, the entry of $A^k = S^{-1}D^kS$ at position (i, j) is bounded by

$$\Big|\sum_{l=1}^{n} s'_{il} x_l^k s_{lj}\Big| \leq \sum_{l=1}^{n} |s'_{il} s_{lj}|.$$

Since the matrices A^k are integral, the set $\{A^k : k \in \mathbb{N}\}$ is finite. Thus there exist $k < l$ with $A^k = A^l$ and $A^{l-k} = 1 = D^{l-k}$. This shows $x_i^{l-k} = 1$ for $i = 1, \ldots, n$. As an irreducible divisor of $X^{l-k} - 1$, α must be a cyclotomic polynomial. □

Theorem A.3.20. *With the notation from Theorem III.12.57,*

$$\mathbb{F}_q C_n \cong \bigtimes_{d \mid m} \bigtimes_{i=1}^{\varphi(d)/\mathrm{ord}_d(q)} \mathbb{F}_q[X]/(\Phi_{d,i})^{p^k}$$

is the Peirce decomposition of $\mathbb{F}_q C_n$. For $d \mid m$ there are $\varphi(d)/\mathrm{ord}_d(q)$ non-isomorphic simple $\mathbb{F}_q C_n$-modules of dimension $\mathrm{ord}_d(q)$ (over $\mathbb{F}_q$). The corresponding projective-indecomposable modules have dimension $\mathrm{ord}_d(q)^{p^k}$.

Proof. For $G = \langle x \rangle \cong C_n$, the map $\mathbb{F}_q[X] \to \mathbb{F}_q G$, $X \mapsto g$ is a ring epimorphism with kernel $(X^n - 1)$. From the Chinese Remainder Theorem for rings, the stated decomposition follows with Theorem III.12.57 (cf. Exercise II.66). Let $R := \mathbb{F}_q[X]/(\Phi_{d,i})^{p^k}$. By the second isomorphism theorem, $M_{d,i} := \mathbb{F}_q[X]/(\Phi_{d,i})$ is a simple R-module. Furthermore,

$$\begin{aligned} M_{d,i} &\to (\Phi_{d,i})^a/(\Phi_{d,i})^{a+1}, \\ \alpha + (\Phi_{d,i}) &\mapsto \alpha\Phi_{d,i}^a + (\Phi_{d,i})^{a+1} \end{aligned}$$

is an isomorphism of R-modules for $a = 1, \ldots, p^k - 1$. The composition factors of the regular R-module are therefore isomorphic. By Theorem II.8.26, R must be a block of $\mathbb{F}_q C_n$. The $\mathbb{F}_q C_n$-submodules of R have the form $(\Phi_{d,i})^a/(\Phi_{d,i})^{p^k}$. In particular, R is projective-indecomposable. The dimensions result from the degrees of the $\Phi_{d,i}$. □

Example A.3.21. In the case $n \mid q - 1$, all irreducible representations of C_n over $\mathbb{F}_q$ have degree 1 (as over $\mathbb{C}$).

Corollary A.3.22. *Let $n \in \mathbb{N}$ and $q \neq 1$ be a prime power. Φ_n is irreducible in $\mathbb{F}_q[X]$ if and only if $g := \gcd(n, q^2) \leq 2$ and $|\langle q + \frac{n}{g}\mathbb{Z} \rangle| = \varphi(n)$.*

Proof. In the case $g = 1$, the claim follows from Theorem III.12.57. In the case $g = 2$, we have $n = 2m$ with $2 \nmid m$. Then $\Phi_n = \Phi_m(-X) = \Phi_m$ holds in $\mathbb{F}_2[X] \subseteq \mathbb{F}_q[X]$. Again, the claim holds by Theorem III.12.57. Now let $g > 2$ and $n = p^k m$ with $p \mid q$ and $p \nmid m$. Then

$$\Phi_n \mid X^n - 1 = \prod_{d|m} \Phi_d^{p^k}.$$

For $d \mid n$, we have $\varphi(d) \leq \varphi(n)$ according to Exercise I.51. Because of

$$\deg \Phi_n = \varphi(n) = \varphi(p^k)\varphi(m) > \varphi(m) \geq \varphi(d) = \deg \Phi_d$$

Φ_n cannot be irreducible. □

Example A.3.23.

(i) The condition in Corollary A.3.22 implies that Φ_n can only be irreducible in $\mathbb{F}_q[X]$ if $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic. According to Corollary I.8.35, n must therefore have the form $4, p^k, 2p^k$ for an odd prime p. Therefore, Φ_{12} is reducible modulo p for every prime p (cf. Example I.8.57).

(ii) For $q = 2$, we have

$$\begin{aligned}\Phi_{21} &= \frac{X^{21}-1}{\Phi_1\Phi_3\Phi_7} = \frac{X^{21}-1}{(X-1)(X^2+X+1)(X^6+\ldots+1)} \\ &= X^{12}+X^{11}+X^9+X^8+X^6+X^4+X^3+X+1 = \Phi_{21,1}\Phi_{21,2} \\ &= (X^6+X^4+X^2+X+1)(X^6+X^5+X^4+X^2+1) \in \mathbb{F}_2[X].\end{aligned}$$

Lemma A.3.24. *For $n \in \mathbb{N}$, we have*

$$\boxed{\Phi_n = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}}$$

with the Möbius function μ.

Proof. The Möbius inversion Theorem I.2.42 also holds if one replaces $(\mathbb{C}, +)$ with the abelian group $(\mathbb{Q}(X)^\times, \cdot)$ (same proof). For $f(n) := \Phi_n$, we have $F(n) = \prod_{d|n} f(d) = X^n - 1$. This shows the claim. □

Remark A.3.25.

(i) If $n = p_1^{a_1} \ldots p_s^{a_s}$ is the prime factorization of $n \in \mathbb{N}$ and $q := p_1 \ldots p_s$, then

$$\Phi_n = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|q} \big((X^{\frac{n}{q}})^{\frac{q}{d}} - 1\big)^{\mu(d)} = \Phi_q(X^{\frac{n}{q}})$$

according to Lemma A.3.24. This reduces the calculation of Φ_n to square-free n. For $p \in \mathbb{P}$ with $p \nmid n$, we have

$$\Phi_{pn} = \prod_{d|n} (X^{\frac{pn}{d}} - 1)^{\mu(d)} (X^{\frac{pn}{pd}} - 1)^{\mu(pd)} = \prod_{d|n} \frac{\big((X^p)^{\frac{n}{d}} - 1\big)^{\mu(d)}}{(X^{\frac{n}{d}} - 1)^{\mu(d)}} = \frac{\Phi_n(X^p)}{\Phi_n}.$$

Finally, $\Phi_p = X^{p-1} + X^{p-2} + \ldots + 1$ for $p \in \mathbb{P}$.

(ii) If one calculates $\Phi_1, \Phi_2, \ldots, \Phi_{104}$, one finds that all coefficients are 0 or ± 1. Surprisingly, this is false in general.

Theorem A.3.26 (SUZUKI). *Every integer is a coefficient of a cyclotomic polynomial.*

Proof. Let $s > 2$ be odd. For sufficiently large $m \in \mathbb{N}$, there exist, according to Chebyshev[1], prime numbers $p_1 < \ldots < p_s$ between m and $2m$. In particular, $p_1 + p_2 > 2m \geq p_s$ holds. Let $n := p_1 \ldots p_s$. Every divisor of n has the form $d = p_{i_1} \ldots p_{i_k}$ with $k \geq 0$. In the case $k < s-1$,

$$(X^{n/d} - 1)^{\mu(d)} \equiv -1 \pmod{X^{p_s+1}}.$$

The number of divisors with $k < s-1$ is $2^s - s - 1 \equiv 0 \pmod 2$. With Lemma A.3.24 it follows that

$$(X-1)\Phi_n \equiv \prod_{i=1}^{s}(X^{p_i} - 1) \equiv X^{p_1} + \ldots + X^{p_s} - 1 \pmod{X^{p_s+1}}.$$

Now $(X-1)(X^{p_s} + X^{p_s-1} + \ldots + X + 1) = X^{p_s+1} - 1 \equiv -1 \pmod{X^{p_s+1}}$ and one obtains

$$\begin{aligned}\Phi_n &\equiv -(X^{p_1} + \ldots + X^{p_s} - 1)(X^{p_s} + X^{p_s-1} + \ldots + X + 1) \\ &\equiv (1-s)X^{p_s} + (2-s)X^{p_s-1} + (2-s)X^{p_s-2} + \ldots \pmod{X^{p_s+1}},\end{aligned}$$

since $p_{s-1} \leq p_s - 2$. Thus $-1, -2, \ldots$ are already coefficients of cyclotomic polynomials. We can certainly assume $p_1 > 2$, so that n is odd. Let $\zeta_1, \ldots, \zeta_t \in \mathbb{C}$ be the primitive n-th roots of unity with $t = \varphi(n) \equiv 0 \pmod 2$. Then $-\zeta_1, \ldots, -\zeta_t$ are the primitive $2n$-th roots of unity. Thus

$$\begin{aligned}\Phi_{2n} &= \prod_{i=1}^{t}(X + \zeta_i) = (-1)^t \prod_{i=1}^{t}(-X - \zeta_i) = \Phi_n(-X) \\ &\equiv (s-1)X^{p_s} + (2-s)X^{p_s-1} + (s-2)X^{p_s-2} + \ldots \pmod{X^{p_s+1}}.\end{aligned}$$

Thus $1, 2, \ldots$ are also coefficients of cyclotomic polynomials. Finally, 0 is a coefficient of $\Phi_4 = X^2 + 1$. □

Definition A.3.27. Let $a, n \in \mathbb{N} \setminus \{1\}$. A prime number p is called a *Zsigmondy prime* with respect to a^n if $p \mid a^n - 1$ and $p \nmid a^k - 1$ for $k = 1, \ldots, n-1$. This means that a has multiplicative order n modulo p.

Lemma A.3.28. *Let $n = p^s m \in \mathbb{N}$ with $p \in \mathbb{P}$ and $s \geq 1$. Then $\Phi_n(a) > a^{p^{s-1}(p-2)}$ holds for $a \in \mathbb{N} \setminus \{1\}$.*

Proof. Because of $s \geq 1$, $n \geq p \geq 2$ holds. Let $\zeta = e^{2\pi \mathrm{i}/n} \in \mathbb{C}$. Then first

$$\Phi_n(a) = \prod_{\substack{1 \leq k \leq n \\ \gcd(n,k)=1}} (a - \zeta^k) = \prod_{\substack{1 \leq k \leq n/2 \\ \gcd(n,k)=1}} |a - \zeta^k|^2 > 0.$$

For $b := a^{p^{s-1}}$, $b^p - 1 \geq b^{p-2}(b^2 - 1)$ holds. As in Remark A.3.25, it follows that

$$\begin{aligned}\Phi_n(a) &= \prod_{d \mid m} \frac{(a^{n/d} - 1)^{\mu(d)}}{(a^{n/(pd)} - 1)^{\mu(d)}} = \frac{\Phi_m(a^{p^s})}{\Phi_m(a^{p^{s-1}})} = \frac{\Phi_m(b^p)}{\Phi_m(b)} = \prod_{\gcd(k,m)=1} \frac{|b^p - \zeta^k|}{|b - \zeta^k|} \\ &> \Big(\frac{b^p - 1}{b+1}\Big)^{\varphi(m)} \geq (b^{p-2}(b-1))^{\varphi(m)} \geq b^{p-2}.\end{aligned}$$

□

[1] See lecture notes number theory

Lemma A.3.29. *Let $a, n \geq 2$. Let p be a prime divisor of $\Phi_n(a)$ and $n = p^s m$ with $p \nmid m$ as well as $s \geq 0$.*

(i) p is a Zsigmondy prime with respect to a^n if and only if $s = 0$.

(ii) If $s \geq 1$, then $m \mid p - 1$. In particular, p is then the largest prime divisor of n.

(iii) If $s \geq 1$ and $p^2 \mid \Phi_n(a)$, then $p = n = 2$.

Proof.

(i) In the case $s \geq 1$, $1 \equiv a^n \equiv (a^p)^{n/p} \equiv a^{n/p}$ by Fermat. Thus p is not a Zsigmondy prime. Conversely, assume that p is not a Zsigmondy prime. Then the order of a modulo p must be a proper divisor of n. In particular, there exists a prime divisor q of n with $a^{n/q} \equiv 1 \pmod{p}$. Let $c := a^{n/q}$. From $\Phi_n(a) \mid \frac{a^n-1}{a^{n/q}-1}$ it follows that

$$0 \equiv \Phi_n(a) \equiv \frac{a^n - 1}{a^{n/q} - 1} \equiv \frac{c^q - 1}{c - 1} = 1 + c + \ldots + c^{q-1} \equiv q \pmod{p},$$

i. e. $p = q \mid n$.

(ii) The above argument shows that the order of a modulo p has the form n/p^t with $t \geq 1$. Thus $\frac{n}{p^t} \mid p - 1$, so $s = t$ and $m \mid p - 1$.

(iii) Let first $p > 2$ and $d := c - 1 = a^{n/p} - 1$. Then $p \mid d$ and

$$\frac{a^n - 1}{a^{n/p} - 1} = \frac{(1 + d)^p - 1}{d} = p + \sum_{k=2}^{p} \binom{p}{k} d^{k-1} \equiv p \pmod{p^2}.$$

Thus $p^2 \nmid \Phi_n(a)$. Now let $p = 2$ and $n > 2$. Then $n = 2^s$ by (ii) and a is odd because of $2 = p \mid a^n - 1$. As above, it follows that

$$\frac{a^n - 1}{a^{n/p} - 1} = \frac{c^2 - 1}{c - 1} = c + 1 = a^{2^{s-1}} + 1 \equiv 2 \pmod{4}.$$

This shows $4 \nmid \Phi_n(a)$. □

Theorem A.3.30 (Zsigmondy)**.** *For $a, n \geq 2$ there always exists a Zsigmondy prime with respect to a^n except in the following cases:*

(i) $n = 2$, $a = 2^k - 1$ for $k \geq 2$.

(ii) $n = 6$, $a = 2$.

Proof. If $\Phi_n(a)$ has more than one prime divisor, then a Zsigmondy prime exists by Lemma A.3.29. So let $\Phi_n(a) = p^k$, where p is the largest prime divisor of n. For $n = 2$, $p = 2$ and $2^k = \Phi_2(a) = a + 1$. So let $n \geq 3$. By Lemma A.3.29, $\Phi_n(a) = p$. In the case $p = 2$, $n = 2^s \geq 4$ and $\Phi_n(a) = a^{2^{s-1}} + 1 > 2 = p$. Thus $p > 2$ and $n = p^s m$ with $m \mid p - 1$. By Lemma A.3.28 it holds that

$$p = \Phi_n(a) > a^{p^{s-1}(p-2)} \geq 2^{p-2} = 2^{p-3} + 2^{p-4} + \ldots + 1 + 1 \geq p - 1.$$

This yields $p = 3$, $a = 2$ and $s = 1$. Thus $n \in \{3, 6\}$. For $a^n = 2^3$, 7 is a Zsigmondy prime. Thus only the exceptional case $n = 6$ remains. □

Remark A.3.31.

(i) For $n = 2$ and $a = 2^k - 1$, we have

$$a^n - 1 = 2^{2k} - 2^{k+1} = 2^k(a - 1)$$

and there is no Zsigmondy prime. The same holds for $(n, a) = (6, 2)$ because of $2^6 - 1 = 63 = 3^2 \cdot 7 = (2^2 - 1)^2(2^3 - 1)$.

(ii) Let $q > 1$ be a prime power. As is well known, $q^n - 1$ is a divisor of $|\mathrm{GL}(n, q)|$. With Zsigmondy and Cauchy, one can thus conclude the existence of invertible matrices with "large" prime order.

A.4 Analytical Proof of the Fundamental Theorem of Algebra

Remark A.4.1. We proved the Fundamental Theorem of Algebra in Theorem I.13.7 with as little analysis as possible (the intermediate value theorem for real polynomials was used). We now provide a shorter proof that uses a bit more analysis (but manages without complex analysis).

Theorem A.4.2. *Every non-constant polynomial $\alpha \in \mathbb{C}[X]$ has a root.*

Proof (Argand). Suppose α has no root. Since α is not constant, there exists an $r > 0$ with $|\alpha(x)| > |\alpha(0)|$ for all $x \in \mathbb{C}$ with $|x| > r$. The continuous function $\mathbb{C} \to \mathbb{R}$, $x \mapsto |\alpha(x)|$ (where $\mathbb{C}$ is viewed as $\mathbb{R}^2$) therefore attains its minimum on the compact set $\{x \in \mathbb{C} : |x| \leq r\}$. Let $|\alpha(x_0)| > 0$ be this minimum. By replacing α with $\alpha(x_0)^{-1}\alpha(X + x_0)$, we can assume $x_0 := 0$ and $\alpha(0) = 1$. Let $k \in \mathbb{N}$ with $\alpha = 1 + aX^k + X^{k+1}\beta$ for $a \in \mathbb{C}^\times$ and $\beta \in \mathbb{C}[X]$. Let $z \in \mathbb{C}$ be a k-th root of $-a^{-1}$. By replacing α with $\alpha(zX)$, we can assume $a = -1$. Since $x \mapsto |\beta(x)|$ is also continuous (possibly $\beta = 0$), there exists a $0 < t < 1$ with $t|\beta(t)| < 1$. Then one obtains the contradiction

$$|\alpha(t)| \leq 1 - t^k + t^k t|\beta(t)| < 1. \qquad \square$$

Remark A.4.3. In linear algebra 1, one usually proves the spectral theorem for symmetric matrices by using the Fundamental Theorem of Algebra for the existence of eigenvalues. This is unfavorable, as the spectral theorem itself does not require complex numbers. The following proof bypasses this problem.

Theorem A.4.4. *Every symmetric matrix $A \in \mathbb{R}^n$ has a real eigenvalue.*

Proof (Geck). Let

$$\mu(A) := \inf\bigl\{v^{\mathrm{t}} A v : v \in \mathbb{R}^n,\ |v| = 1\bigr\}$$

and $B := A - \mu(A)1_n$. For all $v \in \mathbb{R}^n$ it holds that $v^{\mathrm{t}} B v \geq 0$, i. e. B is positive semidefinite. Suppose that B is even positive definite. Using the Gram-Schmidt process, one finds a matrix $S \in \mathrm{GL}(n, \mathbb{R})$ with $B = S^{\mathrm{t}} S$ (Sylvester's Law of Inertia). By the definition of $\mu(A)$, there exists a sequence of normalized vectors $v_1, v_2, \ldots \in \mathbb{R}^n$ with

$$\lim_{i\to\infty} |Sv_i|^2 = \lim_{i\to\infty} v_i^{\mathrm{t}} B v_i = 0.$$

Now every coordinate of Sv_i must also tend to zero as $i \to \infty$. Using the triangle inequality, one obtains the contradiction

$$1 = \lim_{i\to\infty} |v_i| = \lim_{i\to\infty} |S^{-1} S v_i| = 0.$$

Thus $\det(B) = 0$ and there exists a $v \in \mathbb{R}^n$ with $Bv = 0$. Now v is an eigenvector of A for the eigenvalue $\mu(A)$. $\square$

A.5 Transcendental Extensions

Definition A.5.1. A field extension $K \subseteq L$ is called *finitely generated*, if $x_1, \ldots, x_n \in L$ (not necessarily algebraic) exist with $L = K(x_1, \ldots, x_n)$.

Theorem A.5.2. *Let $K \subseteq M \subseteq L$ be field extensions. If L is finitely generated over K, then so is M.*

Proof. Every finite generating set of L contains a transcendence basis of L over K. For a transcendence basis T of M over K, it then holds that $|T| = \operatorname{trg}(M|K) \leq \operatorname{trg}(L|K) < \infty$. By replacing K with $K(T)$, we can assume that M is algebraic over K (certainly L is then still finitely generated). Let B be a transcendence basis of L over K. Because of $|L : K(B)| < \infty$, it suffices to show $|M : K| \leq |L : K(B)|$. Because of

$$\begin{aligned}\operatorname{trg}(M(B)|M) &= \operatorname{trg}(M(B)|M) + \operatorname{trg}(M|K) = \operatorname{trg}(M(B)|K)\\ &= \operatorname{trg}(M(B)|K(B)) + \operatorname{trg}(K(B)|K) = \operatorname{trg}(K(B)|K) = |B|\end{aligned}$$

B is algebraically independent over M. Let $a_1, \ldots, a_n \in M$ be linearly independent over K and $\sum_{i=1}^{n} \lambda_i a_i = 0$ with $\lambda_1, \ldots, \lambda_n \in K(B)$. Multiplying the λ_i by a common denominator, one obtains polynomials $\delta_1, \ldots, \delta_n \in K[X_b : b \in B]$ with $\sum \delta_i(B) a_i = 0$. Since B is algebraically independent over M, it follows that $\sum a_i \delta_i = 0$. A comparison of coefficients yields $\delta_1 = \ldots = \delta_n = 0$, because the a_i are linearly independent over K. Since $K[X_b : b \in B]$ is an integral domain, $\lambda_1 = \ldots = \lambda_n = 0$ also holds. Thus $a_1, \ldots, a_n$ are also linearly independent over $K(B)$. This shows $|M : K| \leq |L : K(B)| < \infty$. □

Theorem A.5.3 (Lüroth)**.** *Let $K \subseteq L \subseteq M$ be field extensions and $x \in M$ with $M = K(x)$. Then there exists an $a \in L$ with $L = K(a)$.*

Proof. If x is algebraic over K, then the assertion follows from Exercise II.19. Thus, let x be transcendental and wlog. $K \subsetneq L \subseteq M = K(X)$. According to Lemma II.4.9, $K \subseteq L$ is (absolutely) transcendental. Therefore,

$$1 = \operatorname{trg}(K(X)|K) \overset{\text{II.4.18}}{=} \operatorname{trg}(K(X)|L) + \operatorname{trg}(L|K) \geq \operatorname{trg}(K(X)|L) + 1$$

and $L \subseteq K(X)$ is algebraic. Let $\alpha \in L[Y]$ be the minimal polynomial of X over L. Since X is transcendental over K, α has a coefficient $a \in L \setminus K$. We now work over the unique factorization domains $R := K[X]$ and $R[Y]$. We write $a = \frac{b}{c}$ with coprime $b, c \in R$. Let $d \in R$ such that $\tilde{\alpha} := d\alpha \in R[Y]$ is primitive. Then d is the leading coefficient of $\tilde{\alpha}$ and $c \mid d$. We define

$$\begin{aligned}\beta &:= cb(Y) - bc(Y) \in R[Y],\\ \gamma &:= \frac{\beta}{c} = b(Y) - ac(Y) \in K(a)[Y] \subseteq M[Y].\end{aligned}$$

Because of $\gamma(X) = \beta(X) = 0$, it follows that $\alpha \mid \gamma$. Therefore, there exists $\delta \in K(X)[Y]$ with $\tilde{\alpha}\delta = \beta$.

We show $\delta \in K$ in three steps. Let $e \in R$ such that $\tilde{\delta} := e\delta \in R[Y]$ is primitive. According to Lemma II.5.24, $e\beta = \tilde{\alpha}\tilde{\delta}$ is also primitive and it follows that $e \in R^\times = K^\times$. Thus $\delta \in R[Y]$. Let $\deg_X \beta$ be the degree of β as a polynomial in X (with coefficients in $K[Y]$). Then

$$\deg_X \beta \leq \max\{\deg b, \deg c\} \leq \deg_X \tilde{\alpha}, \tag{A.5.1}$$

holds, because $\tilde{\alpha}$ has two coefficients that are divisible by c and b respectively. Therefore, even $\delta \in K[Y]$ holds. Euclidean division yields $\sigma_b, \sigma_c, \tau_b, \tau_c \in K[Y]$ with $b(Y) = \sigma_b\delta + \tau_b$, $c(Y) = \sigma_c\delta + \tau_c$ and $\deg \tau_b, \deg \tau_c < \deg \delta$. Because of

$$\beta = cb(Y) - bc(Y) = c(\sigma_b\delta + \tau_b) - b(\sigma_c\delta + \tau_c) = \delta(c\sigma_b - b\sigma_c) + c\tau_b - b\tau_c$$

we have $\delta \mid c\tau_b - b\tau_c$. A comparison of degrees shows $c\tau_b - b\tau_c = 0$. The equation $c\tau_b = b\tau_c$ in $K(Y)[X]$ implies $b \mid c \mid b$. Because of $\gcd(b, c) = 1$ and $b/c = a \notin K$, this is only possible if $\tau_b = \tau_c = 0$. Thus $\delta \mid \gcd(b, c) = 1$, i. e. $\delta \in K$.

Since the minimal polynomial of X over $K(a)$ is a divisor of γ, we have

$$\begin{aligned} |K(X) : L| = |L(X) : L| &= \deg \alpha = \deg \tilde{\alpha} = \deg(\tilde{\alpha}\delta) = \deg \beta = \deg \gamma \\ &\geq |K(a)(X) : K(a)| = |K(X) : K(a)| \overset{a \in L}{\geq} |K(X) : L|. \end{aligned}$$

This shows $L = K(a)$. □

Theorem A.5.4 (Steinitz)**.** *Any two uncountable algebraically closed fields of the same cardinality and the same characteristic are isomorphic.*

Proof. Let K be an uncountable, algebraically closed field. The characteristic of K determines the prime field P of K up to isomorphism. Let B be a transcendence basis of K over P. Then K is the algebraic closure of $P(B)$. According to Corollary II.2.11, K is uniquely determined up to isomorphism by $P(B)$. Since every element of K is a root of a polynomial in $P(B)[X]$, K is a countable union of copies of $P(B)$. Since K is infinitely large, K and $P(B)$ must have the same cardinality. According to Remark II.4.7, $P(B)$ is isomorphic to the field of rational functions $P(X_b : b \in B)$. It therefore suffices to show that $P(B)$ and B have the same cardinality. As is well known, P is at most countable. Every element in $P(B)$ has the form $\alpha(C)/\beta(C)$, where α and β are polynomials with coefficients in P and C is a finite subset of B. If B were finite, then $P(B)$ and K would be countable. Thus B is infinite. Let

$$\mathcal{B} := \{C \subseteq B : |C| < \infty\}.$$

Then $P(B)$ is contained in a set of type $\bigcup_{C \in \mathcal{B}} P$. In particular, $P(B)$ and $\mathcal{B}$ have the same cardinality. In set theory[1] it is shown that $\mathcal{B}$ and B have the same cardinality. Thus K and B also have the same cardinality. Overall, K is uniquely determined up to isomorphism by its cardinality and characteristic. □

Example A.5.5. The countable algebraically closed fields $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}(X)}$ are not isomorphic, since $\overline{\mathbb{Q}(X)}$ is not algebraic over its prime field.

Remark A.5.6. The (formal) derivative for polynomials can be defined just as well for power series and even Laurent series (Exercise II.30). The sum and product rules transfer easily. From the product rule it follows that

$$\alpha' = \left(\frac{\alpha}{\beta}\beta\right)' = \left(\frac{\alpha}{\beta}\right)'\beta + \frac{\alpha\beta'}{\beta}$$

[1] See notes on logic and set theory

for $\alpha, \beta \in K((X))$ and $\beta \neq 0$. By rearranging, one obtains the *quotient rule*

$$\Big(\frac{\alpha}{\beta}\Big)' = \frac{\alpha'\beta - \alpha\beta'}{\beta^2}.$$

According to the universal property, the embedding $K[X] \hookrightarrow K[[X]] \hookrightarrow K((X))$ can be extended to exactly one homomorphism $K(X) \to K((X))$ (Exercise I.40). In the following, we consider $K(X)$ as a subfield of $K((X))$.

Definition A.5.7. Let $\frac{\partial\alpha}{\partial X_k}$ be the (partial) derivative of $\alpha \in K(X_1, \ldots, X_n)$ with respect to X_k.

Lemma A.5.8 (Multidimensional chain rule)**.** *For $\alpha \in K[X_1, \ldots, X_n]$ and $\beta_1, \ldots, \beta_n \in K(X_1, \ldots, X_n)$ it holds that*

$$\frac{\partial\alpha(\beta_1, \ldots, \beta_n)}{\partial X_k} = \sum_{i=1}^{n} \frac{\partial\beta_i}{\partial X_k} \frac{\partial\alpha}{\partial X_i}(\beta_1, \ldots, \beta_n).$$

Proof. Due to the sum rule, we can assume that α is a monomial, say $\alpha = X_1^{a_1} \ldots X_n^{a_n}$. According to the product rule, it holds that

$$\frac{\partial\alpha(\beta_1, \ldots, \beta_n)}{\partial X_k} = \sum_{i=1}^{n} a_i \frac{\partial\beta_i}{\partial X_k} \beta_1^{a_1} \ldots \beta_i^{a_i - 1} \ldots \beta_n^{a_n} = \sum_{i=1}^{n} \frac{\partial\beta_i}{\partial X_k} \frac{\partial\alpha}{\partial X_i}(\beta_1, \ldots, \beta_n). \qquad \square$$

Theorem A.5.9. *Let* $\operatorname{char} K = 0$*. The elements $\alpha_1, \ldots, \alpha_n \in K(X_1, \ldots, X_n)$ form a transcendence basis of $K(X_1, \ldots, X_n)$ over K if and only if* $\det(\partial\alpha_i/\partial X_j) \neq 0$*.*

Proof. Because of $\operatorname{trg}(K(X_1, \ldots, X_n)) = n$, $\alpha_1, \ldots, \alpha_n$ is a transcendence basis if and only if $\alpha_1, \ldots, \alpha_n$ are algebraically independent. Assume $\alpha_1, \ldots, \alpha_n$ are algebraically dependent. Then there exists $\beta \in K[X_1, \ldots, X_n] \setminus K$ with $\beta(\alpha_1, \ldots, \alpha_n) = 0$. Let $\deg\beta$ be as small as possible. The chain rule yields

$$\sum_{j=1}^{n} \frac{\partial\alpha_j}{\partial X_i} \frac{\partial\beta}{\partial X_j}(\alpha_1, \ldots, \alpha_n) = 0$$

for $i = 1, \ldots, n$. This is a linear system of equations in $K(X_1, \ldots, X_n)$ with coefficient matrix $(\partial\alpha_j/\partial X_i)$. Because of $\beta \notin K$ and $\operatorname{char} K = 0$, there exists a j with $\partial\beta/\partial X_j \neq 0$. Since $\deg\beta$ is minimal, $\frac{\partial\beta}{\partial X_j}(\alpha_1, \ldots, \alpha_n) \neq 0$ holds. Thus the system of equations has a non-trivial solution and the determinant of the coefficient matrix must be 0.

Now let $\alpha_1, \ldots, \alpha_n$ be algebraically independent over K. Because of $\operatorname{trg}(K(X_1, \ldots, X_n)) = n$, $X_i, \alpha_1, \ldots, \alpha_n$ are algebraically dependent for $1 \leq i \leq n$. Let $\beta_i \in K[X_0, \ldots, X_n] \setminus K$ with $\beta_i(X_i, \alpha_1, \ldots, \alpha_n) = 0$ and $\deg\beta_i$ minimal. Differentiating with respect to X_k yields

$$\delta_{ik} \frac{\partial\beta_i}{\partial X_0}(X_i, \alpha_1, \ldots, \alpha_n) + \sum_{j=1}^{n} \frac{\partial\alpha_j}{\partial X_k} \frac{\partial\beta_i}{\partial X_j}(X_i, \alpha_1, \ldots, \alpha_n) = 0$$

for $i = 1, \ldots, n$. Since $\alpha_1, \ldots, \alpha_n$ are algebraically independent, X_0 must appear in every β_i. In particular, $\partial\beta_i/\partial X_0 \neq 0$ with smaller degree than β_i. By the choice of β_i, $\frac{\partial\beta_i}{\partial X_0}(X_i, \alpha_1, \ldots, \alpha_n) \neq 0$ for $i = 1, \ldots, n$. This yields a matrix equation in $K[X_1, \ldots, X_n]$:

$$\Big(\frac{\partial\beta_i}{\partial X_j}(X_i, \alpha_1, \ldots, \alpha_n)\Big)\Big(\frac{\partial\alpha_i}{\partial X_j}\Big) = -\Big(\delta_{ij} \frac{\partial\beta_i}{\partial X_0}(X_i, \alpha_1, \ldots, \alpha_n)\Big).$$

Since the determinant of the diagonal matrix on the right side does not vanish, $\det(\partial\alpha_i/\partial X_j) \neq 0$ must hold. $\square$

Remark A.5.10. One calls $(\partial\alpha_i/\partial X_j)$ the *Jacobian matrix* of $\alpha_1, \ldots, \alpha_n$.

Example A.5.11. Let $\alpha = XY$, $\beta = Y + Z$ and $\gamma = \frac{X^2}{Z}$. The determinant of the Jacobian matrix is

$$\det \begin{pmatrix} Y & X & 0 \\ 0 & 1 & 1 \\ \frac{2X}{Z} & 0 & -\frac{X^2}{Z^2} \end{pmatrix} = -\frac{X^2Y}{Z^2} + \frac{2X^2}{Z} = \frac{X^2(2Z - Y)}{Z^2} \neq 0.$$

Therefore α, β, γ is a transcendence basis of $K(X, Y, Z)$.

Definition A.5.12. Let $\alpha \in K[X_1, \ldots, X_n]$ such that the degree of α in each X_i is less than d. One calls

$$\Omega(\alpha) := \alpha(Y, Y^d, \ldots, Y^{d^{n-1}}) \in K[Y]$$

the *Kronecker transformation* of α.

Remark A.5.13. Let $k := \sum_{i=0}^{n-1} k_i d^i$ be a d-adic expansion. Then $\Omega(X_1^{k_0} \ldots X_n^{k_{n-1}}) = Y^k$. Moreover, $\Omega(\alpha \dot{+} \beta) = \Omega(\alpha) \dot{+} \Omega(\beta)$ holds for all α, β, whenever well-defined. By the uniqueness of the d-adic expansion, Ω is an isomorphism between the vector space of polynomials in $K[X_1, \ldots, X_n]$ of degree $< d$ in each variable and the vector space of polynomials in $K[Y]$ of degree $< d^n$ (both spaces have dimension d^n). The following criterion allows one to check the irreducibility of α in the ordinary polynomial ring $K[Y]$.

Theorem A.5.14 (Kronecker Criterion)**.** *Let $\alpha \in K[X_1, \ldots, X_n]$ and $d \geq 2$ such that the degree of α in each X_i is less than d. Then α is irreducible if and only if for every factorization $\Omega(\alpha) = \beta\gamma$ with $\beta, \gamma \in K[Y] \setminus K$, the polynomial $\Omega^{-1}(\beta)\Omega^{-1}(\gamma)$ has degree $\geq d$ in some X_i.*

Proof. Let α be reducible, thus $\alpha = \alpha_1\alpha_2$ with $\alpha_1, \alpha_2 \in K[X_1, \ldots, X_n] \setminus K$. The degree of α_i in each X_j is $< d$. For $\beta := \Omega(\alpha_1)$, $\gamma := \Omega(\alpha_2)$, it holds that $\Omega(\alpha) = \beta\gamma$ and $\Omega^{-1}(\beta)\Omega^{-1}(\gamma) = \alpha$.

Conversely, assume that $\Omega(\alpha) = \beta\gamma$ holds, where the degree of $\Omega^{-1}(\beta)\Omega^{-1}(\gamma)$ in each X_i is less than d. Due to the uniqueness of the Kronecker transformation, $\alpha = \Omega^{-1}(\beta)\Omega^{-1}(\gamma)$ must then hold. Thus α is reducible. □

Example A.5.15. Let $\alpha = X_1 + X_2 \in \mathbb{Q}[X_1, X_2]$ with $d = 2$. Then $\Omega(\alpha) = Y + Y^2 = Y(1 + Y)$, $\Omega^{-1}(Y) = X_1$ and $\Omega^{-1}(1 + Y) = 1 + X_1$. Since the degree of X_1 in $X_1(1 + X_1) = X_1 + X_1^2$ is equal to d, α is irreducible.

A.6 Automorphism Groups of Number Fields

Remark A.6.1. According to Exercise II.20, for every finite group G there exists a Galois extension $K \subseteq L$ with $\mathrm{Gal}(L|K) \cong G$. The inverse Galois problem mentioned in Remark I.12.18 asks whether one can always choose $K = \mathbb{Q}$. In Theorem I.12.19 and Theorem II.11.48 we have verified this for abelian and symmetric groups. We prove in this section that there always exists a (non-normal) field extension $\mathbb{Q} \subseteq L$ with $\mathrm{Aut}(L) = \mathrm{Gal}(L|\mathbb{Q}) \cong G$.

Lemma A.6.2. *Let $X^n + a_1X^{n-1} + \ldots + a_n \in \mathbb{R}[X]$ with n pairwise distinct real roots. Then there exists an $\epsilon > 0$ with the following property: If $b_1, \ldots, b_n \in \mathbb{R}$ with $|a_i - b_i| < \epsilon$ for $i = 1, \ldots, n$, then $X^n + b_1X^{n-1} + \ldots + b_n$ also has n pairwise distinct real roots.*

Proof. We consider the function $f\colon \mathbb{R}^n \to \mathbb{R}^n$ that maps $(x_1, \ldots, x_n)$ to the coefficients $c_1, \ldots, c_n$ of $(X - x_1) \ldots (X - x_n)$. According to Vieta, $f(x)_i = c_i = (-1)^i\sigma_i(x)$ for $i = 1, \ldots, n$. In particular, f_i is continuously differentiable, i. e. all partial derivatives exist and are continuous. By assumption, there exists $y \in \mathbb{R}^n$ with $f(y) = (a_1, \ldots, a_n)$ and $y_i \neq y_j$ for $i \neq j$. We show that the Jacobian matrix $J_f = (\partial f_i/\partial x_j)$ is invertible at y. By multiplying every second row by -1, we can consider

$$A := \Big(\frac{\partial\sigma_i}{\partial x_j}\Big)(y) = \begin{pmatrix} 1 & \cdots & 1 \\ y_2 + \ldots + y_n & \cdots & y_1 + \ldots + y_{n-1} \\ \vdots & & \vdots \\ y_2 \ldots y_n & \cdots & y_1 \ldots y_{n-1} \end{pmatrix}.$$

We subtract $\sigma_1(y)$ times the first row from the second row of A and then multiply it by -1. The second row is then $(y_1, y_2, \ldots, y_n)$. Let us assume inductively that the i-th row (for $i = 1, \ldots, k$) of A has already been transformed into the form $(y_1^{i-1}, \ldots, y_n^{i-1})$ by elementary row operations. We subtract $\sigma_k(y)$ times the first row from the $(k+1)$-th row. In the entry at position $(k+1, j)$, all terms that do not contain y_j vanish as a result. Now we add $\sigma_2(y)$ times the second row to the $(k+1)$-th row. This causes all terms containing exactly one y_j to vanish. Continuing this procedure finally yields at position $(k+1, j)$

$$\frac{\partial\sigma_{k+1}}{\partial x_j}(y) - \sigma_k(y) + y_j\sigma_{k-1}(y) \mp \ldots + (-1)^{k+1}y_j^k\sigma_1(y) = (-1)^{k+1}y_j^{k+1}.$$

By subsequent multiplication by $(-1)^{k+1}$, the $(k+1)$-th row becomes $(y_1^{k+1}, \ldots, y_n^{k+1})$. By induction on k, A thus becomes a Vandermonde matrix with $\det A = \prod_{i<j}(y_j - y_i) \neq 0$. In particular, A and $J_f(y)$ are invertible.

According to the Inverse Function Theorem from analysis[1], f has a continuous inverse function in an open neighborhood U of $(a_1, \ldots, a_n)$. For $(b_1, \ldots, b_n) \in U$, the polynomial $X^n + b_1X^{n-1} + \ldots + b_n$ has real roots "near" $y_1, \ldots, y_n$. In particular, these roots must be pairwise distinct (if close enough). □

Lemma A.6.3. *Let K be a number field and $\alpha \in K[X]$ of degree 3 without double roots. Then α has only real roots if and only if $D_\alpha > 0$.*

[1] See Theorem 8.3 in [O. Forster, *Analysis 2*, Springer Spektrum, Wiesbaden, 2017]

Proof. Let $x, y, z \in \mathbb{C}$ be the roots of α and wlog. $x \in \mathbb{R}$. If $z = \overline{y}$, then

$$D_\alpha = (x-y)^2(x-\overline{y})^2(y-\overline{y})^2 = |x-y|^4\big(2\mathrm{Im}(y)\big)^2 < 0.$$

If, on the other hand, $y, z \in \mathbb{R}$, then $D_\alpha = \big((x-y)(x-z)(y-z)\big)^2 > 0$. □

Theorem A.6.4 (Fried)**.** *Every finite group is the automorphism group of a real number field.*

Proof (Geyer). Let G be a finite group. According to Cayley, we can assume $G \leq S_n$ for an $n \in \mathbb{N}$. Wlog. let $n \geq 3$ be a prime number. As is well known, there exist irreducible polynomials $\overline{\alpha}_2 \in \mathbb{F}_2[X]$ and $\overline{\alpha}_3 \in \mathbb{F}_3[X]$ with degrees $n-2$ and n (for example, minimal polynomials of generators of $\mathbb{F}_{3^n}^\times$). We choose monic polynomials $\alpha_2, \alpha_3 \in \mathbb{Z}[X]$ with $\alpha_p \equiv \overline{\alpha}_p \pmod p$ for $p \in \{2,3\}$ and define

$$\alpha := 3(X^2+X+1)\alpha_2 - 2\alpha_3 \in \mathbb{Z}[X]$$

of degree n. With $\overline{\alpha}_3$, $\alpha \equiv \alpha_3 \pmod 3$ is also irreducible. Since the polynomials $(X^2+X+1)\overline{\alpha}_2$ and $\overline{\alpha}_3$ have no double roots, the discriminant D_α is coprime to 6. According to Dedekind (Theorem II.11.44), $\mathrm{Gal}(\alpha)$ possesses a permutation with cycle type $(2, n-2)$. Since $n-2$ is odd, one obtains a transposition in $\mathrm{Gal}(\alpha)$ by exponentiation. From Lemma II.11.47 it follows that $\mathrm{Gal}(\alpha) \cong S_n$ (cf. Theorem II.11.48). This property is preserved if we add rational numbers of the form $\frac{6k}{1+6l}$ with $k, l \in \mathbb{Z}$ to the coefficients of α. (One can multiply α by a common denominator congruent to 1 modulo 6 to guarantee $\alpha \in \mathbb{Z}[X]$. Dedekind's theorem then remains valid.) In this way, we can bring the coefficients of α arbitrarily close to the corresponding coefficients of $(X-1)(X-2)\dots(X-n)$. According to Lemma A.6.2, α now has only real roots.

Let $L \subseteq \mathbb{R}$ be a splitting field of α and $M := \mathrm{Fix}(G) \subseteq L$. Let $a \in \mathbb{Z}_M \subseteq \mathbb{Z}_L$ be a primitive element of M. According to Theorem II.11.25, $\mathbb{Z}_L$ is a Dedekind domain. Let $P \trianglelefteq \mathbb{Z}_L$ be a prime ideal with $(3) \subseteq P$. We consider the P-adic valuation $\nu := \nu_P$ on $\mathbb{Z}_L$. According to Lemma III.10.5, ν extends to an ultrametric valuation on L. Let R be the corresponding valuation ring from Theorem III.10.9. In the case $\nu(a) < 1$, we replace a by $a+1$. According to Remark III.10.4, then $\nu(a) = 1$ holds. Let $a_1 > \ldots > a_k$ be the Galois conjugates of a in L. By replacing a with $a + 3m$ for an $m \in \mathbb{N}$, one can assume $a_k > 0$. By replacing G with a conjugate subgroup in S_n, one can additionally achieve $a = a_1$. We choose $t = 3^{\frac{b}{c}} \in \mathbb{Q}$ with $b, c \in \mathbb{N} \setminus 3\mathbb{N}$ and $a > \frac{1}{t} > a_2$. Let

$$\beta_i := X^3 - 3X - 2a_i t \in L[X]$$

for $i = 1, \dots, k$. According to Theorem II.11.43, 3 is unramified in $\mathbb{Z}_L \subseteq R$. Because of $\nu(a) = 1$, β_1 is irreducible over L according to the Eisenstein criterion (Exercise III.58). By the choice of t,

$$D_{\beta_1} = 4 \cdot 27 - 4 \cdot 27(at)^2 < 0.$$

According to Lemma A.6.3, β_1 has a root $y \in \mathbb{C} \setminus \mathbb{R}$. We set $K := L(y)$. For $\gamma \in \mathrm{Aut}(K)$, $\gamma(y)$ is a root of $\gamma(\beta_1) = \beta_i$ for some $i \geq 1$. Let us assume $i \neq 1$. Then $D_{\beta_i} > 0$ and Lemma A.6.3 shows $\gamma(y) \in \mathbb{R}$. Now one has the contradiction $y \in K = L(\gamma(y)) \subseteq \mathbb{R}$. Thus $i = 1$ and $\gamma(a) = a$. According to Theorem I.14.25, $\mathrm{Gal}(\beta_1) \cong S_3$. Therefore K can contain only one root of β_1. This shows $\gamma(y) = y$. Overall it follows

$$\mathrm{Aut}(K) = \mathrm{Gal}\big(L(y)|\mathbb{Q}(a,y)\big) = \mathrm{Gal}\big(L(y)|M(y)\big).$$

Because of $\beta_1 \in M[X]$, $|M(y) : M| = \deg \beta_1 = 3$ and $L \cap M(y) = \mathbb{R} \cap M(y) = M$. The translation theorem of Galois theory yields $\mathrm{Gal}\big(L(y)|M(y)\big) \cong \mathrm{Gal}(L|M) \cong G$. Let $z \in \mathbb{R}$ be the real root of β_1. Then $L(z) \cong L[X]/(\beta_1) \cong K$ is a real number field with $\mathrm{Aut}(L(z)) \cong G$. □

Remark A.6.5. The extension $L \subseteq K$ constructed in the proof is not normal, because $\mathrm{Gal}(K|L) \not\trianglelefteq \mathrm{Gal}(\beta_1) \cong S_3$. Therefore, $\mathbb{Q} \subseteq K$ is not a Galois extension.

A.7 Artin-Schreier Theory

Remark A.7.1. We begin with a generalization of Lemma I.14.2.

Definition A.7.2. For $n \in \mathbb{N}$ and a field K, let $(K^\times)^n := \{x^n : x \in K^\times\} \leq K^\times$.

Theorem A.7.3 (Kummer)**.** *Let $n \in \mathbb{N}$ and K be a field containing a primitive n-th root of unity. For $x \in K^\times$, let K_x be a splitting field of $X^n - x$. Then the map $\langle x(K^\times)^n\rangle \mapsto K_x$ is a bijection between the set of cyclic subgroups of $K^\times/(K^\times)^n$ of order n and the set of K-isomorphism classes of Galois extensions $K \subseteq L$ with $\mathrm{Gal}(L|K) \cong C_n$.*

Proof. Let $\zeta \in K$ be a primitive n-th root of unity and $x \in K^\times$ and $|\langle x(K^\times)^n\rangle| = n$. Let $y \in K_x$ with $y^n = x$. Then $\zeta y, \zeta^2 y, \ldots, \zeta^n y$ are the pairwise distinct roots of $X^n - x$. According to Artin, $K \subseteq K_x$ is a Galois extension. According to (the proof of) Lemma I.14.2,

$$d := |K_x : K| = |K(y) : K|$$

is a divisor of n. The minimal polynomial μ_y of y over K divides $X^n - x$ and therefore possesses roots of the form $\zeta^i y$ with $i \in \mathbb{Z}$. The constant term of μ_y thus has the form $\pm\zeta^i y^d$. This shows $y^d \in K$ and $x^d = (y^d)^n \in (K^\times)^n$. Because of $|\langle x(K^\times)^n\rangle| = n$, it follows that $d = n$. According to Lemma I.14.2, $\mathrm{Gal}(L|K) \cong C_n$. Let $x' \in K^\times$ with $\langle x'(K^\times)^n\rangle = \langle x(K^\times)^n\rangle$. Then there exist $m \in \mathbb{N}$ and $a \in K^\times$ with $x' = x^m a^n$. Since $X^n - x'$ has the roots $y^m a\zeta^i \in K_x$ for $i = 1, \ldots, n$, K_x is also the splitting field of $X^n - x'$. It follows that $K_{x'} \cong K_x$. Overall, this shows the well-definedness of the specified mapping $\langle x(K^\times)^n\rangle \mapsto K_x$.

For surjectivity, let $K \subseteq L$ be a Galois extension with $\mathrm{Gal}(L|K) \cong C_n$. According to Lemma I.14.2, L is the splitting field of $X^n - x$ for some $x \in K$. Because of $|L : K| = n$, $X^n - x$ is irreducible and $x^d \notin K$ for $d < n$. Thus $|\langle x(K^\times)^n\rangle| = n$. Finally, let $x, x' \in K^\times$ with $|\langle x(K^\times)^n\rangle| = |\langle x'(K^\times)^n\rangle| = n$ and let $\Gamma\colon K_x \to K_{x'}$ be a K-isomorphism. Wlog. let K_x and $K_{x'}$ be subfields of the algebraic closure $\overline{K}$. Since $\Gamma(K_x) = K_{x'}$ is a splitting field of $\Gamma(X^n - x) = X^n - x$, it now holds that $K_x = K_{x'}$. Let $\mathrm{Gal}(K_x|K) = \langle\sigma\rangle$. Let $y \in K_x$ and $y' \in K_{x'}$ with $y^n = x$ and $(y')^n = x'$. Then $\sigma(y)/y$ and $\sigma(y')/y'$ are primitive n-th roots of unity in K. Wlog. let $\sigma(y) = \zeta y$ and $\sigma(y') = \zeta^m y'$ for some $m \leq n$. Because of $K_x = K(y)$, there exist $\lambda_1, \ldots, \lambda_n \in K$ with $y' = \sum_{i=1}^n \lambda_i y^i$. It follows that

$$\sum_{i=1}^n \lambda_i \zeta^m y^i = \zeta^m y' = \sigma(y') = \sum_{i=1}^n \lambda_i \sigma(y)^i = \sum_{i=1}^n \lambda_i \zeta^i y^i.$$

A comparison of coefficients yields $\lambda_i = 0$ for $i \neq m$. Thus $y' = \lambda_m y^m$ and $x' = (y')^n = \lambda_m^n x^m \in x^m(K^\times)^n$. This shows $\langle x(K^\times)^n\rangle = \langle x'(K^\times)^n\rangle$ and the mapping $\langle x(K^\times)^n\rangle \mapsto K_x$ is injective. □

Example A.7.4. Kummer's theorem can be applied to $K = \mathbb{Q}$ and $n = 2$. For $a, b \in \mathbb{Q}^\times$, it holds that $\mathbb{Q}(\sqrt{a}) \cong \mathbb{Q}(\sqrt{b})$ if and only if $ab^{-1} \in (\mathbb{Q}^\times)^2$ (cf. Exercise I.56).

Theorem A.7.5 (HILBERT's Theorem 90)**.** *Let $K \subseteq L$ be a Galois extension with cyclic Galois group $G = \langle \sigma \rangle$ and $a \in L$.*

(i) $\prod_{\tau \in G} \tau(a) = 1$ *holds if and only if* $a = \frac{b}{\sigma(b)}$ *for some* $b \in L^\times$.

(ii) $\sum_{\tau \in G} \tau(a) = 0$ *holds if and only if* $a = b - \sigma(b)$ *for some* $b \in L$.

Proof. Let $|G| = n$.

(i) For $a = \frac{b}{\sigma(b)}$, it is certain that $N(a) := \prod_{\tau \in G} \tau(a) = 1$. Conversely, let $N(a) = 1$. According to Lemma I.14.1,

$$\Gamma := \mathrm{id}_L + a\sigma + a\sigma(a)\sigma^2 + \ldots + a\sigma(a)\ldots\sigma(a)^{n-2}\sigma^{n-1} \neq 0.$$

So let $c \in L$ with $b := \Gamma(c) \in L^\times$. Then

$$a\sigma(b) = a\sigma(c) + a\sigma(a)\sigma^2(c) + \ldots + N(a)\sigma^n(c) = a\sigma(c) + a\sigma(a)\sigma^2(c) + \ldots + c = b.$$

(ii) For $a = b - \sigma(b)$, it is certain that $S(a) := \sum_{\tau \in G} \tau(a) = 0$. Conversely, let $S(a) = 0$. According to Lemma I.14.1, there exists a $c \in L$ with $S(c) \in L^G \setminus \{0\} = K \setminus \{0\}$. After normalization, $S(c) = 1$ holds. For

$$b := a\sigma(c) + (a + \sigma(a))\sigma^2(c) + \ldots + (a + \ldots + \sigma^{n-2}(a))\sigma^{n-1}(c)$$

it then holds that

$$\sigma(b) = \sigma(a)\sigma^2(c) + \ldots + \underbrace{(\sigma(a) + \ldots + \sigma^{n-1}(a))}_{=S(a)-a=-a}c = \sigma(a)\sigma^2(c) + \ldots - ac = b - aS(c) = b - a. \quad \square$$

Remark A.7.6. The following theorem is a version of Kummer's Lemma in prime characteristic.

Theorem A.7.7. *Let $K \subseteq L$ be a field extension of degree $p = \mathrm{char}\, K > 0$. $K \subseteq L$ is a Galois extension if and only if L is the splitting field of a polynomial $X^p - X - a \in K[X]$.*

Proof. Let L be the splitting field of $\alpha := X^p - X - a \in K[X]$ and $x \in L$ a root of α. Because of

$$\alpha(x+1) = (x+1)^p - x - 1 - a = x^p - x - a + 1 - 1 = \alpha(x) = 0.$$

α has pairwise distinct roots $x, x+1, \ldots, x+p-1$. According to Artin, $K \subseteq L$ is a Galois extension.

Now conversely, let $K \subseteq L$ be a Galois extension with $G := \mathrm{Gal}(L|K) = \langle \sigma \rangle$. Because of $\sum_{\tau \in G} \tau(1) = p = 0$, there exists by Hilbert's Theorem 90 an $x \in L$ with $1 = x - \sigma(x)$. In particular, $x \notin L^G = K$ and $L(x) = K$. Because of

$$a := \sigma(x^p - x) = \sigma(x)^p - \sigma(x) = (x-1)^p - x + 1 = x^p - x \in L^G = K$$

L is the splitting field of $X^p - X - a \in K[X]$. $\square$

Lemma A.7.8. *Let K be a field of characteristic $p > 0$ and $a \in K \setminus \{b^p : b \in K\}$. Then $X^{p^k} - a$ is irreducible in $K[X]$ for every $k \in \mathbb{N}$.*

Proof. Let $\alpha := X^{p^k} - a \in K[X]$ be reducible, say $\alpha = \beta\gamma$ with wlog. monic $\beta, \gamma \in K[X] \setminus K$. For a root x of α in a splitting field, it then holds that

$$\beta \mid \alpha = X^{p^k} - a = X^{p^k} - x^{p^k} = (X - x)^{p^k}.$$

Therefore $\beta = (X - x)^s$ with $0 < s < p^k$. Let $s = p^l t$ with $p \nmid t$ and $l < k$. Then

$$\beta = (X^{p^l} - x^{p^l})^t = X^s - tx^{p^l} X^{p^l(t-1)} + \ldots$$

with $-tx^{p^l} \in K$. Because $p \nmid t$, it follows that $x^{p^l} \in K$. Thus $a = (x^{p^l})^{p^{k-l}} \in \{b^p : b \in K\}$. □

Lemma A.7.9. *Let K be a field in which $X^2 + 1$ is irreducible. Furthermore, let every element in a splitting field of $X^2 + 1$ be a square. Then* $\operatorname{char} K = 0$ *and every sum of squares in K is again a square.*

Proof. Let L be a splitting field of $X^2 + 1$ and $x \in L$ with $x^2 = -1$. It suffices to show that the sum of two squares is a square. For $a, b \in K$ there exist $c, d \in K$ with $a + bx = (c + dx)^2 = c^2 - d^2 + 2cdx$. Thus $a = c^2 - d^2$ and $b = 2cd$. This shows

$$a^2 + b^2 = (c^2 - d^2)^2 + (2cd)^2 = (c^2 + d^2)^2.$$

In the case $\operatorname{char} K = p > 0$, $-1 = 1^2 + \ldots + 1^2$ ($p-1$ summands) would be a square. Thus $\operatorname{char} K = 0$. □

Theorem A.7.10 (Artin-Schreier)**.** *Let $K \subsetneq L$ be a finite field extension and L be algebraically closed. Then $|L : K| = 2$ and* $\operatorname{char} K = 0$*. Furthermore, there exists a $z \in L$ with $L = K(z)$ and $z^2 = -1$.*

Proof. We first show that K is perfect. Let $\operatorname{char} K = p > 0$ and $a \in K$. If a is not a p-th power (i.e., not in the image of the Frobenius homomorphism), then $\alpha := X^{p^k} - a$ is irreducible in $K[X]$ for all $k \in \mathbb{N}$ according to Lemma A.7.8. On the other hand, α has a root x in the algebraically closed field L. This yields the contradiction

$$p^k = |K(x) : K| \leq |L : K| < \infty \qquad \forall k \in \mathbb{N}.$$

Thus K is perfect and $K \subseteq L$ is separable. According to Exercise II.23, $K \subseteq L$ is normal and therefore a Galois extension. Let $G := \operatorname{Gal}(L|K)$.

Case 1: $p := |L : K| = |G| \in \mathbb{P}$.
Let $G = \langle\sigma\rangle$. Assume first that $\operatorname{char} K = p$. According to Theorem A.7.7, $L = K(x)$ with $a := x^p - x \in K$. Since L is algebraically closed, there exists a $y \in L$ with $y^p - y = ax^{p-1}$. We write $y = y_0 + y_1 x + \ldots + y_{p-1}x^{p-1}$ with $y_0, \ldots, y_{p-1} \in K$. Then

$$ax^{p-1} = y^p - y = \sum_{i=0}^{p-1}(y_i^p x^{ip} - y_i x^i) = \sum_{i=0}^{p-1}(y_i^p (x + a)^i - y_i x^i) = (y_{p-1}^p - y_{p-1})x^{p-1} + \ldots.$$

A comparison of coefficients yields $a = y_{p-1}^p - y_{p-1}$. But then y_{p-1} would be a root of $X^p - X - a$ and one would have the contradiction $L = K(x) = K(y_{p-1}) = K$. Thus $\operatorname{char} K \neq p$ and $X^p - 1 \neq (X - 1)^p$ in $K[X]$. The algebraically closed field L consequently possesses a primitive p-th root of unity ζ. Because of $X^p - 1 = (X - 1)(X^{p-1} + \ldots + 1)$, we have $|K(\zeta) : K| \leq p - 1$ and on the other hand $|K(\zeta) : K| \,\big|\, |L : K| = p$. This shows $\zeta \in K$. According to Lemma I.14.1, there exists a $b \in L$ with

$$x := b + \zeta\sigma(b) + \zeta^2\sigma^2(b) + \ldots + \zeta^{p-1}\sigma^{p-1}(b) \neq 0.$$

Because of $\sigma(x) = \zeta^{-1}x \neq x$, we have $L = K(x)$. Furthermore, $x^p = \zeta^{-p}x^p = \sigma(x)^p = \sigma(x^p) \in L^G = K$. We choose $y \in L$ with $y^p = x$. Then $\sigma(y)^{p^2} = \sigma(y^{p^2}) = \sigma(x^p) = x^p = y^{p^2}$, i. e. $\sigma(y) = zy$ with $z^{p^2} = 1$. It holds that $z^p \in \langle\zeta\rangle \subseteq K$. In the case $z^p = 1$, we would have

$$x = y^p = \sigma(y)^p = \sigma(y^p) \in L^G = K.$$

Thus z is a primitive p^2-th root of unity. Because of $(\sigma(z)z^{-1})^p = \sigma(z^p)z^{-p} = 1$, there exists a $k \in \mathbb{Z}$ with $\sigma(z) = z^{1+pk}$. From $\sigma(y) = zy$ it now follows that

$$y = \sigma^p(y) = \sigma^{p-1}(zy) = \ldots = z\sigma(z)\ldots\sigma^{p-1}(z)y = z^{1+(1+pk)+\ldots+(1+pk)^{p-1}}y$$

and

$$0 \equiv \sum_{i=0}^{p-1}(1+pk)^i \equiv \sum_{i=0}^{p-1}(1+ipk) \equiv p + \frac{p(p-1)}{2}pk \pmod{p^2}.$$

Thus $p = 2$ and k is odd. Because of $\sigma(z) = z^{1+2k} = z^3 \neq z$, we have $L = K(z)$ with $z^2 = -1$. Since L is algebraically closed, every element in L is a square. Lemma A.7.9 shows $\operatorname{char} K = 0$ and we are finished.

Case 2: $|L : K| \notin \mathbb{P}$.
Assume first that $|G|$ has an odd prime divisor p. According to Cauchy, there exists a $\sigma \in G$ of order p. For K^σ instead of K, Case 1 now yields a contradiction. Thus $|G|$ is a power of 2. According to Sylow, G has a subgroup H of order 4. By replacing K with L^H, we can assume $|G| = |L : K| = 4$. Then there exists a $\sigma \in G$ of order 2. Case 1 with K^σ instead of K shows $L = K^\sigma(z)$ with $z^2 = -1$. Now one can also apply Case 1 with $K(z)$ instead of K. This yields $L = K(z, w)$ with $w^2 = -1 = z^2$. But then $w = \pm z \in K(z)$. Contradiction. □

Example A.7.11. The extension $\mathbb{R} \subseteq \mathbb{C}$ satisfies the Artin-Schreier condition.

Corollary A.7.12. *Let K be an algebraically closed field and $H \leq \operatorname{Aut}(K)$ with $|H| < \infty$. Then $|H| \leq 2$ and in the case* $\operatorname{char} K > 0$ *even $H = 1$.*

Proof. According to Artin, $K^H \subseteq K$ is a Galois extension. Artin-Schreier shows $|H| = |K : K^H| \leq 2$ and $K = K^H$ if $\operatorname{char} K > 0$. □

Remark A.7.13. Complex conjugation is by far not the only automorphism on $\mathbb{C}$ of order 2. In fact, there are infinitely many conjugacy classes of elements of order 2 in $\operatorname{Aut}(\mathbb{C})$.[1]

[1] See [B. Schnor, *Involutions in the Group of Automorphisms of an Algebraically Closed Field*, J. Algebra 152 (1992), 520–524]

A.8 Separable Algebras

Remark A.8.1. We take the characterization of separable field extensions in Theorem III.7.8 as an occasion to define separable algebras. It turns out that these are exactly the strongly symmetric algebras defined in chapter II.13. In this way, one obtains new applications for the Wedderburn-Malcev Theorem. We also improve the Skolem-Noether Theorem. As usual, we consider finite-dimensional algebras over a field K.

Theorem A.8.2. *For every K-algebra A there exists a finite field extension $K \subseteq L$ and $n_1, \ldots, n_k \in \mathbb{N}$ with $A_L/\mathrm{J}(A_L) \cong L^{n_1 \times n_1} \times \ldots \times L^{n_k \times n_k}$.*

Proof. Let $J := \mathrm{J}(A)$ and $A/J \cong D_1^{n_1 \times n_1} \otimes \ldots \otimes D_1^{n_k \times n_k}$ with division algebras $D_1, \ldots, D_k$. We argue by $d := \sum_{i=1}^{k} \dim D_i$. In the case $d = k$ the claim holds with $L = K$. So let wlog. $\dim D_1 > 1$ and $x \in D_1 \setminus K$ with minimal polynomial $\mu \in K[X]$. Let $L := K(x)$. Obviously $\mathrm{J}(A_L)/(L \otimes J)$ is a nilpotent ideal of $A_L/(L \otimes J)$ with semisimple factor algebra $A_L/\mathrm{J}(A_L)$. Therefore $\mathrm{J}(A_L/(L \otimes J)) = \mathrm{J}(A_L)/(L \otimes J)$. On the other hand

$$A_L/(L \otimes J) \cong L \otimes (A/J) \cong (L \otimes D_1)^{n_1 \times n_1} \times \ldots \times (L \otimes D_k)^{n_k \times n_k}.$$

Let $E_i := L \otimes D_i$ for $i = 1, \ldots, k$. From Lemma II.12.5 it follows that

$$A_L/\mathrm{J}(A_L) \cong (E_1/\mathrm{J}(E_1)) \times \ldots \times (E_k/\mathrm{J}(E_k)).$$

According to Lemma III.7.6, $L \otimes L \cong L[X]/(\mu)$ possesses the zero divisor $(X - x) + (\mu)$. Therefore $E_1 \supseteq L \otimes L$ is not a division algebra, but $\dim_L E_i = \dim_K D_i$ for $i = 1, \ldots, k$. The sum of the dimensions of the division algebras occurring in $A_L/\mathrm{J}(A_L)$ must therefore be smaller than d. The claim follows by induction. □

Definition A.8.3. A K-algebra A is called *separable*, if $A_L = L \otimes A$ is semisimple for every finite field extension $K \subseteq L$.

Example A.8.4.

(i) According to Theorem III.7.8, a finite field extension $K \subseteq L$ is separable if and only if L is a separable K-algebra. The trace map from Definition II.3.17 can be defined for arbitrary algebras. For $A = A_1 \times A_2$ and $a_i \in A_i$, it obviously holds that $S_K^A(a_1, a_2) = S_K^{A_1}(a_1) + S_K^{A_2}(a_2)$. Therefore, Theorem II.3.21 does not hold for algebras (choose $K = A_1 = \mathbb{F}_2(X^2)$ and $A_2 = \mathbb{F}_2(X)$).

(ii) Every separable algebra is semisimple and thus symmetric according to Eilenberg-Nakayama (choose $L = K$).

(iii) Let A and B be algebras such that $A \otimes B$ is separable. Then A and B are separable, because with $L \otimes (A \otimes B)$, A_L and B_L are also semisimple (Remark III.7.5). The converse is proven in Theorem A.8.12.

(iv) Every matrix algebra is separable, because $L \otimes K^{n \times n} \cong L^{n \times n}$ according to Lemma III.7.11.

(v) Let G be a finite group and $\operatorname{char} K \nmid |G|$. According to Maschke, $L \otimes KG \cong LG$ is semisimple for all $K \subseteq L$. Therefore, KG is separable.

Theorem A.8.5. *For every K-algebra A, the following statements are equivalent:*

(1) A is separable.

(2) There exists a finite field extension $K \subseteq L$ and $n_1, \ldots, n_k \in \mathbb{N}$ with

$$A_L \cong L^{n_1 \times n_1} \times \ldots \times L^{n_k \times n_k}.$$

(3) $A \otimes A^o$ is semisimple.

(4) Every A-A-bimodule is semisimple.

(5) There exist simple algebras $A_1, \ldots, A_k$ with $A \cong A_1 \times \ldots \times A_k$, such that $\mathrm{Z}(A_1), \ldots, \mathrm{Z}(A_k)$ are separable field extensions over K.

Proof.

(1)⇒(2): Follows from Theorem A.8.2.

(2)⇒(3): As is well known, $L^{n\times n} \to (L^{n\times n})^o$, $x \mapsto x^{\mathrm{t}}$ is an isomorphism. According to Lemma III.7.11,

$$A_L \otimes_L A_L^o \cong \bigtimes_{i,j} L^{n_i n_j \times n_i n_j}$$

is semisimple. On the other hand, $A_L \otimes_L A_L^o \cong A \otimes (L \otimes_L L) \otimes A^o \cong (A \otimes A^o)_L$. Since $(A \otimes A^o)_L$ is semisimple, $A \otimes A^o$ is also semisimple (Remark III.7.5).

(3)⇔(4): Every A-A-bimodule is an $(A \otimes A^o)$-module and therefore semisimple according to Lemma II.8.4. Conversely, $A \otimes A^o$ is semisimple by definition if the regular module is semisimple.

(3)⇒(5): Since $A \otimes A^o$ is semisimple, A is also semisimple. By Artin-Wedderburn, there exist simple algebras $A_1, \ldots, A_k$ with $A \cong A_1 \times \ldots \times A_k$. It holds that

$$0 = \mathrm{J}(A \otimes A^o) \cong \bigtimes_{i,j=1}^{k} \mathrm{J}(A_i \otimes A_j^o).$$

In particular, $A_i \otimes A_i^o$ is semisimple. By Artin-Wedderburn, $\mathrm{Z}(A_i \otimes A_i^o) \cong \mathrm{Z}(A_i) \otimes \mathrm{Z}(A_i)$ is a direct product of fields and therefore semisimple. According to Theorem III.7.8, $\mathrm{Z}(A_i)$ is separable over K for $i = 1, \ldots, k$.

(5)⇒(1): It suffices to show that $L \otimes A_i$ is semisimple for every finite field extension $K \subseteq L$. As is well known, A_i is a central-simple Z_i-algebra for $Z_i := \mathrm{Z}(A_i)$. By Noether-Jacobson, there exists a separable field extension $Z_i \subseteq L_i$ with $L_i \otimes_{Z_i} A_i \cong L_i^{n_i \times n_i}$. By assumption, $K \subseteq L_i$ is also separable. According to Theorem III.7.8, $L \otimes L_i$ is semisimple. By $z(\lambda \otimes a) := \lambda \otimes za$ for $z \in Z_i$ and $\lambda \otimes a \in L \otimes A_i$, $L \otimes A_i$ becomes a Z_i-algebra. Therefore,

$$(L \otimes A_i) \otimes_{Z_i} L_i \cong L \otimes L_i^{n_i \times n_i} \cong (L \otimes L_i)^{n_i \times n_i}$$

is also semisimple (independent of the base field). As usual, it follows that $L \otimes A_i$ is semisimple. □

Remark A.8.6. Let A be separable and $A_L \cong L^{n_1 \times n_1} \times \ldots \times L^{n_k \times n_k}$ as in Theorem A.8.5(2). For every finite field extension $L \subseteq M$, $M \otimes_L A_L \cong (M \otimes_L L) \otimes_K A \cong M \otimes_K K = A_M$ is semisimple. Therefore, A_L is separable. According to Theorem A.8.5(5), $K \subseteq L$ is separable.

Corollary A.8.7. *Every semisimple algebra over a perfect field is separable.*

Proof. Let A be semisimple over the perfect field K. According to Artin-Wedderburn, there exist simple algebras $A_1, \ldots, A_k$ with $A \cong A_1 \times \ldots \times A_k$. Since K is perfect, $\mathrm{Z}(A_1), \ldots, \mathrm{Z}(A_k)$ are separable over K. □

Corollary A.8.8. *Every central-simple algebra is separable.*

Proof. For a central-simple algebra A, $\mathrm{Z}(A) = K$ is separable over K. □

Theorem A.8.9. *An algebra A is separable if and only if A is strongly symmetric.*

Proof.

$\Longrightarrow$: Let A be separable. According to Example A.8.4, A is symmetric with respect to a bilinear form β. According to Remark A.8.6, there exists a finite separable field extension $K \subseteq L$ with $A_L \cong L^{n_1 \times n_1} \times \ldots \times L^{n_k \times n_k}$. According to Example II.13.10, A_L is strongly symmetric. Let $(e_1, \ldots, e_d)$ and $(f_1, \ldots, f_d)$ be dual bases of A with respect to β. Then $1 \otimes e_1, \ldots, 1 \otimes e_d$ is a basis of A_L and the rule $\beta_L(1 \otimes e_i, 1 \otimes e_j) := \beta(e_i, e_j)$ can be extended to a symmetric, associative, non-degenerate bilinear form of A_L. Now $(1 \otimes e_i)_i$ and $(1 \otimes f_i)_i$ are dual bases of A_L with respect to β_L. Let $1 = x_1, \ldots, x_s \in L$ be a K-basis of L. Then every element in A_L can be uniquely written in the form $x = \sum_{i=1}^{s} x_i \otimes a_i$ with $a_i \in A$. Since A_L is strongly symmetric, there exists such an x with

$$x_1 \otimes 1 = 1 = \sum_{i=1}^{d} (1 \otimes e_i) x (1 \otimes f_i) = \sum_{j=1}^{s} x_j \otimes \sum_{i=1}^{d} e_i a_j f_i = \sum_{j=1}^{s} x_j \otimes \Gamma(a_j).$$

From the uniqueness of the decomposition, it follows that $\Gamma(a_1) = 1$. Thus A is strongly symmetric.

$\Longleftarrow$: Let A be strongly symmetric with respect to a bilinear form β. For $a, b, c \in A^o$, it holds that

$$\beta(a * b, c) = \beta(ba, c) = \beta(a, cb) = \beta(a, b * c).$$

Therefore, A^o is also symmetric with respect to β. Furthermore, $A \otimes A^o$ is symmetric with respect to

$$\hat{\beta}(a_1 \otimes a_2, b_1 \otimes b_2) := \beta(a_1, b_1)\beta(a_2, b_2)$$

for $a_1, a_2, b_1, b_2 \in A$. Let (e_i) and (f_i) be dual bases of A (and A^o) with respect to β and $c \in A$ with $\Gamma(c) = 1$. Since (f_i) and (e_i) are also dual to each other, it holds that

$$\sum_{i=1}^{n} f_i c e_i = \Gamma(c) = 1.$$

The bases $(e_i \otimes e_j)$ and $(f_i \otimes f_j)$ of $A \otimes A^o$ are dual to each other with respect to $\hat{\beta}$. It holds that

$$\sum_{i,j=1}^{n} (e_i \otimes e_j)(c \otimes c)(f_i \otimes f_j) = \sum_{i,j=1}^{n} (e_i c f_i) \otimes (f_j c e_j) = \Gamma(c) \otimes \Gamma(c) = 1.$$

Therefore, $A \otimes A^o$ is strongly symmetric and semisimple according to Theorem II.13.7. □

Remark A.8.10. For algebras, it holds that

$$\text{strongly symmetric} \iff \text{separable} \implies \text{semisimple} \implies \text{symmetric.}$$

The converses are each false (Remark II.13.20 and Example A.8.4).

Corollary A.8.11. *The Wedderburn-Malcev theorem holds for every algebra A for which $A/\mathrm{J}(A)$ is separable. In particular, the theorem holds for all algebras over perfect fields.*

Proof. According to Theorem A.8.9, $A/\mathrm{J}(A)$ is strongly symmetric. □

Theorem A.8.12. *For algebras A and B, it holds that*

$$A, B \text{ separable} \iff A \times B \text{ separable} \iff A \otimes B \text{ separable.}$$

Proof. The first equivalence follows from the uniqueness of the Artin-Wedderburn decomposition and Theorem A.8.5. If $A \otimes B$ is separable, then so are A and B according to Example A.8.4. Now let A and B be separable and thus strongly symmetric. Let β_A and β_B be the corresponding bilinear forms of A and B. It is easy to show that $\beta(a_1 \otimes b_1, a_2 \otimes b_2) := \beta_A(a_1, a_2)\beta_B(b_1, b_2)$ for $a_1, a_2 \in A$ and $b_1, b_2 \in B$ defines a symmetric, associative bilinear form on $A \otimes B$. Let $(e_1, \ldots, e_k)$, $(f_1, \ldots, f_k)$ and $(x_1, \ldots, x_l)$, $(y_1, \ldots, y_l)$ be pairs of dual bases of A and B. Then $(e_i \otimes x_j)_{i,j}$ and $(f_i \otimes y_j)_{i,j}$ are dual bases of $A \otimes B$ with respect to β. In particular, β is non-degenerate. By assumption, there exist $a \in A$ and $b \in B$ with $\Gamma_A(a) = 1$ and $\Gamma(b) = 1$. It follows that

$$\Gamma_{A\otimes B}(a \otimes b) = \sum_{i=1}^{k}\sum_{j=1}^{l}(e_i \otimes x_j)(a \otimes b)(f_i \otimes y_j) = \sum_{i=1}^{k}\sum_{j=1}^{l} e_i a f_i \otimes x_j b y_j = \Gamma_A(a) \otimes \Gamma_B(b) = 1.$$

Thus $A \otimes B$ is strongly symmetric and separable. □

Lemma A.8.13. *Let A be separable and B semisimple. Then $A \otimes B$ is semisimple.*

Proof. According to Artin-Wedderburn and Lemma III.7.11, we can assume that A and B are division algebras. Since A is separable, $\mathrm{Z}(A)$ is also separable (Theorem A.8.5). According to Theorem III.7.8, $\mathrm{Z}(A) \otimes \mathrm{Z}(B) = \mathrm{Z}(A \otimes B)$ is semisimple, i.e., $\mathrm{J}(\mathrm{Z}(A \otimes B)) = 0$. From Lemma III.7.12 it follows that $\mathrm{J}(A \otimes B) = 0$. □

Remark A.8.14. As a further application of Wedderburn-Malcev, we give a new proof of Theorem III.9.42.

Theorem A.8.15 (Jordan-Chevalley decomposition)**.** *Let K be perfect and $a \in K^{m\times m}$. Then there exist uniquely determined matrices $d, n \in K^{m\times m}$ with the following properties:*

(i) $a = d + n$ *and* $dn = nd$.

(ii) d *is diagonalizable over* $\overline{K}$.

(iii) n *is nilpotent.*

Furthermore, there exists $\alpha \in K[X]$ with $\alpha(a) = d$.

Proof. We consider the commutative K-algebra

$$A := K[a] = \{\alpha(a) : \alpha \in K[X]\}.$$

According to Wedderburn-Malcev, there exists a separable algebra $D \cong A/\mathrm{J}(A)$ with $A = D \oplus \mathrm{J}(A)$. Let $d \in D$ and $n \in \mathrm{J}(A)$ with $a = d + n$. Obviously n is nilpotent and $dn = nd$, since A is commutative. According to Artin-Wedderburn, $D_{\overline{K}} = \overline{K} \otimes D \cong K^k$ for some $k \leq m$. Therefore, there exist pairwise orthogonal idempotents $e_1, \ldots, e_k \in D_{\overline{K}}$ with $1_m = e_1 + \ldots + e_k$. One can refine this sum into pairwise orthogonal primitive idempotents of $\overline{K} \otimes K^{m\times m} = \overline{K}^{m\times m}$. According to Theorem II.8.22, there exists $s \in \mathrm{GL}(n, \overline{K})$ with $sD_{\overline{K}}s^{-1} = \bigoplus_{i=1}^{k} \overline{K}1_{a_i}$ and $a_1 + \ldots + a_k = m$. In particular, d is diagonalizable over $\overline{K}$.

Let also $a = d' + n'$ with $d'n' = n'd'$, n' nilpotent and d' diagonalizable over $\overline{K}$. Then d' commutes with $d' + n' = a$. Thus d' also commutes with all elements in $A = K[a]$. According to linear algebra, d and d' are diagonalizable with respect to a common basis over $\overline{K}$. Thus $d - d'$ is also diagonalizable over $\overline{K}$. At the same time, however, $d - d' = n' - n$ is nilpotent. This shows $d' = d$ and $n' = n$. The last assertion follows from the construction. □

Theorem A.8.16. *Let A and B be algebras such that $A/\mathrm{J}(A)$ is separable. Then*

$$\boxed{\mathrm{J}(A \otimes B) = \mathrm{J}(A) \otimes B + A \otimes \mathrm{J}(B).}$$

Proof. The nilpotent ideal $I := \mathrm{J}(A) \otimes B + A \otimes \mathrm{J}(B)$ lies in the kernel of the epimorphism $A \otimes B \to (A/\mathrm{J}(A)) \otimes (B/\mathrm{J}(B))$, $a \otimes b \mapsto (a + \mathrm{J}(A)) \otimes (b + \mathrm{J}(B))$. According to Lemma A.8.13, $(A/\mathrm{J}(A)) \otimes (B/\mathrm{J}(B))$ is semisimple and $I = \mathrm{J}(A \otimes B)$. □

Lemma A.8.17. *Let A and B be K-algebras and B central-simple. Suppose the A-B-bimodules M and N are isomorphic as A-modules. Then M and N are also isomorphic as bimodules.*

Proof. Let $\varphi\colon M \to N$ be an isomorphism of A-modules. Let L be a splitting field for B. Then $M_L := L \otimes M$ and $N_L := L \otimes N$ are A_L-modules and the map $M_L \to N_L$, $\lambda \otimes m \mapsto \lambda \otimes \varphi(m)$ is an isomorphism. Furthermore, M_L and N_L are A_L-B_L bimodules with

$$(\lambda \otimes a)(\mu \otimes m)(\rho \otimes b) := \lambda\mu\rho \otimes amb$$

for $\lambda, \mu, \rho \in L$, $a \in A$, $b \in B$ and $m \in M$ (analogously for N). One can thus view M_L and N_L as modules over the algebra $A_L \otimes_L B_L^o \cong (A \otimes B^o)_L$. Suppose we have already shown the claim for L instead of K. Then there exists an isomorphism $M_L \to N_L$ of $(A \otimes B^o)_L$-modules. We can also consider M_L and N_L as isomorphic $A \otimes B^o$-modules, where $A \otimes B^o$ acts trivially on the factor L in each case. Then

$$M^{|L:K|} \simeq_{A\otimes B^o} K^{|L:K|} \otimes M \simeq_{A\otimes B^o} M_L \simeq N_L \simeq_{A\otimes B^o} N^{|L:K|}.$$

From Krull-Schmidt it follows that $M \simeq_{A\otimes B^o} N$. We can therefore replace K by L.

Thus $B \cong K^{n\times n}$ and $A \otimes B^o \cong A^{n\times n}$. We must show that M and N are isomorphic $A^{n\times n}$-modules. The action is given by

$$(a_{ij})x := \Big(\sum_{i,j=1}^{n} a_{ij} \otimes E_{ij}\Big)x = \sum_{i,j=1}^{n} a_{ij} x E_{ij}$$

for $(a_{ij}) \in A^{n\times n}$ and $x \in M$. As is well known, $1_n = E_{11} + \ldots + E_{nn}$ is a decomposition into pairwise orthogonal primitive idempotents. Therefore $M = M_1 \oplus \ldots \oplus M_n$ with $M_i := ME_{ii}$ is a direct decomposition of A-modules. Obviously

$$\varphi_{ij}\colon M_i \to M_j, \qquad x \mapsto xE_{ij} = xE_{ij}E_{jj}$$

is a homomorphism of A-modules. Because of $\varphi_{ji} \circ \varphi_{ij} = \mathrm{id}_{M_i}$, φ_{ij} is an isomorphism. It follows that $(M_1)^n \simeq_A M \simeq_A N \simeq_A (N_1)^n$. By Krull-Schmidt there exists an isomorphism $\varphi_1\colon M_1 \to N_1$. We consider

$$\psi\colon M \to N, \qquad x \mapsto \sum_{k=1}^{n} \varphi_1(xE_{k1})E_{1k}.$$

For $(a_{ij}) \in A^{n\times n}$ it holds that

$$\begin{aligned}\psi((a_{ij})x) &= \sum_{k=1}^{n}\sum_{i,j=1}^{n} a_{ij}\varphi_1(xE_{ij}E_{k1})E_{1k} = \sum_{k=1}^{n}\sum_{i=1}^{n} a_{ik}\varphi_1(xE_{i1})E_{1k} = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ki}\varphi_1(xE_{k1})E_{1i}\\ &= \sum_{i,k=1}^{n} a_{ki}\sum_{j=1}^{n}\varphi_1(xE_{j1})E_{1j}E_{ki} = (a_{ij})\psi(x),\end{aligned}$$

i. e. ψ is $A^{n\times n}$-linear. For $x \in \mathrm{Ker}(\psi)$ it holds that

$$x = xE_{11} + \ldots + xE_{nn} = xE_{11} + xE_{21}E_{12} + \ldots + xE_{n1}E_{1n} = 0,$$

i. e. ψ is injective. Because of $\dim_K M = \dim_K N$, ψ is an isomorphism. □

Theorem A.8.18 (Skolem-Noether)**.** *Let A and B be K-algebras and B be central-simple. Then for all homomorphisms $f, g\colon B \to A$ there exists an $a \in A^\times$ such that $f(x) = ag(x)a^{-1}$ for all $x \in B$.*

Proof. As in the proof of Theorem III.7.20, we consider the $A \otimes B^o$-modules $M_f = A = M_g$ with

$$(a \otimes b)m := amf(b) \qquad (a \in A, b \in B, m \in M)$$

(analogously for M_g). As there, it suffices to show that M_f and M_g are isomorphic. Since M_f and M_g are regular as A-modules, the assertion follows from Lemma A.8.17. □

A.9 Profinite groups

Remark A.9.1. In Definition III.11.33, we defined the Krull topology on Galois groups of (infinite) Galois extensions. In this section, we show how abstract groups with topological properties can be characterized as Galois groups. For such (profinite) groups, we prove generalizations of the theorems of Lagrange and Sylow.

Definition A.9.2. Let M be a non-empty set. A family of subsets $\mathcal{F} \subseteq \mathcal{P}(M)$ is called a *filter* of M if:

- $\varnothing \neq \mathcal{F} \neq \mathcal{P}(M)$.
- $A, B \in \mathcal{F} \Longrightarrow A \cap B \in \mathcal{F}$.
- $A \supseteq B \in \mathcal{F} \Longrightarrow A \in \mathcal{F}$.

If $\mathcal{F}$ is maximal with respect to inclusion, then $\mathcal{F}$ is called an *ultrafilter*.

Remark A.9.3. The first condition in Definition A.9.2 is equivalent to $\varnothing \notin \mathcal{F}$ and $M \in \mathcal{F}$.

Example A.9.4.

(i) For every subset $\varnothing \neq A \subseteq M$,

$$\mathcal{F}(A) := \{B \subseteq M : A \subseteq B\}$$

is a filter. For $x \in M$, let $\mathcal{F}(x) := \mathcal{F}(\{x\})$.

(ii) The set Ω of all filters containing a given filter $\mathcal{F}$ is ordered by $\subseteq$. It is easy to see that the union of a totally ordered subset of Ω is again a filter. By Zorn's Lemma, there always exists an ultrafilter containing $\mathcal{F}$.

Lemma A.9.5. *For every filter $\mathcal{F}$ of $M \neq \varnothing$, the following statements are equivalent:*

(1) $\mathcal{F}$ is an ultrafilter.

(2) For all $A \subseteq M$, either $A \in \mathcal{F}$ or $M \setminus A \in \mathcal{F}$.

(3) For all $A_1, \ldots, A_n \subseteq M$ with $A_1 \cup \ldots \cup A_n \in \mathcal{F}$, there exists an i such that $A_i \in \mathcal{F}$.

Proof.

(1)⇒(2): Let

$$\mathcal{G} := \big\{B \subseteq M : \exists F \in \mathcal{F} : A \cap F \subseteq B\big\}.$$

If $\varnothing \in \mathcal{G}$, then there exists an $F \in \mathcal{F}$ with $F \subseteq M \setminus A$. Then $M \setminus A \in \mathcal{F}$ also holds. Otherwise, $\mathcal{G}$ is a filter containing $\mathcal{F}$. Since $\mathcal{F}$ is an ultrafilter, $A = A \cap M \in \mathcal{G} = \mathcal{F}$ holds.

(2)⇒(3): Let us assume $A_i \notin \mathcal{F}$ for $i = 1, \ldots, n$. By (2), $M \setminus A_i \in \mathcal{F}$ holds for $i = 1, \ldots, n$. Since $\mathcal{F}$ is a filter, the contradiction follows:

$$\varnothing = \Big(\bigcup_{i=1}^{n} A_i\Big) \cap \Big(M \setminus \bigcup_{i=1}^{n} A_i\Big) = \Big(\bigcup_{i=1}^{n} A_i\Big) \cap \bigcap_{i=1}^{n} (M \setminus A_i) \in \mathcal{F}.$$

(3)⇒(1): Suppose $\mathcal{F}$ is not an ultrafilter. Then there exists a filter $\mathcal{G} \supsetneq \mathcal{F}$ and an $A \in \mathcal{G} \setminus \mathcal{F}$. Because of $A \cup (M \setminus A) \in \mathcal{F}$, it follows from (3) that $M \setminus A \in \mathcal{F} \subseteq \mathcal{G}$. But then $\varnothing = A \cap (M \setminus A) \in \mathcal{G}$ would hold. □

Definition A.9.6. Let M be a topological space (cf. Lemma III.11.34).

- M is called a *Hausdorff space*, if for any two distinct points $x, y \in M$ there exist disjoint open sets $U_x, U_y \subseteq M$ with $x \in U_x$ and $y \in U_y$ (*separation axiom*).
- $K \subseteq M$ is called *compact*, if from every cover $K \subseteq \bigcup_{i \in I} U_i$ with open sets U_i, a "subcover" $K \subseteq \bigcup_{j \in J} U_j$ with $|J| < \infty$ can be selected. If M itself is compact, one speaks of a compact topological space.
- $Z \subseteq M$ is called *connected*, if for any two open sets $U, V \subseteq M$ with $Z = (U \cap Z) \dot\cup (V \cap Z)$ it holds: $Z \subseteq U$ or $Z \subseteq V$. If every connected subset of M has at most one element, then M is called *totally disconnected*.
- A map $f\colon A \to B$ between topological spaces A and B is called *continuous*, if for every open set $U \subseteq B$, $f^{-1}(U)$ is also open. If f is bijective and f, f^{-1} are continuous, then f is called a *homeomorphism*.

Remark A.9.7.

(i) Every metric space (M, d) is a Hausdorff space, because for distinct $x, y \in M$, the open ϵ-balls around x and y with $\epsilon := \frac{1}{2} d(x, y)$ are disjoint by the triangle inequality.

(ii) If $K \subseteq M$ is compact and $A \subseteq K$ is closed, then A is also compact, because if $A \subseteq \bigcup_{i \in I} U_i$ is an open cover, then so is $K \subseteq (M \setminus A) \cup \bigcup_{i \in I} U_i$.

(iii) A map $f\colon A \to B$ is continuous if and only if preimages of closed sets are closed, because $A \setminus f^{-1}(C) = f^{-1}(B \setminus C)$ for all $C \subseteq B$.

(iv) The composition of continuous maps is obviously continuous.

(v) If $f\colon A \to B$ is continuous and $K \subseteq A$ is compact, then $f(K)$ is also compact, because if $f(K) \subseteq \bigcup_{i \in I} U_i$ is an open cover, then so is $K \subseteq \bigcup_{i \in I} f^{-1}(U_i)$.

(vi) In contrast to homomorphisms, the inverse map of a bijective continuous map is not automatically continuous. Consider for example $A = B = \mathbb{N}$ with the discrete topology on A (every subset is open) and the trivial topology on B (only $\varnothing$ and B are open). Then $f\colon A \to B$, $a \mapsto a$ is continuous, but f^{-1} is not.

Lemma A.9.8. *Every compact subset of a Hausdorff space is closed.*

Proof. Let K be compact in the Hausdorff space M. Let $x \in M \setminus K$. For all $a \in K$ there exist disjoint open sets $U_a, V_a \subseteq M$ with $a \in U_a$ and $x \in V_a$. Due to compactness, there exist $a_1, \ldots, a_n \in K$ with $K \subseteq U_{a_1} \cup \ldots \cup U_{a_n}$. Now $V_{a_1} \cap \ldots \cap V_{a_n}$ is an open set in $M \setminus K$ containing x. Thus $M \setminus K$ is open and K is closed. □

Corollary A.9.9. *Let A be a compact space and B a Hausdorff space. Then every continuous bijection $A \to B$ is a homeomorphism.*

Proof. Let $f\colon A \to B$ be a continuous bijection and $U \subseteq A$ closed. According to Remark A.9.7, U and $f(U)$ are compact. According to Lemma A.9.8, $f(U)$ is closed. Therefore f^{-1} is continuous. □

Definition A.9.10. A filter $\mathcal{F}$ of a topological space M *converges* to $x \in M$ if all open subsets in $\mathcal{F}(x)$ also lie in $\mathcal{F}$.

Lemma A.9.11. *A topological space M is compact if and only if every ultrafilter of M converges to a point.*

Proof. Let M be compact. Suppose an ultrafilter $\mathcal{F}$ of M converges to no point. For all $x \in M$ there then exists an open set $U_x \notin \mathcal{F}$ with $x \in U_x$. Since M is compact, there exists a finite set $X \subseteq M$ with $M = \bigcup_{x \in X} U_x$. This contradicts Lemma A.9.5.

Now assume that M is not compact. Then there exists an open cover $M = \bigcup_{i \in I} U_i$ without a finite subcover. Consequently,

$$\left\{A \subseteq M : \exists i_1, \ldots, i_n \in I : M \setminus A \subseteq U_{i_1} \cup \ldots \cup U_{i_n}\right\}$$

is a filter that lies in an ultrafilter $\mathcal{F}$. Suppose $\mathcal{F}$ converges to x. Let $i \in I$ with $x \in U_i$. Then $\varnothing = U_i \cap (M \setminus U_i) \in \mathcal{F}$ would hold. □

Definition A.9.12. Let G be a group and at the same time a topological space.

- One obtains the *product topology* on $G \times G$ by defining open sets as arbitrary unions of products of the form $U \times V$ with open sets $U, V \subseteq G$.
- One calls G *topological*, if the map $G \times G \to G$, $(x, y) \mapsto xy^{-1}$ is continuous with respect to the corresponding topologies.
- A topological group G is called *profinite*, if G is compact and totally disconnected.

Theorem A.9.13. *For every Galois extension $K \subseteq L$, $\mathrm{Gal}(L|K)$ is profinite with respect to the Krull topology.*

Proof. Let $G := \mathrm{Gal}(L|K)$ and $\varphi\colon G \times G \to G$, $(x, y) \mapsto xy^{-1}$. Let $\mathcal{N}$ be the set of open normal subgroups in G as in Definition III.11.33. Every open set $U \subseteq G$ has the form $U = \bigcup_{i \in I} g_i N_i$ with $g_i \in G$ and $N_i \in \mathcal{N}$ for $i \in I$. Then

$$\varphi^{-1}(U) = \bigcup_{i \in I} \varphi^{-1}(g_i N_i) = \bigcup_{i \in I} \bigcup_{x \in G} (g_i x N_i, x N_i)$$

is open and φ is continuous. Thus G is a topological group.

Now let $Z \subseteq G$ be connected. Suppose there exist distinct $x, y \in Z$. According to Remark III.11.32, $\bigcap_{N \in \mathcal{N}} N = 1$ holds. Therefore there exists an $N \in \mathcal{N}$ with $x^{-1}y \notin N$. But then $U := xN$ and $V := \bigcup_{gN \neq xN} gN$ would be disjoint open sets with $x \in U$, $y \in V$ and $Z = (Z \cap U) \cup (Z \cap V)$. Thus G is totally disconnected.

For the proof of the compactness of G, it suffices to show that every ultrafilter $\mathcal{F}$ converges to a point (Lemma A.9.11). For every $x \in L$ there exists a finite Galois extension $K \subseteq M$ with $x \in M$. Here $N := \mathrm{Gal}(L|M)$ has finite index in G. According to Lemma A.9.5, $gN \in \mathcal{F}$ holds for some $g \in G$. Let also $K \subseteq \tilde{M}$ be a finite Galois extension with $x \in \tilde{M}$ and $\tilde{N} := \mathrm{Gal}(L|\tilde{M})$. Let $\tilde{g}\tilde{N} \in \mathcal{F}$. Since $\mathcal{F}$ is a filter, $gN \cap \tilde{g}\tilde{N} \neq \varnothing$ holds. For $\sigma \in gN \cap \tilde{g}\tilde{N}$ it holds that $\sigma^{-1}g(x) = x = \sigma^{-1}h(x)$ and $g(x) = h(x)$. In this way one obtains a well-defined map $\gamma\colon L \to L$, $x \mapsto g(x)$. One easily shows $\gamma \in G$. Let $\gamma \in gN$. Then $gN = \gamma N$ holds. As above, there exists an $h \in G$ with $hN \in \mathcal{F}$. For $x \in L^N$ it holds that $h(x) = \gamma(x)$. This shows $h^{-1}\gamma \in N$ and $gN = hN \in \mathcal{F}$. Thus $\mathcal{F}$ converges to γ. □

Lemma A.9.14. *For every profinite group G the following holds:*

(i) For $x \in G$, the maps $G \to G$, $g \mapsto xg$, $G \to G$, $g \mapsto gx$ and $G \to G$, $g \mapsto g^{-1}$ are homeomorphisms.

(ii) Every finite subset of G is closed.

(iii) G is a Hausdorff space.

(iv) A subgroup $H \leq G$ is open if and only if H is closed and $|G : H| < \infty$.

(v) Every open, closed subset $U \subseteq G$ with $1 \in U$ contains an open normal subgroup.

(vi) The intersection of all open normal subgroups of G is trivial.

Proof.

(i) Every open set in $G \times G$ is a union of sets of the form $U \times V$ with $U, V \subseteq G$ open. The preimage of $U \times V$ under the map $\varphi\colon G \to G \times G$, $g \mapsto (g, x^{-1})$ is either empty or U. Therefore φ is continuous. By definition, $\psi\colon G \times G \to G$, $(g, h) \mapsto gh^{-1}$ is also continuous. Thus $\psi \circ \varphi\colon G \to G$, $g \mapsto gx$ is continuous. Analogously, $\varphi\colon G \to G \times G$, $g \mapsto (1, g)$ and $\psi \circ \varphi\colon G \to G$, $g \mapsto g^{-1}$ are also continuous. This shows that $\varphi\colon G \to G \times G$, $g \mapsto (x, g^{-1})$ and $\psi \circ \varphi\colon G \to G$, $g \mapsto xg$ are also continuous. It is clear that in all cases the inverse maps are also continuous.

(ii) Let $x, y \in G$ be distinct. Since $\{x, y\}$ is not connected, there exists an open set $U_y \subseteq G$ containing y but not x. Now $\{x\} = \bigcap_{y \in G \setminus \{x\}} G \setminus U_y$ is closed. As a finite union of single-element subsets, every finite subset is closed.

(iii) Let $x, y \in G$ be distinct. According to (ii), $\{xy^{-1}\}$ is closed. Therefore there exists an open set $U \subseteq G$ with $1 \in U$ and $xy^{-1} \notin U$. Since the preimage of U under $G \times G \to G$, $(g, h) \mapsto gh^{-1}$ is open, there exist open sets $V, W \subseteq G$ with $1 \in V \cap W$ and $VW^{-1} \subseteq U$. From $x^{-1}y \notin VW^{-1}$ it follows that $xV \cap yW = \varnothing$ with $x \in xV$ and $y \in yW$. According to (i), xV and yW are open.

(iv) Let H be open. Then $G \setminus H = \bigcup_{g \in G \setminus H} gH$ is open, i. e. H is closed. Since the open cover $G = \bigcup_{g \in G} gH$ has a finite subcover, $|G : H| < \infty$. Conversely, let H be closed with $|G : H| < \infty$. Then $G \setminus H$ is closed as a finite union of closed cosets. Thus H is open.

(v) Let $x \in U$. Since $G \times G \to G$, $(g, h) \mapsto gh$ is continuous, there exist open sets $L_x, R_x \subseteq G$ with $1 \in L_x \cap R_x =: S_x$ and $L_x R_x \subseteq Ux^{-1}$. Now $S_x S_x \subseteq Ux^{-1}$ holds. Since G is compact, the closed set U is also compact. From the open cover $U \subseteq \bigcup_{x \in U} S_x x$, one can choose a finite subcover $U \subseteq \bigcup_{i=1}^{n} S_{x_i} x_i$. Now $S := S_{x_1} \cap \ldots \cap S_{x_n}$ is also open and $1 \in S$. Furthermore,

$$SU \subseteq \bigcup_{i=1}^{n} S S_{x_i} x_i \subseteq \bigcup_{i=1}^{n} U x_i^{-1} x_i \subseteq U.$$

Because $1 \in U$, it follows that $S \subseteq U$. Finally, let $T := S \cap S^{-1}$ and $H := \bigcup_{i=1}^{\infty} T^i$. It is easily shown that H is a subgroup of G. Because $T^i = \bigcup_{t \in T^{i-1}} tT$, T^i and H are open. From $SU \subseteq U$ it

follows that $H \subseteq U$. According to (iv), $|G : H| < \infty$. Therefore the core $N := H_G$ also has finite index (Exercise I.17). Because $|G : \mathrm{N}_G(H)| \leq |G : H| < \infty$, N is open as a finite intersection of conjugates of H with $N \subseteq U$.

(vi) Let $1 \neq x \in G$. Since $\{1, x\}$ is disconnected, there exists an open, closed subset $U_x \subseteq G$ with $1 \in U_x$ and $x \notin U_x$. According to (v), there exists an open normal subgroup $N_x \trianglelefteq G$ with $N_x \subseteq U_x$. Therefore $\bigcap_{x \in G \setminus \{1\}} N_x = 1$. □

Theorem A.9.15 (Leptin)**.** *Every profinite group is the Galois group of a Galois extension with respect to the Krull topology.*

Proof. According to Lemma A.9.14, there exists a family $\mathcal{N}$ of open normal subgroups with $\bigcap_{N \in \mathcal{N}} N = 1$ and $|G : N| < \infty$ for all $N \in \mathcal{N}$. Therefore, G acts faithfully on the disjoint union $\Omega := \dot{\bigcup}_{N \in \mathcal{N}} G/N$ by left multiplication. Let K be an arbitrary field and $L := K(X_\omega : \omega \in \Omega)$. By permutation of the X_ω, G acts on L. Let $M := L^G$ and $\Gamma \colon G \to \mathrm{Gal}(L|M)$ be the canonical monomorphism. For $\omega = gN \in \Omega$, the orbit of X_ω under G has length $|G : N| < \infty$. Therefore, X_ω is a root of the separable polynomial $\prod_{\delta \in {}^G\omega}(Y - X_\delta) \in M[Y]$. This shows that $M \subseteq L$ is a separable field extension.

Let $x \in L$ be arbitrary. Then there exists a finite subset $\Delta_x \subseteq \Omega$ with

$$M(x) \subseteq M(X_\delta : \delta \in \Delta_x) =: M(\Delta_x).$$

Wlog. let ${}^G\Delta_x = \Delta_x$. Then G induces a finite automorphism group on $M(\Delta_x)$. According to Theorem II.3.10, $M \subseteq M(\Delta_x)$ is a Galois extension. According to Theorem III.11.28, $M \subseteq L = \bigcup_{x \in L} M(\Delta_x)$ is therefore a Galois extension.

Let $M \subseteq M_1$ be an arbitrary finite Galois extension. According to Artin, $M_1 = M(x)$ for some $x \in L$. This shows

$$H := \Gamma^{-1}\big(\mathrm{Gal}(L|M(\Delta_x))\big) \subseteq \Gamma^{-1}\big(\mathrm{Gal}(L|M_1)\big) =: H_1.$$

Because $|\Delta_x| < \infty$, H is the intersection of finitely many $N \in \mathcal{N}$. In particular, H is open. As a union of cosets of H, H_1 is also open. For $\sigma \in \mathrm{Gal}(L|M)$, $\Gamma^{-1}(\sigma\mathrm{Gal}(L|M_1))$ is either empty or a coset of H_1. This shows that Γ is continuous. Consequently, $\Gamma(G)$ is compact according to Remark A.9.7 and therefore closed in $\mathrm{Gal}(L|M)$ according to Lemma A.9.8, because $\mathrm{Gal}(L|M)$ is a Hausdorff space according to Lemma A.9.14. Krull's theorem shows $\Gamma(G) = \mathrm{Gal}(L|L^{\Gamma(G)}) = \mathrm{Gal}(L|M)$, i. e. Γ is a bijection. Due to Corollary A.9.9, Γ is a homeomorphism. □

Corollary A.9.16. *In every profinite group, every open subset is a union of cosets of open normal subgroups.*

Proof. According to Leptin, every profinite group is a Galois group and one can use the definition of the Krull topology (Definition III.11.33). □

Lemma A.9.17. *Let G be profinite and $\mathcal{N}$ the set of open normal subgroups of G. For every closed subgroup $H \leq G$, $H = \bigcap_{N \in \mathcal{N}} HN$ holds.*

Proof. Certainly $H \subseteq HN$ for all $N \in \mathcal{N}$. Conversely, let $x \in G \setminus H$. Because $xH \cap \bigcap_{N \in \mathcal{N}} N = xH \cap \{1\} = \varnothing$, $G = (G \setminus xH) \cup \bigcup_{N \in \mathcal{N}} G \setminus N$ is an open cover. Since G is compact, there exist $N_1, \ldots, N_k \in \mathcal{N}$ with $G = (G \setminus xH) \cup G \setminus (N_1 \cap \ldots \cap N_k)$. For $N := N_1 \cap \ldots \cap N_k \in \mathcal{N}$, it holds that $xH \subseteq G \setminus N$. This shows $x \notin HN$. □

Definition A.9.18.

- Let Π be the set of all mappings $\mathbb{P} \to \mathbb{N}_0 \cup \{\infty\}$. We write $\pi \in \Pi$ as a formal product $\pi = \prod_{p\in\mathbb{P}} p^{\pi(p)}$. For $\pi_i \in \Pi$ with $i \in I$ let

$$\pi_i \mid \pi_j \ :\Longleftrightarrow\ \forall p \in \mathbb{P} : \pi_i(p) \le \pi_j(p),$$
$$\prod_{i\in I} \pi_i = \prod_{p\in\mathbb{P}} p^{\sum_{i\in I} \pi_i(p)},$$
$$\operatorname{lcm}(\pi_i : i \in I) = \prod_{p\in\mathbb{P}} p^{\sup\{\pi_i(p):i\in I\}}$$

  with the obvious rule $k + \infty = \infty$ for $k \in \mathbb{N}_0 \cup \{\infty\}$.

- Let G be a profinite group and $\mathcal{N}$ the set of open normal subgroups in G. For a closed subgroup H we define (motivated by Lemma A.9.17)

$$|G : H| := \operatorname{lcm}\big(|G : HN| : N \in \mathcal{N}\big),$$
$$|G| := |G : 1|$$

  (note: $|G : HN| \le |G : N| < \infty$ according to Lemma A.9.14).

Remark A.9.19. Let G be a profinite group and $H \le G$ closed.

(i) Let $|G : H| < \infty$. According to Lagrange, $|G : HN| \,\big|\, |G : H|$ holds for all $N \in \mathcal{N}$. According to Lemma A.9.14, H is open and according to Corollary A.9.16 there exists an $N \in \mathcal{N}$ with $N \subseteq H$. Therefore $|G : H| = |G : HN|$ coincides with the usual index.

(ii) A subset $U \subseteq H$ is called *open in* H if there exists an open set $V \subseteq G$ with $U = V \cap H$. In this way, H itself becomes a topological space (*relative topology*). According to Remark A.9.7, H is compact and obviously also totally disconnected. For $\varphi\colon G \times G \to G$, $(x, y) \mapsto xy^{-1}$, it holds that $\varphi^{-1}_{|H\times H}(U) = \varphi^{-1}(V) \cap H \times H$. This shows that H is a profinite group. For every closed subgroup A in H, $|H : A|$ is therefore defined. By definition, there exists an open set $U \subseteq G$ with $H \setminus A = U \cap H$. Because $G \setminus A = (G \setminus H) \cup U$, A is also closed in G.

Theorem A.9.20 (Lagrange for profinite groups)**.** *Let G be a profinite group and $A, B \le G$ closed with $A \le B$. Then*

$$|G : A| = |G : B||B : A|.$$

Proof. The statement is known to hold for subgroups with finite index. For $N \in \mathcal{N}$, it follows that

$$|G : AN| = |G : BN||BN : AN| = |G : BN||B : B \cap AN| = |G : BN||B : (B \cap N)A|$$

by the Dedekind identity. Obviously, $B \cap N$ is an open normal subgroup of B with respect to the relative topology (Remark A.9.19). This shows

$$\begin{aligned}|G : A| &= \operatorname{lcm}\big(|G : AN| : N \in \mathcal{N}\big) \,\big|\, \operatorname{lcm}\big(|G : BN| : N \in \mathcal{N}\big) \operatorname{lcm}\big(|B : (B \cap N)A| : N \in \mathcal{N}\big)\\ &= |G : B||B : A|.\end{aligned}$$

Now let M be an open normal subgroup in B. By the definition of the relative topology, there exists an open set $U \subseteq G$ with $M = U \cap B$. By Corollary A.9.16, there exists an $M_1 \in \mathcal{N}$ with $M_1 \le U$. Now $B \cap N \cap M_1 \trianglelefteq B$ is also open in B and contained in M. It follows that

$$|G : BN||B : MA| \,\big|\, |G : B(N \cap M_1)||B : (B \cap N \cap M_1)A| = |G : A(N \cap M_1)| \,\big|\, |G : A|.$$

This shows $|G : B||B : A| \,\big|\, |G : A|$. □

Definition A.9.21. Let G be a profinite group and $H \leq G$ closed. H is called a *p-subgroup* of G if $|H|$ is a divisor of $p^\infty \in \Pi$. A p-subgroup H is called a *p-Sylow subgroup* of G if $|G : H|$ is not divisible by p.

Theorem A.9.22 (Sylow for profinite groups)**.** *Let G be a profinite group and $p \in \mathbb{P}$. Then G possesses a Sylow p-subgroup P and every p-subgroup of G is conjugate to a subgroup of P. In particular, any two Sylow p-subgroups in G are conjugate.*

Proof. Let $\mathcal{P}$ be the set of all closed subgroups $H \leq G$ such that $|G : H|$ is not divisible by p. Because of $G \in \mathcal{P}$, $\mathcal{P}$ is non-empty and ordered by $\subseteq$. Let $\mathcal{Q} \subseteq \mathcal{P}$ be totally ordered, $S := \bigcap_{Q \in \mathcal{Q}} Q \leq G$ and $N \in \mathcal{N}$. Then $SN = \bigcup_{s \in S} sN$ is open and closed according to Lemma A.9.14. As a closed subset of the compact space G, $G \setminus SN$ is also compact (Remark A.9.7). The open cover

$$G \setminus SN \subseteq G \setminus S = \bigcup_{Q \in \mathcal{Q}} G \setminus Q$$

thus possesses a finite subcover. Since $\mathcal{Q}$ is totally ordered, there exists a $Q \in \mathcal{Q}$ with $Q \leq SN$. By Lagrange, $|G : SN| \mid |G : Q|$ is coprime to p. Since $N \in \mathcal{N}$ was arbitrary, it follows that $S \in \mathcal{P}$. Thus S is a lower bound for $\mathcal{Q}$. By Zorn's Lemma, $\mathcal{P}$ has a minimal element P. Assume P is not a p-subgroup. Then there exists an open normal subgroup M of P such that $|P : M|$ is not a p-power. Due to Corollary A.9.16, there exists an $N \in \mathcal{N}$ with $P \cap N \leq M$. In particular, $|P : P \cap N|$ is also not a p-power. By the finite Sylow theorem, there exists a p-Sylow group $\tilde{P}/(P \cap N) < P/(P \cap N)$. As a union of cosets of $P \cap N$, $\tilde{P}$ is open in P. Because of $|P : \tilde{P}| < \infty$, $\tilde{P}$ is also closed in P and in G (Remark A.9.19). By Lagrange, $|G : \tilde{P}| = |G : P||P : \tilde{P}|$ is coprime to p. Hence, $\tilde{P} \in \mathcal{P}$, in contradiction to the choice of P. This shows that P is a p-Sylow group of G.

Now let $U \leq G$ be a p-subgroup. For all $N \in \mathcal{N}$,

$$T(N) := \{g \in G : gUg^{-1} \leq PN\} \neq \varnothing$$

by the finite Sylow theorem for G/N. As a union of cosets of N, $T(N)$ is open. Let us assume $\bigcap_{N \in \mathcal{N}} T(N) = \varnothing$. Since G is compact, there exist $N_1, \ldots, N_k \in \mathcal{N}$ with $\bigcap_{i=1}^k T(N_i) = \varnothing$. However, this contradicts $\varnothing \neq T(N_1 \cap \ldots \cap N_k) \subseteq \bigcap_{i=1}^k T(N_i)$. Thus there exists a $g \in \bigcap_{N \in \mathcal{N}} T(N)$. From Lemma A.9.17 it follows that

$$gUg^{-1} = \bigcap_{N \in \mathcal{N}} gUNg^{-1} \leq \bigcap_{N \in \mathcal{N}} PN = P.$$

For the last statement, let U be a p-Sylow group of G and $g \in G$ with $gUg^{-1} \leq P$. Then $|G : gUg^{-1}| = |G : P||P : gUg^{-1}|$ is coprime to p. As in the proof of Theorem A.9.20, on the other hand,

$$|P : gUg^{-1}| = \operatorname{lcm}\big(|P : (P \cap N)gUg^{-1}| : N \in \mathcal{N}\big) \mid \operatorname{lcm}\big(|P : P \cap N| : N \in \mathcal{N}\big) = |P|$$

is a p-power. This shows $gUg^{-1} = P$. □

Example A.9.23. Let $2 < p \in \mathbb{P}$ and $G := \mathrm{Gal}(\mathbb{Q}_{p^\infty}|\mathbb{Q})$ as in Example III.11.30. According to Theorem A.9.13, G is profinite. Let $\sigma \in G$ with $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{1+p}$ for all $n \in \mathbb{N}$. According to (the proof of) Theorem I.8.34, the restriction of σ to $\mathbb{Q}_{p^n}$ generates a Sylow p-subgroup of $\mathrm{Gal}(\mathbb{Q}_{p^n}|\mathbb{Q})$. Thus $\mathbb{Q}_{p^n}^\sigma = \mathbb{Q}_p$ and $\mathbb{Q}_{p^\infty}^\sigma = \mathbb{Q}_p$. Let $H = \mathrm{Gal}(\mathbb{Q}_{p^\infty}|\mathbb{Q}_p) \trianglelefteq G$ be the closure of $\langle\sigma\rangle$ in G. Then $|G : H| = |\mathrm{Gal}(\mathbb{Q}_p|\mathbb{Q})| = p - 1$ holds. Let $\mathbb{Q}_p \subseteq L$ be a finite Galois extension with $L \subseteq \mathbb{Q}_{p^\infty}$. There exists an $n \in \mathbb{N}$ with $L \subseteq \mathbb{Q}_{p^n}$. For $N := \mathrm{Gal}(\mathbb{Q}_{p^\infty}|L) \trianglelefteq H$ we have

$$|H : N| = |L : \mathbb{Q}_p| \mid |\mathbb{Q}_{p^n} : \mathbb{Q}_p| = p^{n-1}.$$

This shows that H is a Sylow p-subgroup of G. As an infinite Galois group, H is uncountable according to Theorem III.11.29. In particular, $H > \langle\sigma\rangle$.

Remark A.9.24. For arbitrary (infinite) groups G, one defines Sylow p-subgroups completely differently. One calls $P \leq G$ a p-subgroup if P consists only of p-elements. A maximal p-subgroup with respect to inclusion is called a Sylow p-subgroup. In this generality, however, all parts of Sylow's theorem are false.

A.10 The Lindemann-Weierstraß Theorem

Definition A.10.1. For $\alpha = \sum a_k X^k \in \mathbb{C}[X]$, $n \in \mathbb{N}_0$ and $x \in \mathbb{C}$ let

$$\begin{aligned}\alpha^{(\Sigma)} &:= \sum_{k=0}^{\infty} \alpha^{(k)} \in \mathbb{C}[X],\\ \epsilon_n(x) &:= e^{-|x|} \sum_{k=1}^{\infty} \frac{x^k n!}{(n+k)!} \in \mathbb{C},\\ \alpha^*(x) &:= \sum a_k \epsilon_k(x) x^k \in \mathbb{C}.\end{aligned}$$

Remark A.10.2. Because of $\frac{(n+k)!}{n!k!} = \binom{n+k}{n} \geq 1$ we have

$$e^{|x|} = 1 + \sum_{k=1}^{\infty} \frac{|x|^k}{k!} > \sum_{k=1}^{\infty} \frac{|x|^k n!}{(n+k)!}$$

and $|\epsilon_n(x)| < 1$ for all $n \in \mathbb{N}_0$ and $x \in \mathbb{C}$.

Lemma A.10.3. *For $\alpha \in \mathbb{C}[X]$ and $x \in \mathbb{C}$ we have $e^x \alpha^{(\Sigma)}(0) = \alpha^{(\Sigma)}(x) + \alpha^*(x) e^{|x|}$.*

Proof. Since the maps $\alpha \mapsto \alpha^{(\Sigma)}$ and $\alpha \mapsto \alpha^*$ are linear, we can assume $\alpha = X^n$ with $n \in \mathbb{N}_0$. Then

$$\alpha^{(\Sigma)}(x) + \alpha^*(x) e^{|x|} = x^n + n x^{n-1} + \ldots + n! + x^n \sum_{k=1}^{\infty} \frac{x^k n!}{(n+k)!} = n! \sum_{k=0}^{\infty} \frac{x^k}{k!} = e^x \alpha^{(\Sigma)}(0). \qquad \square$$

Lemma A.10.4. *Let $\alpha \in \mathbb{Z}[X]$, $n \in \mathbb{N}$, $\beta := \frac{X^n}{(n-1)!}\alpha$ and $\gamma := \frac{X^{n-1}}{(n-1)!}\alpha$. Then $\beta^{(\Sigma)}(0) \in n\mathbb{Z}$ and $\gamma^{(\Sigma)}(0) \in \alpha(0) + n\mathbb{Z}$ hold.*

Proof. Wlog. let $\alpha = X^m$ with $m \in \mathbb{N}_0$. Then

$$\begin{aligned}\beta^{(\Sigma)}(0) &= \beta^{(n+m)}(0) = \frac{(n+m)!}{(n-1)!} \in n\mathbb{Z},\\ \gamma^{(\Sigma)}(0) &= \beta^{(n+m-1)}(0) = \frac{(n+m-1)!}{(n-1)!} \in \alpha(0) + n\mathbb{Z}.\end{aligned} \qquad \square$$

Theorem A.10.5 (Lindemann-Weierstrass)**.** *For pairwise distinct $a_1, \ldots, a_n \in \overline{\mathbb{Q}}$, the values $e^{a_1}, \ldots, e^{a_n}$ are linearly independent over $\overline{\mathbb{Q}}$.*

Proof. Suppose there exist $b_1, \dots, b_n \in \overline{\mathbb{Q}} \setminus \{0\}$ with

$$b_1 e^{a_1} + \ldots + b_n e^{a_n} = 0. \tag{A.10.1}$$

Let $\mu_i \in \mathbb{Q}[X]$ be the minimal polynomial of b_i and let L be a splitting field of $\mu_1 \dots \mu_n$. Let $G := \mathrm{Gal}(L|\mathbb{Q})$ and $\alpha := b_1 X_1 + \ldots + b_n X_n \in L[X_1, \dots, X_n]$. Then

$$\beta := \prod_{\sigma \in G} \sigma(\alpha) = \sum_{\substack{i_1,\dots,i_n \geq 0 \\ i_1+\dots+i_n = |G|}} \lambda_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n} \in L^G[X_1, \dots, X_n] = \mathbb{Q}[X_1, \dots, X_n]$$

and $\beta(e^{a_1}, \dots, e^{a_n}) = 0$. On the other hand, $\beta(e^{a_1}, \dots, e^{a_n})$ is a rational linear combination of terms of the form $e^{i_1 a_1 + \dots + i_n a_n}$ with algebraic exponents. By grouping terms with the same exponents, we obtain $b'_1 e^{a'_1} + \ldots + b'_m e^{a'_m} = 0$ with $a'_1, \dots, a'_m \in \overline{\mathbb{Q}}$ pairwise distinct and $b'_1, \dots, b'_m \in \mathbb{Q}$. We sort the a_i lexicographically $(\mathrm{Re}(a_1), \mathrm{Im}(a_1)) < \dots < (\mathrm{Re}(a_n), \mathrm{Im}(a_n))$. Since $e^{|G|a_1}$ occurs only once in $\beta(e^{a_1}, \dots, e^{a_n})$ (with coefficient $\prod \sigma(b_1) \neq 0$), not all b'_i can vanish. We therefore replace a_i by a'_i and b_i by b'_i. After multiplication by the common denominator, it then holds that $b_1, \dots, b_n \in \mathbb{Z} \setminus \{0\}$.

Now let $\mu_i \in \mathbb{Q}[X]$ be the minimal polynomial of a_i and L a splitting field of $\mu_1 \dots \mu_n$ with $G := \mathrm{Gal}(L|\mathbb{Q}) = \{\sigma_1, \dots, \sigma_s\}$. We analogously consider

$$0 = \prod_{\sigma \in G} \sum_{i=1}^{n} b_i e^{\sigma(a_i)} = \sum_{1 \leq k_1, \dots, k_s \leq n} b_{k_1} \dots b_{k_s} e^{\sigma_1(a_{k_1}) + \dots + \sigma_s(a_{k_s})}. \tag{A.10.2}$$

For $\tau \in G$ there exists a permutation $\pi \in S_s$ with $\tau\sigma_i = \sigma_{\pi(i)}$ for $i = 1, \dots, s$. It follows that

$$\tau\Big(\sum_{i=1}^{s} \sigma_i(a_{k_i})\Big) = \sum_{i=1}^{s} \sigma_{\pi(i)}(a_{k_i}) = \sum_{i=1}^{s} \sigma_i(a_{k_{\pi^{-1}(i)}})$$

and $b_{k_1} \dots b_{k_s} = b_{k_{\pi^{-1}(1)}} \dots b_{k_{\pi^{-1}(s)}}$. Therefore G acts on the set of exponents in (A.10.2) and any two terms in the same orbit have the same coefficient. This property is preserved when we group terms with the same exponents. For $i = 1, \dots, s$ we choose $m_i \in \{1, \dots, n\}$ with $(\mathrm{Re}(\sigma_i(a_{m_i})), \mathrm{Im}(\sigma_i(a_{m_i}))) < (\mathrm{Re}(\sigma_i(a_l)), \mathrm{Im}(\sigma_i(a_l)))$ for all $l \neq m_i$. Since the exponent $\sigma_1(a_{m_1}) + \dots + \sigma_s(a_{m_s})$ occurs only once in (A.10.2) (with coefficient $b_{m_1} \dots b_{m_s} \neq 0$), not all terms in (A.10.2) vanish. We may thus replace a_i by $\sigma_1(a_{k_1}) + \dots + \sigma_s(a_{k_s})$ and b_i by $b_{k_1} \dots b_{k_s}$. Subsequently, (A.10.1) has the form

$$\sum_{i=1}^{t} b_i \sum_{j=1}^{s_i} e^{a_{ij}} = 0,$$

where $\{a_{ij} : j = 1, \dots, s_i\}$ for $i = 1, \dots, t$ are the orbits of G on $\{a_1, \dots, a_n\}$. By multiplying this equation by $\sum_{j=1}^{t_1} e^{-a_{1j}}$ and subsequently splitting G-orbits again, we can assume $a_{11} = 0$ and $t_1 = 1$ (because $a_{1j} \neq a_{ik}$ for $i > 1$, the terms e^0 cannot cancel each other out). After renaming, we obtain

$$b_0 + \sum_{i=1}^{t} b_i \sum_{j=1}^{s_i} e^{a_{ij}} = 0 \tag{A.10.3}$$

with $b_0, \dots, b_t \in \mathbb{Z} \setminus \{0\}$ and $a_{ij} \neq 0$ for all i, j. Furthermore, let $n = s_1 + \dots + s_t$.

According to Theorem II.11.15, there exists a $c \in \mathbb{N}$ such that ca_{ij} is algebraic integer for all i, j. Then $\alpha := c^n \prod_{i,j}(X - a_{ij}) \in \mathbb{Z}[X]$ follows from Remark I.8.53. We choose a prime number $p > \max\{c, b_0, |\alpha(0)|\}$ and define

$$\gamma := \frac{(cX)^{p-1}}{(p-1)!} \alpha^p \in \mathbb{Q}[X].$$

Multiplication of (A.10.3) by $\gamma^{(\Sigma)}(0)$ yields

$$b_0\gamma^{(\Sigma)}(0) + \sum_{i=1}^{t} b_i \sum_{j=1}^{s_i} \gamma^{(\Sigma)}(a_{ij}) + \sum_{i=1}^{t} b_i \sum_{j=1}^{s_i} \gamma^*(a_{ij}e^{|a_{ij}|} = 0 \tag{A.10.4}$$

according to Lemma A.10.3. From Lemma A.10.4 and the choice of p it follows that

$$b_0\gamma^{(\Sigma)}(0) \equiv b_0 c^{p-1}\alpha^p(0) \not\equiv 0 \pmod{p}.$$

Furthermore, it holds that

$$\gamma_{ij} := \gamma(X + a_{ij}) = \frac{X^p}{(p-1)!}\big(c(X+a_{ij})\big)^{p-1}\Big(c^n \prod_{(k,l)\neq(i,j)} (X + a_{ij} - a_{kl})\Big)^p = \frac{X^p}{(p-1)!}\delta_{ij},$$

where $\delta_{ij} \in \mathbb{C}[X]$ has algebraic integer coefficients (polynomials in the ca_{kl}). On the other hand, $\sum_{j=1}^{t_i} \gamma_{ij} \in L^G[X] = \mathbb{Q}[X]$ and from Remark I.8.53 it follows that $\sum_{j=1}^{t_i} \gamma_{ij} = \frac{X^p}{(p-1)!}\delta_i$ with $\delta_i := \sum_{j=1}^{t_i} \delta_{ij} \in \mathbb{Z}[X]$. By the chain rule, $\gamma'_{ij} = \gamma'(X + a_{ij})$ and Lemma A.10.4 yields

$$\sum_{j=1}^{t_i} \gamma^{(\Sigma)}(a_{ij}) = \sum_{j=1}^{t_i} \gamma_{ij}^{(\Sigma)}(0) \in p\mathbb{Z}.$$

The sum of the first two (integer) summands in (A.10.4) is thus not divisible by p and therefore at least 1 in absolute value.

For a fixed $x \in \mathbb{C}$, there exists a constant $C \in \mathbb{R}$ with

$$|\gamma^*(x)| \overset{\text{A.10.2}}{\leq} \frac{(c|x|)^{p-1}}{(p-1)!}\alpha(|x|)^p \leq \frac{C^p}{(p-1)!}.$$

If p is large enough, it follows that

$$\Big|\sum_{i=1}^{t} b_i \sum_{j=1}^{s_i} \gamma^*(a_{ij})e^{|a_{ij}|}\Big| < 1.$$

This contradicts (A.10.4). □

Example A.10.6. For $a_1 = 0$ and $a_2 = 1$, one obtains the transcendence of e. Let $x \in \overline{\mathbb{Q}} \setminus \{0\}$. Then $\cos(x)e^0 - \frac{1}{2}e^{x\mathrm{i}} - \frac{1}{2}e^{-x\mathrm{i}} = 0$. According to Lindemann-Weierstraß, $\cos(x)$ is transcendent. Because of $\cos(\pi) = -1 \in \mathbb{Q}$, π is transcendent. Now let $x \in \overline{\mathbb{Q}} \cap \mathbb{R} \setminus \{1\}$ and $x > 0$. Then $xe^0 - e^{\log(x)} = 0$ and $\log(x)$ is transcendent.

Corollary A.10.7. *$a_1, \ldots, a_n \in \overline{\mathbb{Q}}$ are linearly dependent over $\mathbb{Q}$ if and only if $e^{a_1}, \ldots, e^{a_n}$ are algebraically dependent over $\mathbb{Q}$.*

Proof. First, let $a_1, \ldots, a_n$ be linearly dependent, say $\sum_{i=1}^{n} \lambda_i a_i = 0$ for $\lambda_1, \ldots, \lambda_n \in \mathbb{Q}$ (not all 0). After multiplication by the common denominator, we can assume $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$. After renumbering, $\lambda_1, \ldots, \lambda_k > 0$, $\lambda_{k+1}, \ldots, \lambda_l < 0$ and $\lambda_{l+1} = \ldots = \lambda_n = 0$ holds. It follows that

$$\prod_{i=1}^{k} (e^{a_i})^{\lambda_i}\Big(\prod_{i=k+1}^{l} (e^{a_i})^{-\lambda_i}\Big)^{-1} = e^{\lambda_1 a_1 + \ldots + \lambda_n a_n} = e^0 = 1.$$

For the polynomial

$$\alpha := X_1^{\lambda_1} \dots X_k^{\lambda_k} - X_{k+1}^{-\lambda_{k+1}} \dots X_l^{-\lambda_l} \in \mathbb{Q}[X_1, \dots, X_n] \setminus \{0\},$$

we thus have $\alpha(e^{a_1}, \dots, e^{a_n}) = 0$. Thus $e^{a_1}, \dots, e^{a_n}$ are algebraically dependent over $\mathbb{Q}$.

Now let $e^{a_1}, \dots, e^{a_n}$ be algebraically dependent over $\mathbb{Q}$. Then there exists

$$\alpha = \sum_{i_1,\dots,i_n \geq 0} \lambda_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n} \in \mathbb{Q}[X_1, \dots, X_n] \setminus \{0\}$$

with $\alpha(e^{a_1}, \dots, e^{a_n}) = 0$. Thus the numbers $e^{i_1 a_1 + \dots + i_n a_n}$ with $\lambda_{i_1,\dots,i_n} \neq 0$ are linearly dependent over $\mathbb{Q}$. According to Lindemann-Weierstraß, there exist tuples $(i_1, \dots, i_n) \neq (j_1, \dots, j_n)$ with $i_1 a_1 + \dots + i_n a_n = j_1 a_1 + \dots + j_n a_n$. Thus $a_1, \dots, a_n$ are linearly dependent over $\mathbb{Q}$. □

Remark A.10.8.

(i) One can also derive the Lindemann-Weierstraß theorem from Corollary A.10.7. For this, let $a_1, \dots, a_n \in \overline{\mathbb{Q}}$ be pairwise distinct. Suppose there exist $b_1, \dots, b_n \in \overline{\mathbb{Q}} \setminus \{0\}$ with $\sum_{i=1}^n b_i e^{a_i} = 0$. Wlog. let $a_1, \dots, a_k$ be a $\mathbb{Q}$-basis of $\langle a_1, \dots, a_n \rangle$. Then there exist $\lambda_{ij} \in \mathbb{Q}$ with $a_i = \sum_{j=1}^k \lambda_{ij} a_j$ for $i = k+1, \dots, n$. Choose $s \in \mathbb{N}$ with $s_{ij} := s\lambda_{ij} \in \mathbb{Z}$ for all i, j. Let $s_j := \min\{0, s_{k+1,j}, \dots, s_{n,j}\} \leq 0$ for $j = 1, \dots, k$. Then

$$\gamma := X_1^{-s_1} \dots X_k^{-s_k} \Big(\sum_{i=1}^k b_i X_i^s + \sum_{i=k+1}^n b_i X_1^{s_{i,1}} \dots X_k^{s_{i,k}} \Big) \in \overline{\mathbb{Q}}[X_1, \dots, X_k].$$

Since $a_{k+1}, \dots, a_n$ are pairwise distinct, the exponent tuples $(s_{i,1}, \dots, s_{i,k})$ for $i = k+1, \dots, n$ are pairwise distinct. Since these a_i are also distinct from $a_1, \dots, a_k$, none of the tuples has the form $(0, \dots, 0, s, 0, \dots, 0)$. The monomials in the above bracket are therefore pairwise distinct. This shows $\gamma \neq 0$. It holds that

$$\begin{aligned} \gamma(e^{a_1/s}, \dots, e^{a_k/s}) &= e^{-(a_1 s_1 + \dots + a_k s_k)/s} \Big(\sum_{i=1}^k b_i e^{a_i} + \sum_{i=k+1}^n b_i e^{a_1 \lambda_{i1} + \dots + a_k \lambda_{ik}} \Big) \\ &= e^{-(a_1 s_1 + \dots + a_k s_k)/s} \sum_{i=1}^n b_i e^{a_i} = 0. \end{aligned}$$

According to Lemma II.4.6, $e^{a_1/s}, \dots, e^{a_k/s}$ are algebraically dependent over $\overline{\mathbb{Q}}$. Wlog. let $e^{a_1/s}$ be algebraic over $\overline{\mathbb{Q}}(e^{a_2/s}, \dots, e^{a_k/s})$. From Theorem II.4.18 it follows that

$$\begin{aligned} \operatorname{trg}\big(\mathbb{Q}(e^{a_1/s}, \dots, e^{a_k/s}) | \mathbb{Q}\big) &\leq \operatorname{trg}\big(\overline{\mathbb{Q}}(e^{a_1/s}, \dots, e^{a_k/s}) | \mathbb{Q}\big) = \operatorname{trg}\big(\overline{\mathbb{Q}}(e^{a_1/s}, \dots, e^{a_k/s}) | \overline{\mathbb{Q}}\big) \\ &= \operatorname{trg}\big(\overline{\mathbb{Q}}(e^{a_2/s}, \dots, e^{a_k/s}) | \overline{\mathbb{Q}}\big) \leq k - 1. \end{aligned}$$

Thus $e^{a_1/s}, \dots, e^{a_k/s}$ are algebraically dependent over $\mathbb{Q}$. According to Corollary A.10.7, $a_1, \dots, a_k$ would be linearly dependent over $\mathbb{Q}$. This contradiction shows that $e^{a_1}, \dots, e^{a_n}$ are linearly independent over $\overline{\mathbb{Q}}$.

(ii) The transcendence of the logarithm (Example A.10.6) was generalized by Baker: Let $a_1, \dots, a_n \in \overline{\mathbb{Q}} \setminus \{0, 1\}$ such that $\log(a_1), \dots, \log(a_n)$ are linearly independent over $\mathbb{Q}$. Then $1, \log(a_1), \dots, \log(a_n)$ are linearly independent over $\overline{\mathbb{Q}}$ (in particular, $\log(a_1), \dots, \log(a_n)$ are transcendental). This does not depend on the specific choice of the complex logarithm. Let us assume, for example, that $a = 2^{\sqrt{2}}$ is algebraic. Because of $\log(a) = \sqrt{2}\log(2)$, $\log(a)$ and $\log(2)$ are linearly dependent over $\overline{\mathbb{Q}}$. According to Baker, $\log(a)$ and $\log(2)$ are also linearly dependent over $\mathbb{Q}$. But then $\sqrt{2} = \frac{\log(a)}{\log(2)} \in \mathbb{Q}$. This contradiction shows the transcendence of $2^{\sqrt{2}}$.

(iii) An open conjecture by SCHANUEL states: If $a_1, \ldots, a_n \in \mathbb{C}$ are linearly independent over $\mathbb{Q}$, then $\operatorname{trg}(\mathbb{Q}(a_1, \ldots, a_n, e^{a_1}, \ldots, e^{a_n})|\mathbb{Q}) \geq n$. In the case $a_1, \ldots, a_n \in \overline{\mathbb{Q}}$ one obtains Lindemann-Weierstraß and in the case $e^{a_1}, \ldots, e^{a_n} \in \overline{\mathbb{Q}}$ the theorem of Baker follows.

A.11 Rings with Finiteness Condition

Remark A.11.1. The following theorem generalizes Wedderburn's theorem on finite division rings (Theorem II.8.7) and Exercise II.7.

Theorem A.11.2 (Jacobson)**.** *Let R be a ring in which for every $x \in R$ there exists an $n \geq 2$ with $x^n = x$. Then R is commutative.*

Proof (Wamsley). We identify $\mathbb{Z}$ with $\mathbb{Z}1_R$. By assumption, there exists an $n \geq 2$ with $2^n = 2$. Therefore, the order $o(x)$ of $x \in R$ in $(R, +)$ is a divisor of $2^n - 2$. Suppose there exists a prime p with $p^2 \mid o(x)$. Then $\tilde{x} := \frac{o(x)}{p} x \neq 0$ and $\tilde{x}^2 = 0$. By assumption, however, there exists an $m \geq 2$ with $\tilde{x}^m = \tilde{x}$. This contradiction shows $o(x) = p_1 \dots p_r$ with pairwise distinct primes $p_1, \dots, p_r$. For $p \in \mathbb{P}$ let

$$R_p := \{x \in R : px = 0\} \trianglelefteq R$$

(for $p > 2^n - 2$ we have $R_p = 0$). For $i = 1, \dots, r$ let $x_i := \frac{o(x)}{p_i} x \in R_{p_i}$. According to the Euclidean algorithm, there exist $a_1, \dots, a_r \in \mathbb{Z}$ with $a_1 \frac{o(x)}{p_1} + \dots + a_r \frac{o(x)}{p_r} = 1$. It follows that $x = a_1 x_1 + \dots + a_r x_r$ and $R = \bigoplus_{p \in \mathbb{P}} R_p$. Let $1 = \sum_{p \in \mathbb{P}} e_p$ with idempotents $e_p \in R_p$. Obviously, R_p is then a ring with identity element e_p. We can therefore assume $R = R_p$ for some $p \in \mathbb{P}$, i. e. R has characteristic p.

Assume that R is not commutative. Let $x \in R \setminus \mathrm{Z}(R)$. Then

$$S := \big\{\alpha(x) : \alpha \in \mathbb{Z}[X]\big\} \subseteq R$$

is a finite and thus Artinian ring. Since R has no nilpotent elements by assumption, $\mathrm{J}(S) = 0$ (Lemma II.8.15). By Artin-Wedderburn, $S \cong Q_1^{n_1 \times n_1} \times \dots \times Q_t^{n_t \times n_t}$, where $Q_1, \dots, Q_t$ are finite fields by Wedderburn. In the case $n_i > 1$, there would be $E_{12} \in Q_i^{n_i \times n_i}$ with $E_{12}^2 = 0$ in contradiction to the assumption. Thus $n_1 = \dots = n_t = 1$. Let $x = x_1 + \dots + x_t$ with $x_i \in Q_i$. Because $x \notin \mathrm{Z}(R)$, there must exist an i with $x_i \notin \mathrm{Z}(R)$. By replacing x with x_i, we can assume that S is a finite field.

Let $|S| = p^r = q$ and $e \in S$ be the identity element of S. Let $f := 1 - e$. For $r \in R$ we have $(erf)^2 = 0$ and thus $eRf = 0$. Analogously, $fRe = 0$. This shows $R = eRe \oplus fRf$ with $x \in eRe$. If $x \in \mathrm{Z}(eRe)$ were true, then $x \in \mathrm{Z}(R)$ would hold. We can thus assume $R = eRe$, i. e. $e = 1$. In this way, R becomes an S-vector space. We consider the S-linear maps $\alpha_x \colon R \to R$, $r \mapsto xr$ and $\beta_x \colon R \to R$, $r \mapsto rx$. By the associative law, $\alpha_x \circ \beta_x = \beta_x \circ \alpha_x$ holds. Let $\delta_x := \alpha_x - \beta_x$. By the binomial formula, $\delta_x^p = \alpha_x^p - \beta_x^p = \alpha_{x^p} - \beta_{x^p} = \delta_{x^p}$ and $\delta_x^q = \delta_{x^q} = \delta_x$ hold. Because $X^q - X = \prod_{\lambda \in S}(X - \lambda) \in S[X]$, we have

$$0 = \delta_x^q - \delta_x = \prod_{\lambda \in S} (\delta_x - \lambda \,\mathrm{id}) \in \mathrm{End}_S(R).$$

For $y \in R \setminus \mathrm{C}_R(x)$ we have $\delta_x(y) \neq 0$. Therefore, there exist $l \geq 2$ and pairwise distinct elements $0 = \lambda_1, \dots, \lambda_l \in S$ with

$$z := (\delta_x - \lambda_{l-1} \,\mathrm{id}) \dots (\delta_x - \lambda_1 \,\mathrm{id})(y) \neq 0$$

and $(\delta_x - \lambda_l \,\mathrm{id})(z) = 0$, i. e. $zx = (x - \lambda_l)z \in Sz$. Since S is generated by x, it holds that $zS = Sz$. Because $\lambda_l \neq 0$, we have $xz \neq zx$. Therefore, x and z generate a finite non-commutative subring T of R. As above, however, T must be a direct product of fields. Contradiction. □

A.12 Free Modules with Infinite Rank

Theorem A.12.1. *Let R be a principal ideal domain and M a free R-module. Then every submodule $N \leq M$ is free with* $\operatorname{rk} N \leq \operatorname{rk} M$.

Proof. Let B be a basis of M and $N_C := \langle C \rangle \cap N$ for $C \subseteq B$. Let $\mathcal{M}$ be the set of all triples (C, Γ, f) consisting of a subset $C \subseteq B$, such that N_C is free with basis Γ and $f\colon \Gamma \to C$ is an injective map. Because of $(\varnothing, \varnothing, \varnothing) \in \mathcal{M}$, $\mathcal{M}$ is non-empty and ordered by

$$(C, \Gamma, f) \leq (C', \Gamma', f') :\Longleftrightarrow C \subseteq C',\ \Gamma \subseteq \Gamma',\ f'_\Gamma = f.$$

Let $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ be totally ordered and

$$(C, \Gamma) := \Big(\bigcup_{(D,\Delta,g)\in\mathcal{N}} D,\ \bigcup_{(D,\Delta,g)\in\mathcal{N}} \Delta \Big).$$

Then N_C is clearly free with basis Γ. For $\gamma \in \Gamma$ there exists $(D, \Delta, g) \in \mathcal{N}$ with $\gamma \in \Delta$. We define $f(\gamma) := g(\gamma)$. Then $g\colon \Gamma \to C$ is clearly a well-defined injective map. Thus $(C, \Gamma, f) \in \mathcal{M}$ is an upper bound of $\mathcal{N}$. By Zorn's Lemma, there exists a maximal element $(C, \Gamma, f) \in \mathcal{M}$. We assume $C \neq B$ and choose $b \in B \setminus C$. For $C' := C \cup \{b\}$ we have

$$N_{C'}/N_C = N_{C'}/(N_{C'} \cap \langle C \rangle) \simeq (N_{C'} + \langle C \rangle)/\langle C \rangle \leq \langle C' \rangle/\langle C \rangle \simeq Rb \simeq R.$$

In the case $N_{C'} = N_C$, $(C', \Gamma, f) \in \mathcal{M}$ would hold, contradicting the maximality of (C, Γ, f). Thus $N_{C'} \neq N_C$. Since R is a principal ideal domain, there exists $\delta \in N_{C'}$ with $N_{C'}/N_C = R(\delta + N_C)/N_C \simeq R$, i. e. $N_{C'} = R\delta + N_C$. Therefore $\Gamma' := \Gamma \cup \{\delta\}$ is a generating set of $N_{C'}$. Let $r_\gamma, r_\delta \in R$ with

$$r_\delta \delta + \sum_{\gamma\in\Gamma} r_\gamma \gamma = 0.$$

Then $r_\delta \delta \in N_C$ and from $N_{C'}/N_C \simeq R$ it follows that $r_\delta = 0$. Since Γ is linearly independent, $r_\gamma = 0$ for all $\gamma \in \Gamma$ as well. Therefore $N_{C'}$ is free with basis Γ'. Finally, $f\colon \Gamma \to C$ can be extended to an injective map $f'\colon \Gamma' \to C'$ with $f'(\delta) = b$. Thus $(C', \Gamma', f') \in \mathcal{M}$, contradicting the maximality of (C, Γ, f). This shows $C = B$ and $N = N_B$ is free with basis Γ. The map $f\colon \Gamma \to B$ shows $\operatorname{rk} N = |\Gamma| \leq |B| = \operatorname{rk} M$. □

Theorem A.12.2 (Baer)**.** *The abelian group $\mathbb{Z}^\mathbb{N} = \prod_\mathbb{N} \mathbb{Z}$ is not free.*

Proof (Schröer). Assume $G := \mathbb{Z}^\mathbb{N}$ is free with basis B. Let $e_i \in G$ with a 1 at position i and zeros otherwise. We write $e_i = \sum_{b\in B} \lambda_{ib} b$ with $\lambda_{ib} \in \mathbb{Z}$. As a countable union of finite sets,

$$C := \{b \in B : \exists i \in \mathbb{N} : \lambda_{ib} \neq 0\}$$

is countable. Thus $H := \langle C \rangle \leq G$ is also countable. On the other hand, G and therefore also B is uncountable. Furthermore, G/H is free with basis $B \setminus C$. Obviously there exist uncountably many $(a_1, a_2, \ldots) \in G$ with $a_i \geq 2$ for $i = 1, \ldots$. Therefore one can find certain a_i with $x := (a_1, a_1 a_2, \ldots) \notin H$.

Let $\lambda_b \in \mathbb{Z}$ with $x \equiv \sum_{b \in B \setminus C} \lambda_b b \pmod{H}$. Because $x \notin H$ there exists a $b' \in B \setminus C$ with $\lambda_{b'} \neq 0$. Because $e_1, e_2, \ldots \in H$ it holds that

$$a_1 \ldots a_i(0, \ldots, 0, a_{i+1}, a_{i+1}a_{i+2}, \ldots) \equiv x \equiv \sum_{b \in B \setminus C} \lambda_b b \pmod{H}.$$

A comparison of coefficients yields the contradiction $a_1 \ldots a_i \mid \lambda_{b'}$ for all $i \in \mathbb{N}$. □

A.13 Group Determinants

Definition A.13.1. Let G be a finite group and $R := \mathbb{C}[X_g : g \in G]$ the polynomial ring in $|G|$ unknowns. One calls $\Theta(G) := \det((X_{gh^{-1}})_{g,h\in G}) \in R$ the *determinant* of G.

Remark A.13.2.

(i) For $\pi \in \mathrm{Sym}(G)$ it holds that $(X_{\pi(g)\pi(h)^{-1}})_{g,h} = P^{-1}(X_{gh^{-1}})P$, where $P = (\delta_{g\pi(h)})_{g,h}$ is the permutation matrix of π. This shows that $\Theta(G)$ does not depend on the order of the $g \in G$.

(ii) According to the Leibniz formula, $\Theta(G)$ is a homogeneous polynomial of degree n and monic in X_1, i. e. every monomial of $\Theta(G)$ has degree n and the coefficient of X_1^n is 1. Since R is a unique factorization domain according to Gauss, one can ask about the prime factorization of $\Theta(G)$.

Lemma A.13.3. *Let K be an infinite field and $\alpha, \beta \in K[X_1, \ldots, X_n]$ with $\alpha(x_1, \ldots, x_n) = \beta(x_1, \ldots, x_n)$ for all $x_1, \ldots, x_n \in K$. Then $\alpha = \beta$.*

Proof. For $n = 1$, $\alpha - \beta$ has infinitely many roots and it follows that $\alpha = \beta$ from Theorem I.8.29. Now let $n \geq 2$ and $\alpha - \beta = \sum_{k=0}^{d} \gamma_k X_n^k$ with $\gamma_0, \ldots, \gamma_d \in K[X_1, \ldots, X_{n-1}]$. For all $x_1, \ldots, x_{n-1} \in K$,

$$\sum_{k=0}^{d} \gamma_k(x_1, \ldots, x_{n-1}) X_n^k \in K[X_n]$$

has infinitely many roots and it follows again that $\gamma_k(x_1, \ldots, x_{n-1}) = 0$. By induction on n, $\gamma_0 = \ldots = \gamma_d = 0$ and thus $\alpha = \beta$. □

Lemma A.13.4. *The polynomial $\det\big((X_{ij})_{i,j}\big) \in \mathbb{C}[X_{ij} : 1 \leq i, j \leq n]$ is irreducible.*

Proof. According to the Leibniz formula, $\delta := \det(X_{ij})$ is linear as a polynomial in X_{kl} with coefficients over the integral domain $\mathbb{C}[X_{ij} : (i, j) \neq (k, l)]$. Let $\delta = \alpha\beta$ with $\alpha, \beta \in \mathbb{C}[X_{ij} : 1 \leq i, j \leq n]$. Each X_{kl} then appears either in α or in β, because linear polynomials are always irreducible. Wlog. let X_{11} appear in α. Suppose X_{1k} appears in β for some $k > 1$. Then

$$\delta = (\alpha_0 + \alpha_1 X_{11})(\beta_0 + \beta_1 X_{1k}) = \alpha_0\beta_0 + \alpha_1\beta_0 X_{11} + \alpha_0\beta_1 X_{1k} + \alpha_1\beta_1 X_{11}X_{1k},$$

where X_{11} does not appear in α_0 and X_{1k} does not appear in β_0. Because $\alpha_1\beta_1 \neq 0$, $X_{11}X_{1k}$ occurs in δ. However, this contradicts the Leibniz formula. Thus $X_{11}, \ldots, X_{1n}$ only appear in α. By the same argument, $X_{1j}, \ldots, X_{nj}$ only appear in α, because $X_{1j}X_{kj}$ does not occur in δ for $k > 1$. Overall, $\beta \in \mathbb{C}$ and δ is irreducible. □

Lemma A.13.5. *Let $\Delta_1, \dots, \Delta_k$ be the non-similar irreducible representations of G over $\mathbb{C}$. Then the map*

$$\Delta_1 \oplus \ldots \oplus \Delta_k \colon \mathbb{C}G \to \bigtimes_{i=1}^{k} \mathbb{C}^{\deg \Delta_i \times \deg \Delta_i},$$
$$x \mapsto (\Delta_i(x))_i$$

is an isomorphism of algebras.

Proof. Because $\dim \mathbb{C}G = |G| = \sum_{i=1}^{k} \deg(\Delta_i)^2$, it suffices to show that $\Delta_1 \oplus \ldots \oplus \Delta_k$ is injective. So let $x \in \bigcap_{i=1}^{k} \operatorname{Ker}(\Delta_i)$. Then x also lies in the kernel of the regular representation. In particular, $x = x \cdot 1 = 0$. □

Lemma A.13.6. *Let $\Delta \colon G \to \mathrm{GL}(d, \mathbb{C})$ be an irreducible representation of G and*

$$(\alpha_{ij})_{i,j} := \sum_{g \in G} X_g \Delta(g) \in R^{d \times d}.$$

Then the polynomials α_{ij} are linearly independent over $\mathbb{C}$.

Proof. Let $c_{ij} \in \mathbb{C}$ with $\sum_{1 \le i,j \le n} c_{ij}\alpha_{ij} = 0$. For all $x_g \in \mathbb{C}$ ($g \in G$), $\sum_{1 \le i,j \le n} c_{ij}\alpha_{ij}(x_g) = 0$ holds. According to Lemma A.13.5, the extension $\Delta \colon \mathbb{C}G \to \mathbb{C}^{d \times d}$ is surjective. For $1 \le k, l \le n$, there exists therefore an $x := \sum x_g g \in \mathbb{C}G$ with $(\alpha_{ij}(x_g))_{i,j} = \Delta(x) = (\delta_{ik}\delta_{jl})$. It follows that $c_{kl} = \sum_{1 \le i,j \le n} c_{ij}\alpha_{ij}(x_g) = 0$ for $k, l = 1, \dots, n$. □

Theorem A.13.7 (Frobenius)**.** *The prime factorization of $\Theta(G)$ in R has the form*

$$\Theta(G) = \prod_{\chi \in \mathrm{Irr}(G)} \theta_\chi^{\chi(1)},$$

where θ_χ is irreducible and homogeneous of degree $\chi(1)$.

Proof. Let $n := |G|$ and $\Gamma \colon \mathbb{C}G \to \mathbb{C}^{n \times n}$ be the regular representation of G. For $x = \sum_{g \in G} x_g g \in \mathbb{C}G$ and $h \in G$, it holds that $xh = \sum_{g \in G} x_{gh^{-1}} g$. With respect to the canonical basis G, it therefore holds that $\Gamma(x) = (x_{gh^{-1}})_{g,h \in G}$. On the other hand, Γ is similar to $\Delta_1^{d_1} \oplus \ldots \oplus \Delta_k^{d_k}$, where $\Delta_1, \dots, \Delta_k$ are the non-similar irreducible representations of G and $d_i := \deg \Delta_i$ (Remark II.13.26). In particular, $\det\big((x_{gh^{-1}})_{g,h}\big) = \prod_{i=1}^{k} \det\big(\Delta_i(x)\big)^{d_i}$ for all $(x_g)_g \in \mathbb{C}^n$. From Lemma A.13.3 it follows that

$$\Theta(G) = \prod_{i=1}^{k} \det\Big(\sum_{g \in G} X_g \Delta_i(g)\Big)^{d_i}.$$

Let then $\theta_i := \det\big(\sum_{g \in G} X_g \Delta_i(g)\big) \in R$ for $i = 1, \dots, k$. According to the Leibniz formula, θ_i is homogeneous of degree d_i and monic in X_1. Let $(\alpha_{st})_{s,t} = \sum_{g \in G} X_g \Delta_i(g)$. According to Lemma A.13.6, the α_{st} are linearly independent over $\mathbb{C}$ and linear in all X_g. The X_g span a $\mathbb{C}$-vector space $V \le R$ of dimension n. We can therefore extend α_{st} by $\beta_1, \dots, \beta_{n-d_i^2}$ to a basis of V. Let F be an arbitrary bijection between $\{\alpha_{st}, \beta_j : 1 \le s, t \le d_i, j = 1, \dots, n - d_i^2\}$ and $\{X_g : g \in G\}$. Then F extends to an automorphism of the $\mathbb{C}$-algebra R. Under F, θ_i is mapped to $\det(X_{st})$, where the $X_{st} := F(\alpha_{st}) \in \{X_g : g \in G\}$ are pairwise distinct. According to Lemma A.13.4, $\det(X_{st})$ is irreducible in $\mathbb{C}[X_{st} : 1 \le s, t \le d_i]$.

A factorization of $\det(X_{st})$ in R would also be a factorization in $\mathbb{C}[X_{st}]$ (degree comparison). Therefore, $\det(X_{st})$ and θ_i are also irreducible in R.

It remains to show that θ_i and θ_j are not associate for $i \neq j$. Since all θ_i are monic in X_1, it suffices to show $\theta_i \neq \theta_j$ (note $R^\times = \mathbb{C}$). For this, let χ_i be the character of Δ_i. Let $g \in G \setminus \{1\}$. By setting $X_h = 0$ for $h \in G \setminus \{1, g\}$, θ_i becomes $\det(X_1^{d_i} + \Delta_i(g)X_g)$. Again according to the Leibniz formula, it holds that

$$\det(X_1^{d_i} + \Delta_i(g)X_g) = X_1^{d_i} + \chi_i(g)X_1^{d_i-1}X_g + \gamma,$$

where the degree of X_1 in γ is less than d_i. From $\chi_i \neq \chi_j$ it now follows that $\theta_i \neq \theta_j$. □

Example A.13.8. For $G = C_n$ one obtains the cyclic determinant

$$\Theta(G) = |X_{i-j \pmod n}| = \begin{vmatrix} X_0 & X_{n-1} & \cdots & X_1 \\ X_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & X_{n-1} \\ X_{n-1} & X_{n-2} & \cdots & X_0 \end{vmatrix}.$$

The proof of Theorem A.13.7 shows

$$\Theta(G) = \prod_{\chi \in \mathrm{Irr}(G)} \Big(\sum_{g \in G} \chi(g) X_g \Big) = \prod_{i=0}^{n-1} \Big(\sum_{j=0}^{n-1} \zeta^{ij} X_j \Big),$$

where $\zeta = e^{2\pi \mathrm{i}/n} \in \mathbb{C}$. Setting $X_1 = 1$ and $X_i = 0$ for $i \neq 1$, one obtains the permutation matrix of an n-cycle with determinant $\zeta^{0+1+\ldots+n-1} = \zeta^{n(n-1)/2} = (-1)^{n-1}$.

A.14 Frobenius-Schur Indicators

Remark A.14.1. In the following, let G be a finite group. It frequently happens that the character of a representation $\Delta\colon G \to \mathrm{GL}(n,\mathbb{C})$ takes only real values, although Δ is not similar to any $\mathbb{R}$-representation $G \to \mathrm{GL}(n,\mathbb{R})$. In this section, we introduce an invariant of χ that indicates whether Δ is similar to an $\mathbb{R}$-representation. As an application, one obtains a formula for the number of square roots of a group element.

Definition A.14.2. Let V be a $\mathbb{C}G$-module and $W := V \otimes V$. According to Theorem III.3.18, $f\colon W \to W$, $v \otimes w \mapsto w \otimes v$ defines a homomorphism of $\mathbb{C}G$-modules. In particular,

$$S^2(V) := \mathrm{Ker}(f - \mathrm{id}_W), \qquad A^2(V) := \mathrm{Ker}(f + \mathrm{id}_W)$$

are $\mathbb{C}G$-modules. One calls $S^2(V)$ the *symmetric square* and $A^2(V)$ the *alternating square* of V. Because of $v \otimes w = \frac{1}{2}(v \otimes w + w \otimes v) + \frac{1}{2}(v \otimes w - w \otimes v)$, we have $W = S^2(V) \oplus A^2(V)$.

Lemma A.14.3. *Let V be a $\mathbb{C}G$-module with character χ. Then $S^2(V)$ has the character $\chi_s(g) := \frac{1}{2}(\chi(g)^2 + \chi(g^2))$ and $A^2(V)$ has the character $\chi_a(g) := \frac{1}{2}(\chi(g)^2 - \chi(g^2))$ for $g \in G$.*

Proof. Let $b_1, \ldots, b_n$ be a basis of V and $gb_i = \sum_{j=1}^n \lambda_{ji} b_j$ for $g \in G$ and $\lambda_{ji} \in \mathbb{C}$. Then $\chi(g) = \sum_{i=1}^n \lambda_{ii}$ and $\chi(g^2) = \sum_{i,j=1}^n \lambda_{ij}\lambda_{ji}$. Furthermore, $\{b_i \otimes b_j - b_j \otimes b_i : i < j\}$ is a basis of $A^2(V)$ and

$$g(b_s \otimes b_t - b_t \otimes b_s) = \sum_{i,j=1}^n (\lambda_{is}\lambda_{jt} - \lambda_{it}\lambda_{js}) b_i \otimes b_j = \sum_{i<j} (\lambda_{is}\lambda_{jt} - \lambda_{it}\lambda_{js})(b_i \otimes b_j - b_j \otimes b_i).$$

This shows

$$\chi_a(g) = \frac{1}{2} \sum_{s,t=1}^n (\lambda_{ss}\lambda_{tt} - \lambda_{st}\lambda_{ts}) = \frac{1}{2}(\chi(g)^2 - \chi(g^2)).$$

The formula for $\chi_s(g)$ follows from $V = S^2(V) \oplus A^2(V)$. □

Definition A.14.4. For $\chi \in \mathrm{Irr}(G)$, one calls

$$\epsilon(\chi) := \frac{1}{|G|} \sum_{g \in G} \chi(g^2)$$

the *Frobenius-Schur indicator* of χ.

Remark A.14.5. Obviously, $\theta\colon G \to \mathbb{C}$, $g \mapsto |\{x \in G : x^2 = g\}|$ is a class function with

$$(\chi, \theta) = \frac{1}{|G|} \sum_{g \in G} \sum_{\substack{x \in G \\ x^2 = g}} \chi(x^2) = \frac{1}{|G|} \sum_{x \in G} \chi(x^2) = \epsilon(\chi)$$

for $\chi \in \mathrm{Irr}(G)$. Therefore,

$$\boxed{|\{x \in G : x^2 = g\}| = \sum_{\chi \in \mathrm{Irr}(G)} \epsilon(\chi)\chi(g)}$$

holds for $g \in G$.

Example A.14.6.

(i) If $\chi(1) = 1$, then χ is a homomorphism and one obtains $\epsilon(\chi) = (\chi^2, \mathbb{1}_G) = (\chi, \overline{\chi}) = 1$ if $\chi = \overline{\chi}$ and $\epsilon(\chi) = 0$ otherwise. In particular, $\epsilon(\mathbb{1}_G) = 1$.

(ii) If $|G|$ is odd, then $G \to G$, $g \mapsto g^2$ is a bijection. It follows that $\theta = \mathbb{1}_G$, i. e. $\epsilon(\chi) = 0$ for $\chi \neq \mathbb{1}_G$.

(iii) According to Exercise I.26, the quaternion group $G = Q_8$ has exactly one involution. Because of $G/G' \cong C_2^2$, $\mathrm{Irr}(G)$ consists of four real linear characters and one character χ of degree 2 (Lemma II.14.42). According to Remark A.14.5,

$$2 = |\{x \in G : x^2 = 1\}| = 4 + 2\epsilon(\chi)$$

and $\epsilon(\chi) = -1$ holds.

Theorem A.14.7. *For all $\chi \in \mathrm{Irr}(G)$, $\epsilon(\chi) \in \{-1, 0, 1\}$ and*

$$\epsilon(\chi) = (\chi_s - \chi_a, \mathbb{1}_G) = \begin{cases} 0 & \text{if } \overline{\chi} \neq \chi, \\ 1 & \text{if } (\chi_s, \mathbb{1}_G) = 1, \\ -1 & \text{if } (\chi_a, \mathbb{1}_G) = 1. \end{cases}$$

Proof. According to Lemma A.14.3, $0 \leq (\chi_s, \mathbb{1}_G) + (\chi_a, \mathbb{1}_G) = (\chi^2, \mathbb{1}_G) = (\chi, \overline{\chi}) \leq 1$ holds. The assertion follows from this. □

Remark A.14.8.

(i) Let $V = \mathbb{C}^n$ be a $\mathbb{C}G$-module with standard scalar product $[v, w] := v^{\mathrm{t}}\overline{w} = \sum_{i=1}^n v_i\overline{w_i}$ for $v, w \in V$ (positive definite hermitian sesquilinear form). Then

$$\beta(v, w) := \sum_{g \in G} [gv, gw]$$

defines a G-invariant scalar product, i. e. $\beta(gv, gw) = \beta(v, w)$ for all $v, w \in V$ and $g \in G$. By the Gram-Schmidt process, V has an orthonormal basis $b_1, \ldots, b_n$ with respect to β. Let $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ be the representation of V with respect to $b_1, \ldots, b_n$. For the standard basis $e_1, \ldots, e_n \in \mathbb{C}^n$ it then holds that

$$e_i^{\mathrm{t}}\Delta(g)^{\mathrm{t}}\overline{\Delta(g)}e_j = \beta(gb_i, gb_j) = \beta(b_i, b_j) = \delta_{ij} \qquad (1 \leq i, j \leq n).$$

Thus $\Delta(g)$ is a unitary matrix, i. e. $\Delta(g)^{\mathrm{t}}\overline{\Delta(g)} = 1_n$. Every representation is therefore similar to a *unitary representation*

$$G \to \mathrm{GU}(n, \mathbb{C}) := \{A \in \mathrm{GL}(n, \mathbb{C}) : A^{\mathrm{t}}\overline{A} = 1_n\}.$$

(ii) Let $\beta' \colon V \times V \to \mathbb{C}$ also be a G-invariant scalar product. For $v, w \in V$ let $\beta_v(w) := \beta(v, w)$. Obviously $\gamma \colon V \to V^*$, $v \mapsto \beta_v$ is linear. Because of $\beta_v(v) > 0$ for $v \neq 0$ and $\dim V = \dim V^*$, γ is an isomorphism. Analogously there exists an isomorphism $\gamma' \colon V \to V^*$, $v \mapsto \beta'_v$. Therefore $\sigma := \gamma^{-1} \circ \gamma' \in \mathrm{GL}(V)$ with

$$\beta(\sigma(v), w) = \beta_{\sigma(v)}(w) = \gamma(\sigma(v))(w) = \gamma'(v)(w) = \beta'(v, w)$$

for all $v, w \in V$. For $g \in G$ it follows that

$$\beta(\sigma(gv), gw) = \beta'(gv, gw) = \beta'(v, w) = \beta(\sigma(v), w) = \beta(g\sigma(v), gw).$$

Therefore $\sigma(gv) = g\sigma(v)$ and $\sigma \in \mathrm{C}_{\mathrm{GL}(V)}(\Delta(G))$. If V is simple, then $\sigma \in \mathbb{C}^\times \mathrm{id}_V$ follows from Theorem II.14.47, i. e. β is uniquely determined up to a constant factor.

(iii) We now investigate when a G-invariant bilinear form exists on V.

Theorem A.14.9. *Let V be an irreducible $\mathbb{C}G$-module with character χ. Then:*

(1) V possesses a non-trivial symmetric G-invariant bilinear form if and only if $\epsilon(\chi) = 1$.

(2) V possesses a non-trivial alternating G-invariant bilinear form if and only if $\epsilon(\chi) = -1$.

(3) V possesses no non-trivial G-invariant bilinear form if and only if $\epsilon(\chi) = 0$.

Proof. According to the universal property of the tensor product (Theorem III.3.18), every G-invariant bilinear form $V \times V \to \mathbb{C}$ corresponds to a $\mathbb{C}G$-homomorphism $V \otimes V \to \mathbb{C}$. A non-trivial bilinear form therefore exists if and only if $\mathbb{1}_G$ occurs in $\chi^2 = \chi_s + \chi_a$. If $\mathbb{1}_G$ occurs in χ_s, then a homomorphism $f \colon S^2(V) \to \mathbb{C}$ corresponds to a symmetric bilinear form

$$V \times V \to \mathbb{C}, \qquad (v, w) \mapsto f(v \otimes w + w \otimes v).$$

Conversely, if $\beta \colon V \times V \to \mathbb{C}$ is a non-trivial symmetric G-invariant bilinear form, then

$$S^2(V) \to \mathbb{C}, \qquad v \otimes w + w \otimes v \mapsto \beta(v, w) + \beta(w, v) = 2\beta(v, w)$$

is a non-trivial homomorphism, i. e. $\mathbb{1}_G$ occurs in χ_s. The claim for alternating bilinear forms is proven analogously. □

Theorem A.14.10. *For $\chi \in \mathrm{Irr}(G)$, $\epsilon(\chi) = 1$ holds if and only if there exists an $\mathbb{R}G$-module with character χ.*

Proof. Let V be an $\mathbb{R}G$-module with character χ and basis $b_1, \ldots, b_n$. Then $\hat{V} := \mathbb{C} \otimes V = \mathbb{C}b_1 + \ldots + \mathbb{C}b_n$ is a $\mathbb{C}G$-module with character χ (keyword: extension of scalars). For $v = \sum_{i=1}^n v_i b_i$ and $w = \sum_{i=1}^n w_i b_i$ in $\hat{V}$, $[v, w] := \sum_{i=1}^n v_i w_i$ defines a symmetric bilinear form on V. Obviously,

$$\beta(v, w) := \sum_{g \in G} [gv, gw] \in \mathbb{C}$$

defines a symmetric G-invariant bilinear form. Because $gb_1 \in V$ for $g \in G$, it holds that $\beta(b_1, b_1) > 0$. In particular, β is non-trivial. From Theorem A.14.9 it follows that $\epsilon(\chi) = 1$.

Conversely, let $\epsilon(\chi) = 1$ and V be a $\mathbb{C}G$-module with character χ and basis $b_1, \ldots, b_n$. According to Theorem A.14.7, $\overline{\chi} = \chi$. For $g \in G$, let $gb_k = \sum_{j=1}^{n} (\lambda_{jk} + \mathrm{i}\mu_{jk}) b_j$ with $\lambda_{jk}, \mu_{jk} \in \mathbb{R}$ for $j, k = 1, \ldots, n$. Then $\hat{V} := \mathbb{R}b_1 + \mathbb{R}\mathrm{i}b_1 + \ldots + \mathbb{R}b_n + \mathbb{R}\mathrm{i}b_n$ is an $\mathbb{R}G$-module with character

$$\hat{\chi}(g) = 2 \sum_{j=1}^{n} \lambda_{jj} = \chi(g) + \overline{\chi}(g) = 2\chi(g)$$

for $g \in G$. It therefore suffices to show that $\hat{V}$ is not simple. Let $f \colon \hat{V} \to V$, $\lambda b_j + \mu \mathrm{i} b_j \mapsto (\lambda + \mathrm{i}\mu) b_j$ be the canonical isomorphism of $\mathbb{R}$-vector spaces. For $v \in \hat{V}$ and $g \in G$, it holds that $f(gv) = gf(v)$ (even if V is not an $\mathbb{R}G$-module). According to Theorem A.14.9, there exists a non-trivial symmetric G-invariant bilinear form $\beta \colon V \times V \to \mathbb{C}$. By

$$\hat{\beta} \colon \hat{V} \times \hat{V} \to \mathbb{R}, \qquad (v, w) \mapsto \mathrm{Re}\big(\beta(f(v), f(w))\big)$$

one obtains a symmetric G-invariant bilinear form on $\hat{V}$. Since β is non-trivial, there exist $v, w \in V$ with $\beta(v, w) \neq 0$. Because $\beta(v+w, v+w) = \beta(v, v) + 2\beta(v, w) + \beta(w, w)$, there exists $v \in V$ with $\beta(v, v) \neq 0$. After normalization, $\beta(v, v) = 1$ and $\beta(\mathrm{i}v, \mathrm{i}v) = -1$ hold. For $\hat{v} := f^{-1}(v)$ and $\hat{w} := f^{-1}(v + \mathrm{i}v)$, it holds that $\hat{\beta}(\hat{v}, \hat{v}) = 1$ and

$$\hat{\beta}(\hat{w}, \hat{w}) = \mathrm{Re}\big(\beta(v, v) + 2\mathrm{i}\beta(v, v) - \beta(v, v)\big) = 0.$$

Therefore, $\hat{\beta}$ is non-trivial and $\{v \in \hat{V} : \hat{\beta}(v, v) = 0\}$ is a non-trivial submodule of $\hat{V}$. In particular, $\hat{V}$ is not simple. □

Example A.14.11. According to Example A.14.6 and Theorem A.14.10, there is no faithful (and thus irreducible) representation of the form $Q_8 \to \mathrm{GL}(2, \mathbb{R})$, i. e. Q_8 is not isomorphic to any subgroup of $\mathrm{GL}(2, \mathbb{R})$ (cf. Exercise I.26). On the other hand, $D_8 \leq \mathrm{GL}(2, \mathbb{R})$. According to Exercise II.69, the Frobenius-Schur indicators can therefore not be read from the character table.

Remark A.14.12.

(i) Let V be a simple $\mathbb{C}G$-module with character χ and $\epsilon(\chi) = -1$. Then there exists a non-trivial alternating G-invariant bilinear form $\beta \colon V \times V \to \mathbb{C}$. Since V is simple, β is non-degenerate, i. e. for all $v \in V \setminus \{0\}$ there exists a $w \in V$ with $\beta(v, w) \neq 0$ (otherwise $\{v \in V : \beta(v, V) = 0\}$ would be a non-trivial proper submodule of V). By induction on $\dim V$ it can be shown that V possesses a so-called *symplectic* basis of the form $b_1, c_1, \ldots, b_n, c_n$ with $\beta(b_i, b_j) = 0 = \beta(c_i, c_j)$ and $\beta(b_i, c_j) = \delta_{ij}$ for $i, j = 1, \ldots, n$.[1] In particular, $\chi(1) = \dim V = 2n$ is even.

(ii) For the Schur index of $\chi \in \mathrm{Irr}(G)$ it holds that $m_{\mathbb{R}}(\chi) = 2 \iff \epsilon(\chi) = -1$ (see proof of Theorem A.14.10).

Theorem A.14.13. *Let V be a simple $\mathbb{C}G$-module with character χ and basis $b_1, \ldots, b_n$. Let $\hat{V}$ be the corresponding $\mathbb{R}G$-module with basis $b_1, \mathrm{i}b_1, \ldots, b_n, \mathrm{i}b_n$ and character $\chi + \overline{\chi}$. Then*

$$\mathrm{End}_{\mathbb{R}G}(\hat{V}) \cong \begin{cases} \mathbb{R}^{2\times 2} & \text{if } \epsilon(\chi) = 1, \\ \mathbb{C} & \text{if } \epsilon(\chi) = 0, \\ \mathbb{H} & \text{if } \epsilon(\chi) = -1. \end{cases}$$

[1] See lecture notes combinatorial group theory.

Proof. In the case $\epsilon(\chi) = 1$, $\hat{V}$ decomposes into two isomorphic absolutely irreducible $\mathbb{R}G$-modules with character χ (cf. proof Theorem A.14.10). Lemma II.7.20 and Theorem II.14.47 show $\mathrm{End}_{\mathbb{R}G}(\hat{V}) \cong \mathbb{R}^{2\times 2}$. Now let $\epsilon(\chi) = 0$, i. e. $\overline{\chi} \neq \chi$. Then $\hat{V}$ is simple and $\mathrm{End}_{\mathbb{R}G}(V)$ is an $\mathbb{R}$-division algebra. Otherwise $\hat{V}_{\mathbb{C}}$ decomposes into two non-isomorphic simple modules with character χ and $\overline{\chi}$ respectively. From Lemma III.7.59 and Lemma II.7.20 it follows that

$$\dim_{\mathbb{R}} \mathrm{End}_{\mathbb{R}G}(\hat{V}) = \dim_{\mathbb{C}} \mathrm{End}_{\mathbb{C}G}(\hat{V}_{\mathbb{C}}) = \dim_{\mathbb{C}}(\mathbb{C} \times \mathbb{C}) = 2.$$

By Theorem III.7.27 it holds that $\mathrm{End}_{\mathbb{R}G}(\hat{V}) \cong \mathbb{C}$. Finally, let $\epsilon(\chi) = -1$. Then $\hat{V}_{\mathbb{C}}$ decomposes into two isomorphic simple modules with character $\chi = \overline{\chi}$. Thus $\dim_{\mathbb{R}} \mathrm{End}_{\mathbb{R}G}(\hat{V}) = 4$ and $\mathrm{End}_{\mathbb{R}G}(\hat{V}) \cong \mathbb{H}$ by Theorem III.7.27. □

GAP Commands

Many calculations can be performed in the free computer algebra system GAP[1]:

Object	Code
Division of a by d with remainder	`QuoInt(a,d); RemInt(a,d); a mod d;`
Euclidean algorithm $\gcd(a,b) = ax + by$	`Gcd(a,b); Gcdex(a,b);`
$\operatorname{lcm}(a,b)$	`Lcm(a,b);`
$a \in \mathbb{P}$?	`IsPrime(a);`
Prime factorization of a	`Factors(a);`
Solution of $ax \equiv b \pmod{d}$	`a^-1*b mod d;`
Chinese Remainder Theorem	`ChineseRem([d1,d2],[a1,a2]);`
ISBN check digit	`CheckDigitISBN(n);`
$\varphi(n)$	`Phi(n);`
$\mu(n)$	`MoebiusMu(n);`
Jacobi symbol $\left(\frac{a}{n}\right)$	`Jacobi(a,n);`
S_n	`SymmetricGroup(n);`
A_n	`AlternatingGroup(n);`
D_{2n}	`DihedralGroup(2*n);`
Decomposition into disjoint cycles	`(1,2,3)*(3,5,1);`
$\operatorname{sgn}(a)$	`SignPerm(a);`
$G := \langle a,b \rangle$ for permutations a,b	`G:=Group(a,b);`
$\lvert G \rvert$	`Order(G); Size(G);`
$\lvert \langle x \rangle \rvert$	`Order(x);`
G abelian, cyclic?	`IsAbelian(G); IsCyclic(G);`
$H \leq G$?	`IsSubgroup(G,H);`
$\lvert G : H \rvert$	`Index(G,H);`
Hg	`RightCoset(g,H);`
$\langle U,V \rangle$ for $U,V \leq G$	`ClosureGroup(U,V);`
UV for $U,V \subseteq G$	`SetX(U,V,PROD);`
$U \cap V$	`Intersection(U,V);`
$N \trianglelefteq G$?	`IsNormal(G,N);`
G/N	`G/N;`
canonical epimorphism $G \to G/N$	`NaturalHomomorphismByNormalSubgroup(G,N);`

[1] `https://www.gap-system.org/`

Object	Code
Isomorphism type of G (if sensible)	`StructureDescription(G);`
$G \cong H$?	`IsIsomorphicGroup(G,H);`
$G \times H$	`DirectProduct(G,H);`
Orbits of the G-set M	`Orbits(G,M);`
Conjugacy classes of G	`ConjugacyClasses(G); Orbits(G,G);`
$k(G)$	`NrConjugacyClasses(G);`
g and h conjugate in G?	`IsConjugate(G,g,h);`
$\mathrm{C}_G(g)$, $\mathrm{C}_G(H)$	`Centralizer(G,g); Centralizer(G,H);`
$\mathrm{N}_G(H)$	`Normalizer(G,H);`
G_x	`Stabilizer(G,x);`
$\mathrm{Z}(G)$	`Center(G);`
$P \in \mathrm{Syl}_p(G)$	`P:=SylowSubgroup(G,p);`
G simple, solvable?	`IsSimple(G); IsSolvable(G);`
non-solvable groups G with $\|G\| \leq 60$	`AllGroups([1..60],IsSolvable,false);`
Composition series of G	`CompositionSeries(G);`
$\mathrm{Aut}(G)$	`AutomorphismGroup(G);`
$\mathrm{GL}(n,q)$, $\mathrm{SL}(n,q)$	`GL(n,q); SL(n,q);`
$\mathbb{Z}$	`Integers;`
$\mathbb{Q}$	`Rationals;`
$\mathbb{F}_q$	`GF(q);`
$\mathbb{Z}/n\mathbb{Z}$	`ZmodnZ(n);`
$R^\times$	`Units(R);`
$(a,b) \trianglelefteq R$	`Ideal(R,[a,b]);`
$a = X^2 + 3X - 1 \in K[X]$	`x:=X(K,"X"); a:=x^2+3*x-1;`
Coefficients of a	`CoefficientsOfUnivariatePolynomial(a);`
$a(y)$ for $y \in K$	`Value(a,y);`
Roots of a in K	`RootsOfPolynomial(K,a);`
$\deg a$	`Degree(a);`
$\gcd(a,b) = ax + by$ in $K[X]$	`Gcd(a,b); GcdRepresentation(a,b);`
$a \in K[X]$ irreducible?	`IsIrreducible(a);`
Prime factorization in $K[X]$	`Factors(a);`
$I_n(q)$ (Exercise I.61)	`IrreduciblePolynomialsNr(n,q);`
Derivative a'	`Derivative(a);`
Minimal polynomial of $a \in L$ over K	`MinimalPolynomial(K,a);`
$K(a)$	`Field(K,a); Field(a);`
Splitting field of $a \in K[X]$	`SplittingField(a);`
$\sqrt{a}$	`Sqrt(a);`
primitive n-th root of unity z	`z:=E(n);`
Φ_n	`CyclotomicPolynomial(Rationals,n);`

Object	Code
$\mathbb{Q}_n$	`CyclotomicField(Rationals,n); CF(n);`
Gal$(K\|P(K))$	`GaloisGroup(K);`
Gal(a) for $a \in \mathbb{Q}[X]$ as permutation group	`TransitiveGroup(Degree(a),GaloisType(a));`
Discriminant of $a \in \mathbb{Q}[X]$	`Discriminant(a);`
Smith normal form of A	`SmithNormalFormIntegerMat(A);`
Frobenius normal form of A	`S:=RationalCanonicalFormTransform(A);;`
	`S^-1*A*S;`
Normal basis of K over $P(K)$	`NormalBase(K);`
Group algebra KG	`GroupRing(K,G);`
Augmentation ideal $I(KG)$	`AugmentationIdeal(KG);`
Jacobson radical J(KG)	`RadicalOfAlgebra(KG);`
Artin-Wedderburn decomposition of KG	`WedderburnDecomposition(KG);`
irreducible representations of G over K	`IrreducibleRepresentations(G,K);`
Character table of G	`Display(CharacterTable(G));`
Resultant of a, b w.r.t. X	`Resultant(a,b,x);`
Division of a by b, c in $K[X_1, \ldots, X_n]$	`PolynomialReduction(a,[b,c],MonomialLexOrdering);`
Gröbner basis of (b, c)	`GrobnerBasis([b,c],MonomialLexOrdering);`
reduced Gröbner basis	`ReducedGrobnerBasis([b,c],MonomialGrlexOrdering);`
H_7	`LoadPackage("guava"); C:=HammingCode(3,GF(2));`
G_{24}	`ExtendedBinaryGolayCode();`
$\dim C$	`Dimension(C);`
$d(C)$	`MinimumDistance(C);`
$C^{\perp}$	`DualCode(C);`
$W_C(X)$	`WeightDistribution(C);`
Generator matrix	`GeneratorMat(C);`
Check matrix	`CheckMat(C);`
cyclic codes	`CyclicCodes(n,GF(q));`

Index

Symbols
(χ, ψ), 221
$\mathbb{1}_G$, 221
$a \mid b$, 9
$\alpha \mid \beta$, 54
$A^2(V)$, 515
ad, 370
$\mathrm{A}(K^n)$, 261
A^b, 200
Ab, 316
$a \equiv b \pmod{d}$, 12
$\alpha \equiv \beta \pmod{\gamma}$, 54
$a + d\mathbb{Z}$, 13
$\mathrm{Alg}_K(A, K)$, 416
A_n, *26*, 42
$\mathrm{Ann}_R(M)$, 152
$A \sim B$, 169
$A \otimes_R B$, 244
$a \otimes b$, 244
$\mathrm{Aut}(G)$, 25
$\mathrm{Aut}(\mathbb{C})$, 59
$\mathrm{Aut}(K)$, 59
$\mathrm{Aut}(\mathbb{Q})$, 109
$\mathrm{Aut}(\mathbb{R})$, 109
$B^2(G, L^\times)$, 349
B_α, 175
β_λ, 312
$\mathrm{Br}(K)$, 343
$\mathrm{Br}(L|K)$, 347
$\mathbb{C}$, 9
C^+, 216
$C(A)$, 200
$\mathcal{C} \approx \mathcal{D}$, 321
$\mathrm{CF}(G)$, 221
$\mathrm{C}_G(H)$, 30
$\mathrm{C}_G(g)$, 30
$C^\perp$, 438
$\mathrm{char}\, K$, 73
χ_λ, 301
$\mathrm{Cl}(G)$, 221
C_n, 28
$C^n(G, L^\times)$, 349
$\mathcal{C}^o$, 316
$A \cong_{\mathcal{C}} B$, 316
$\mathrm{conv}(S)$, 464
$\mathcal{C}/\!\sim$, 318
D_{2n}, 103
$\mathcal{D}^{\mathcal{C}}$, 319
$\dim R$, 256
D_α, 94
$\deg \alpha$, 52
$\deg A$, 354
$\Delta \oplus \Gamma$, 219
$\mathrm{Der}(L)$, 454
$\det \chi$, 221
$e(A)$, 354
E_{ij}, 161
$\mathrm{End}_R(M)$, 145
$e_p(P)$, 190
$\epsilon(\chi)$, 515
ϵ_q, 357
$\exp(\delta)$, 454
$\mathbb{F}_4$, 75
$\mathbb{F}_p$, 47
$f_p(P)$, 190
$\mathbb{F}_q$, 74
$\overline{\mathbb{F}_p}$, 87
G', 105
$G_1 \times \ldots \times G_n$, 20
$N_1 \oplus \ldots \oplus N_k$, 36
G_{23}, 441
G_{24}, 441
gH, 20
G/H, 20
$|G : H|$, 20
$G \cong H$, 25
$\mathrm{GL}(n, K)$, 20
$\mathfrak{gl}(V)$, 368
$\mathfrak{gl}(n, K)$, 368
$\mathrm{GL}(n, R)$, 168
$\mathrm{cd}(a_1, \ldots, a_n)$, 10
$\mathrm{GU}(n, \mathbb{C})$, 516
$\mathrm{Gal}(L|K)$, 67
$\Gamma(A)$, 207
$\gamma(A)$, 204
$\gcd(n, m)$, 12
$\gcd(a_1, \ldots, a_n)$, 10, 55, 138
Grp, **grp**, 316
$\mathbb{H}$, 108
$H^2(G, L^\times)$, 349
$H \leq G$, $H < G$, 20
H_G, 103
H^G, 103
$H \trianglelefteq G$, $H \lhd G$, 23

$h(P)$, 256
h_{st}, 306
$\mathrm{Hom}_{\mathcal{C}}(A,B)$, 315
$\mathrm{Hom}_G(S,L)$, 416
$\mathrm{Hom}_R(M,N)$, 145
H_{st}, 306
Hg, 22
$(I{:}S)$, 254
$\mathcal{I}(A)$, 261
$I(KG)$, 214
$I \trianglelefteq R$, $I \lhd R$, 46
I^{-1}, 186
$\mathrm{Inn}(G)$, 30, 104
$\mathrm{Irr}(G)$, 221
$\mathrm{Irr}_K(G)$, 221
$\mathrm{J}(M)$, 158
$K(A)$, 264
$K[A]$, 263
$k(G)$, 30
K-**mat**, 316
$K(X)$, 53
$K(X_i : i \in I)$, 124
$K[X]$, 52
$K[X_1, \ldots, X_n]$, 92
$K[X_i : i \in I]$, 119
$K[X]^{\times}$, 53
$K[[X]]$, 240
$K((X))$, 240
$K(\chi)$, 233
$K_e(x)$, 430
$\mathrm{Ker}(\chi)$, 225
$\mathrm{lcm}(n,m)$, 12
$\mathrm{lcm}(a_1, \ldots, a_n)$, 11, 138
$K(n)$, 304
L', 369
$L(G)$, 455
L^H, 67
$|L : K|_s$, 123
$\mathrm{lm}\,\alpha$, 270
$\mathrm{lm}\,I$, 271
$\lambda^{\pm}$, 306
$\lambda \trianglelefteq \mu$, 297
$\lambda_T^{(k)}$, 304
λ', 298
$\mathfrak{L}_n$, 390
L^{σ}, 67
M_{24}, 443
$m_K(\chi)$, 235
$M \simeq N$, 145
$\mu(n)$, 17
$\mathrm{N}_G(H)$, 30
N_K^L, 410
$\mathrm{N}(L)$, 374
$\mathbb{N}$, 9
$\mathbb{N}_0$, 9
$\mathrm{Ob}(\mathcal{C})$, 315
$\Omega(G)$, 37
$\mho(G)$, 37
$\mathrm{Out}(G)$, 104
$\frac{\partial \alpha}{\partial X_k}$, 482
$\mathrm{PSL}(n,K)$, 43
$\partial\lambda$, 349
$\varphi(n)$, 16
$\Phi(\mathcal{C})$, 317
$\Phi \Rightarrow \Psi$, 319
π, 87
π_{λ}, 301
$P(n)$, 297
$\mathbb{Q}$, 9
$Q(A)$, 362
$\mathbb{Q}_{12}$, 81
$\mathbb{Q}_{15}$, 110
$q(T)$, 299
$\hat{\mathbb{Q}}_p$, 403
Q_{λ}, 299
$\mathbb{Q}_n$, 78
$\mathbb{Q}_{p^{\infty}}$, 425
$\overline{\mathbb{Q}}$, 86
Q_8, 105
$Q(R)$, 107
$\mathbb{Q}(\sqrt{\pi})$, 425
$\mathbb{R}$, 9
$R(A)$, 213
$r(C)$, 432
R_P, 251
RS, 144
$R[S^{-1}]$, 250
${}_RS$, S_R, 417
$R[T]$, 181
$\mathrm{res}(\alpha,\beta)$, 266
$\mathrm{rk}\,M$, 166
${}_R$**Mod**, **Mod**$_R$, ${}_R$**mod**, 316
Rng, 316
R^o, 143
$S^2(V)$, 515
S_K^L, 126
$\mathfrak{sl}(n,K)$, 369
$\mathrm{SL}(n,K)$, 25
S_T, 298
$ST(\lambda)$, 304
$S(\alpha,\beta)$, 266
$\mathrm{Sec}_{p'}(x)$, 277
$\mathrm{Sec}_{p'}(G)$, 277
Set, **set**, 316
$\mathrm{sgn}(\sigma)$, 25
σ_k, 92
S_n, 20
$\mathrm{Soc}(M)$, 242
$\mathrm{Spec}(R)$, 236
$\mathrm{Syl}_p(G)$, 32
$\mathrm{Sym}(\Omega)$, 20
$\mathrm{T}(M)$, 172

$T(\lambda)$, 298
$T(\lambda)/\sim$, 298
$\mathrm{trg}(L|K)$, 131
U^G, 287
$U(L)$, 389
$U(R)$, 45
$U^\perp$, 283
V^*, 283
V_4, 103
$\mathcal{V}(P)$, 261
V_λ, 371
$V \otimes W$, 282
$v \otimes w$, 282
W^-, 299
$W_C(X)$, 443
$\sqrt{I}$, 237
$W_n(A)$, 431
$W_\perp$, 283
$w(x)$, 435
XY, 23
$[x, y]$, 105
ξ_λ, 313
$\mathbb{Z}$, 9
$Z^2(G, L^\times)$, 349
$\mathrm{Z}(G)$, 30
$\mathrm{Z}(R)$, 46
$\mathbb{Z}[X]$, 60
$\mathrm{Z}(\chi)$, 225
$\mathbb{Z}/d\mathbb{Z}$, 13
$(\mathbb{Z}/n\mathbb{Z})^\times$, *47*, 49, 58
$\mathbb{Z}_{[p]}$, 403

A

Abel-Ruffini, 91
abelian, 19
action, 29
  faithful, 29
  transitive, 29
  trivial, 29
adjunction, 63
Ado, 393
Albert-Brauer-Hasse-Noether, 354
algebra, 194
  central, 340
  central simple, 340
  cyclic, 452
  free, 358, 387
  L-separated, 416
  separable, 490
  strongly symmetric, 207
  symmetric, 206
algebraic, 63
algebraic closure, 85
algebraic integer, 181
algebraically (in)dependent, 128
algebraically closed, 84
alternating group, 26
  simplicity, 42
alternating square, 312, 515
Angle trisection, 99
annihilator, 152
Approximation Theorem, 407
Argand, 479
arrow, 357
  inverse, 359
  source, 357
  target, 357
arrow ideal, 358
Artin, 68
Artin-Schreier, 488
Artin-Wedderburn, 156
Artin-Whaples, 407
ASCII code, 435
associated, 135
associative, 19
augmentation ideal, 215
augmentation map, 215
automorphism, 24
  inner, 104
automorphism group
  cyclic group, 49, 108
  inner, 30, 104
  of a code, 435
  of a field, 59
  of a group, 25
  outer, 104
Axiom of Choice, 115

B

b-adic expansion, 101
Baer, 510
Baker, 507
balanced, 330
basic algebra, 200
basic idempotent, 201
basis
  for modules, 165
  for vector spaces, 118
  integral, 185
basis axtension theorem
  for modules over skew fields, 167
basis extension theorem
  for transcendence bases, 130
  for vector spaces, 118
Bauer, 470
Berman, 279
bimodule, 329
block, 163
block algebra, 163
block code, 430
block idempotent, 163
bound

lower, 114
upper, 114
branching rule, 306
Brauer, 278
Brauer group, 343
Brauer's Permutation Lemma, 232
Brauer-Speiser, 235
Brauer-Thrall conjecture, 282
Brauer-Tsushima, 277
Bring-Jerrard, 91
Buchberger algorithm, 273
Buchberger criterion, 272
Burnside's Lemma, 34
Burnside's p^aq^b-Theorem, 226
byte, 435
Bézout, 139

C

cancellation of congruences, 14
cancellation rule, 46
Cantor-Bernstein, 114
Cardano, 8, 90
Carmichael number, 107
Cartan criterion
semisimplicity, 379
solvability, 378
Cartan matrix, 200
Cartan-Jacobson, 421
Casimir operator, 384
casus irreducibilis, 8
category, 315
abelian, 325
automorphism, 316
congruence, 318
dual, 316
epimorphism, 316
equivalent, 321
isomorphism, 316
locally small, 315
monomorphism, 316
small, 315
Cauchy, 33, 106
Cayley, 30
Cayley-Hamilton, 177
center
of a character, 225
of a group, 30
of a ring, 46
centralizer, 30
chain, 114
chain rule, 110
multidimensional, 482
character, 220
(ir)reducible, 220
degree, 220
faithful, 225
linear, 221
regular, 221
trivial, 221
character table, 222
A_5, 314
S_5, 303
characteristic, 73
Chase, 352
Chebotarev's density theorem, 192
check bit, 435
check digit, 14
check polynomial, 444
Chinese Remainder Theorem
for rings, 50
in $\mathbb{Z}$, 15
Christmas puzzle, 109
class, 315
class equation, 31
class function, 221
class group, 188
class number, 30, 188
class sum, 216
Clifford, 294
Clifford correspondence, 295
cocycle, 349
code, 430
ASCII code, 435
binary, 436
corrects errors, 431
cyclic, 444
detects errors, 431
dual, 438
equivalent, 435
extended, 440
generating function, 443
ISBN code, 435
length, 430
linear, 435
MDS code, 434
parity code, 435
perfect, 434
repetition code, 431
self-dual, 438
ternary, 436
trivial, 431
codeword, 430
Cohen, 242
cohomology group, 349
common divisors
in $\mathbb{Z}$, 10
in $K[X]$, 55
common multiple, 11
commutator, 105
commutator algebra, 369
commutator space, 204, 347
companion matrix, 175

complement, 118
completion, 401
composition, 304
composition factor, 43
composition series
    for groups, 43
    for modules, 146
compositum, 71
congruence
    in $\mathbb{Z}$, 12
    in $K[X]$, 54
congruence equations, 14
conjugacy class, 30
conjugation, 30
    complex, 59
constant term, 52
constructible, 96
continuous, 497
convergence
    of filters, 498
convex, 464
convex hull, 464
Conway, 443
coordinate ring, 263
coprime, 138
    in $\mathbb{Z}$, 10
    in $K[X]$, 56
coproduct, 165
corner, 306
correspondence theorem
    for groups, 26
    for modules, 145
coset, 20
critical, 116
cross product, 368
cubic resolvent, 95
cycle, 21
cycle notation, 21
cycle type, 21
cyclic, 19
cyclotomic field, 78
cyclotomic polynomial, 79, 475

D

decoding, 430
Dedekind, 88, 191
Dedekind domain, 186
Dedekind identity, 23
degree
    of a field extension, 63
    of a polynomial, 52
    of a representation, 218
    of an algebra, 354
degree theorem
    for field extensions, 64
    for separability degree, 124
    for transcendence degree, 132
del Ferro, 8, 90
Delian problem, 99
derivation, 454
    inner, 454
derivative, 73
    k-th, 110
    in $K((X))$, 481
    partial, 482
derived subgroup, 105
Descartes' Rule of Signs, 465
DHM key exchange, 13
Diamond lemma, 387
Dickson, 291
Dieudonné, 361
dihedral group, 104
dimension, 119
direct product
    of algebras, 195
    of groups, 20
    of modules, 144
    of rings, 45
direct sum, 36
Dirichlet's prime number theorem, 81, 192
discriminant
    of a basis, 471
    of a polynomial, 94, 268
distance, 430
distributive, 45
divisibility
    in $\mathbb{Z}$, 9
    in $K[X]$, 54
    in integral domains, 135
divisibility rules, 102
division algebra, 194
division ring, 46
    finite, 157
dominance order
    for compositions, 304
Double Centralizer Theorem, 344
double coset, 292
dual space, 283
Dynkin diagram, 366

E

Eilenberg-Nakayama, 347
Eisenstein criterion, *61*, 240, 455
Eisenstein integer, 108
element
    (in)separable, 121
    algebraic, 63
    algebraic integer, 61, *181*
    greatest, 114
    integral, 181
    invertible, 45
    least, 114

maximal, 114
minimal, 114
nilpotent, 46
transcendental, 63
elementary abelian, 77
elementary divisors, 170
elimination ideal, 269
embedding
real/complex, 414
encoding, 430
endomorphism, 24
endomorphism ring, 145
Engel, 374
epimorphism, 24
canonical, 25
for rings, 49
equivalence
of categories, 321
of matrices, 169
Euclid, 12
Euclidean division
in $\mathbb{Z}$, 9
in $K[X]$, 55
Euler-Fermat, 48
Euler's φ-function, 16
formula, 17
evaluation homomorphism, 54
Exchange Theorem
for modules over skew fields, 167
for transcendence bases, 130
Extended Euclidean algorithm
in $\mathbb{Z}$, 10
in $K[X]$, 55
runtime, 102
extension of scalars, 346
Extension Theorem, 65, 422

F

factor group, 24
of abelian group, 105
of cyclic group, 28
factor module, 145
factor system, 349
normalized, 349
Fein, 235
Fein-Yamada, 235
Feit-Thompson, 43
Fermat prime, 99, 101
Fermat's Last Theorem, 57
Ferrari, 8, 90
field extension, 63
(in)separable, *121*, 127, 238, 341
absolutely transcendental, 128
algebraic, 63
finite, 63
finitely generated, 480
normal, 239
purely inseparable, 121
purely transcendental, 128
transcendental, 128
field of fractions, 107
universal property, 107
filter, 496
Fitting, 151
Five Lemma, 451
fixed field, 67
forgetful functor, 317
Frattini argument, 32
Freshman's Dream, 74
Fried, 485
Frobenius, 226, 513
Frobenius element, 192
Frobenius group, 227
Frobenius homomorphism, 74
Frobenius normal form, 176
Frobenius reciprocity, 289
Frobenius-Nakayama reciprocity, 288
Frobenius-Schur indicator, 515
Frobenius-Young, 301
functor, 317
adjoint, 323
constant, 317
contravariant, 318
covariant, 318
equivalence, 321
faithful, 317
full, 317
isomorphic, 319
isomorphism, 318
functor category, 319
fundamental equation, 190
fundamental theorem
finite abelian groups, 37
finitely generated abelian groups, 174
Galois theory, *69*, 416, 427
of algebra, 85
symmetric polynomials, 92
symmetric rational functions, 133

G

G-set, 29
Gabriel, 366
Galois, 90
Galois conjugate, 232
Galois extension, 68
for skew fields, 419
infinite, 424
Galois group
absolute, 424
of a field extension, 67
of a polynomial, 89
Galois splitting field, 348

Garnir element, 305
Gauss
construction of n-gon, 99
cyclotomic polynomial, 80
factorial rings, 140
lemma, 60
period length, 107
unit group, 58
Gauss sum, 461
Gauss-Lucas, 464
Gaussian integers, 141
Geck, 479
general linear group, 20
generating set
of groups, 20
of modules, 144
generator, 333
generator matrix, 437
generator polynomial, 444
Gershgorin, 467
Geyer, 485
Gilbert bound, 434
Girard-Newton identities, 94
Glass-Ng, 308
Golay code
(extended) binary, 441
(extended) ternary, 442
grading, 358
greatest common divisor
in $\mathbb{Z}$, 10
in $K[X]$, 55
in factorial rings, 138
Green's Indecomposability Theorem, 295
Greiter, 474
Griesmer bound, 437
group, 19
abelian, 19
cyclic, 19
free abelian, 165
isomorphic, 25
nilpotent, 37
of Lie type, 43
order pq, 41
order 4, 38
order 6, 38
order 8, 105
order 12, 33
order 15, 33
profinite, 498
residually finite, 426
simple, 40
classification, 43
solvable, 40, 44
sporadic, 43
topological, 498
trivial, 19
group algebra, 214
crossed, 351
group determinant, 512
Gröbner, 271
Gröbner basis, 271
reduced, 274

H

Hadamard matrix, 431
Hall, 291
Hall's Marriage Theorem, 116
Hamel basis, 118
Hamilton, 108
Hamming bound, 433
Hamming code, 439
Hamming distance, 430
Hausdorff space, 497
Heegner numbers, 184
height, 256
Hensel's Lemma, 408
Hermite normal form, 171
Herstein, 348
Higman, 246, 293
Higman ideal, 207
Hilbert, 193
Basis Theorem, 250
Nullstellensatz, 261
Theorem 90, 487
Hom-functor, 318
homeomorphism, 406, 497
homomorphism
dual, 284
of algebras, 194
of fields, 59
of groups, 24
of modules, 145
of rings, 48
homomorphism theorem
for categories, 319
for groups, 26
for modules, 145
for rings, 49
hook, 306
Hook length formula, 308
Hopkins-Levitzki, 160
Horner scheme, 54
hypersurface, 265

I

ideal, 46
admissible, 360
fractional, 185
generated, 47
invertible, 186
maximal, 46
nilpotent, 160

primary, 253
ideal group, 188
idempotent, 45
lifting, 196
orthogonal, 161
primitive, 161
identity, 315
identity element, 19
identity functor, 317
indeterminate, 52
index, 20, 354
inertia degree, 190
inflation, 223
information rate, 432
injection, 324
integral closure, 183
integral domain, 45
finite, 106
integral ring extension, 181
integrally closed, 183
interpolation, 57
inverse element, 19
Inverse Galois problem, 82, 428, 484
irreducible, 56, 136
ISBN, 14
ISBN code, 435
isomorphism, 24
isomorphism theorems
for groups, 26
for modules, 146
for rings, 50
Iwasawa, 392

J

Jacobi identity, 367
Jacobi symbol, 460
Jacobian matrix, 483
Jacobson, 392, 509
Jacobson radical, 158
Jacobson's Density Theorem, 164
James' Submodule Theorem, 300
Jordan-Chevalley decomposition, 377, 493
Jordan-Hölder, 43

K

K-isomorphism, 63
Kaplansky, 198
Kasch, 422
kernel
of a character, 225
of group homomorphisms, 24
of ring homomorphisms, 49
Killing form, 378
Klein four-group, 103
Knapp-Schmid, 226
Koh, 196
Korselt, 107
Kostka number, 302
Krasner's Lemma, 412
Kronecker, 66, 474
Kronecker coefficient, 303
Kronecker criterion, 483
Kronecker product, 228
Kronecker transformation, 483
Kronecker-Weber, 82
Krull, 427
Height Theorem, 258
Intersection Theorem, 256
maximal ideals, 119
Principal Ideal Theorem, 257
Krull dimension, 256
Krull topology, 427
Krull-Schmidt, 151
Kummer, 88, 486
Kürschák, 413

L

Lagrange, 22
for profinite groups, 501
Lagrange polynomial, 57
Lamé, 102
Landau, 106
Lasker-Noether, 254
Laurent polynomial, 251
Laurent series, 240
leading coefficient, 52, 270
leading monomial, 270
least common multiple, 11, 138
left coset, 20
left ideal, 144
left module, 143
Legendre symbol, 460
Leibniz formula, 168
Leibniz rule, 453
length
of a cycle, 21
of an orbit, 29
Leptin, 500
Levi, 386
Lie, 376
Lie algebra, 367
abelian, 367
center, 369
free, 390
general linear, 368
homomorphism, 370
adjoint, 370
ideal, 368
nilpotent, 372
radical, 373
representation, 381
semisimple, 372

simple, 369
solvable, 372
special linear, 369
special orthogonal, 380
symplectic, 380
universal enveloping algebra, 389
Lie bracket, 367
Lie module, 381
adjoint, 381
semisimple, 382
simple, 381
Lie quotient algebra, 369
Lie subalgebra, 368
Lindemann, 87
Lindemann-Weierstraß, 128, *504*
linear factor, 57
linearly (in)dependent
for modules, 165
for vector spaces, 118
Liouville, 86
localization, 251
universal property, 252
Loewy length, 448
logarithm
discrete, 13
loop, 357
Lüroth, 480

M

Mackey formulas, 292
MacWilliams identity, 443
Maschke, 215
Mathieu group, 443
matrix ring, 45
maximal order, 183
maximum norm, 406
McKay, 106
MDS code, 434
minimal polynomial
of a matrix, 175
of an algebraic element, 63
minimum distance, 430
minimum weight, 436
Minkowski, 230
module, 143
Artinian, 147
dual, 283
finitely generated, 144
free, 165
indecomposable, 150
induced, 287
injective, 246
noetherian, 147
projective, 197
projective-indecomposable, 198
regular, 143
self-dual, 283
semisimple, 148
simple, 146
torsion-free, 172
trivial, 143, 215
modulo, 12
Mohr-Mascheroni, 100
monomial, 52
monomial order, 269
monomorphism, 24
Monster group, 43
Morita, 337
Morita context, 334
morphism, 315
codiagonal, 324
diagonal, 324
multiplicatively closed, 250
Murty, 466
Möbius function, 17
Möbius inversion, 17

N

Nagata, 258
Nakayama, 158, 212
Nathanson, 465
natural isomorphism, 319
natural transformation, 319
necklaces, 34
Newton's method, 86
nilpotency class, 373, 454
nilradical, 374
Nine Lemma, 451
Ninot, 418
Noether normalization, 264, 265
Noether-Jacobson, 348
norm, 406
equivalent, 406
norm map, *410*, 452
normal basis, 179
Normal Basis Theorem, 179
normal closure, 423
normal subgroup, 23
normalizer, 30
normed space, 406
Nullstellensatz
Hilbert's, 261
weak, 260
number field, 64

O

object, 315
coproduct, 324
product, 324
open/closed set, 426
orbit, 29
orbit equation, 31

order
of a group, 19
of a permutation, 22
of an element, 20
order relation, 114
orthogonality relations, 223
Ostrowski, 399, 404

P

p-adic integer, 403
p-adic numbers, 403
p-factor, 277
p-group, 31
elementary abelian, 77
order p, 28
order p^2, 31
order p^3, 38
solvable, 41
parity code, 435
parity-check matrix, 437
partial fraction decomposition, 86
partition, 297
symmetric, 298
path, 357, 359
cycle, 357
length, 357
path algebra, 357
Peel, 306
Peirce, 162
perfect, 76
period length, 107
permutation, 20
disjoint, 21
even/odd, 26
permutation module, 218
permutation representation, 218
Perron-Frobenius, 204
pivot, 171
Plotkin bound, 433
Poincaré-Birkhoff-Witt, 389
polynomial, 52
constant, 52
discriminant, 94
elementary symmetric, 92
homogeneous, 307
irreducible, 56
monic, 52, 270
non-commutative, 387
primitive, 60, 139
reducible, 56
separable, 121
solvable, 89
symmetric, 92
universal property, 108
power basis, 179
power series, 240
p'-section, 277
primary decomposition, 255
Prime Avoidance, 258
prime divisor, 11
prime element, 136
prime factorization
for groups, 43
in $\mathbb{Z}$, 12
in $K[X]$, 56
in factorial rings, 138
prime field, 73
prime ideal, 138, 236
associated, 254
height, 256
minimal over, 256
prime ideal factorization, 187
prime number, 11
inert, 142, 191
ramified, 141, 191
split, 142, 191
primitive element, 78
Primitive Element Theorem, 78, 121
primitive root, 57
principal block, 215
principal ideal, 47
in $K[X]$, 58
principal ideal domain, 138
Problems of Antiquity, 98
product category, 316
product rule, 74
product topology, 498
progenerator, 334
projection, 324
projective center, 207
Prüfer group, 149

Q

quadratic reciprocity law, 460
quadratic residue, 460
quaternion division ring, 108
quaternion group, 105
Quillen, 198
quiver, 357
connected, 359
morphism, 365
quotient category, 318
quotient ring, 47
quotient rule, 482

R

Rabinowitsch, 262
radical, 158, 237
of an ideal, 253
radical extension, 89
radical ideal, 253
ramification index, 190, 295

rank, 166
rate, 432
rational functions, 53
reducible, 56
reduction, 387
reduction modulo p, 62
Reed-Solomon code, 446
relation, 362
relative topology, 501
remainder, 9, 271
repetition code, 431
representation, 218
  (ir)reducible, 219
  absolutely irreducible, 230
  direct sum, 219
  dual, 219
  of a Lie algebra, 381
  quiver, 364
    admissible, 365
  regular, 218
  restriction, 219
  similar, 219
  trivial, 218
  unitary, 516
representation type, 282
residue class, 13
  prime, 48
resultant, 266
Reynolds ideal, 213
right cosets, 22
Ring
  factorial, *137*
ring, 45
  Artinian, 155
  commutative, 45
  Euclidean, 140
  factorial, 57
  local, 196
  Morita equivalent, 337
  Noetherian, 155
  opposite, 143
  semisimple, 155
  simple, 160
ring of integers, 183
Roiter, 282
root, 54
  multiplicity, 57
  number of, 57
  rational, 61
  simple/multiple, *57*, 74
root of unity, 78
  primitive, 78
RSA method, 48
R-S-homomorphism, 329
Rubik's Cube, 30

S

Schanuel conjecture, 508
Schanuel's Lemma, 198
Schur, 193, 232, 469
Schur index, 235
Schur polynomial, 312
Schur's Lemma, 146
separability degree, 123
separable, 121
separable closure, 123
separation axiom, 497
sequence
  exact, 450
set
  totally ordered, 114
  well-ordered, 114
Shafarevich, 82
Shannon, 434
sign, 26
signum, 26
simple, 40
Singleton bound, 433
skeleton category, 323
Skolem-Noether, 246, 344, *495*
Smith normal form, 169
socle, 242
solvable, 40
Specht, 306
Specht module, 299
special linear group, 25
spectral radius, 204
spectrum, 236
splitting field, 346
  of a group, 230
  of a polynomial, 65
  of an algebra, 346
Squaring the circle, 98
stabilizer, 29
standard monomial, 275
standard tableau, 304
Steinitz, 66, 481
Stickelberger, 471
Straßmann, 409
structure constants, 195
Sturm, 466
subalgebra, 194
subfield, 63
subgroup, 20
  abelian group, 38
  closed, 419
  generated, 20
  normal, 23
  of $K^\times$, 57, 111
  of cyclic group, 28
  of index 2, 23
  proper, 20

submodule, 144
  generated, 144
subquiver, 357
  full, 357
subring, 46
substitution, 54
Sudoku, 248
sum of digits, 102
sum rule, 74
supplementary laws, 460
Suzuki, 476
Sylow, 32
  for profinite groups, 502
Sylow p-subgroup, 32
Sylow subgroup
  of profinite groups, 502
Sylvester, 465
Sylvester matrix, 266
symmetric algebra, 347
symmetric difference, 106
symmetric group, 20
symmetric square, 312, 515
symmetrizer, 312
Syndrome, 439
Syndrome decoding, 439
system of representatives, 116

T
tableau, 298
Tartaglia, 8, 90
Taussky, 245
Taylor series, 110
tensor product, 340
  for arbitrary rings, 330
  for commutative rings, 244
  for group algebras, 282
  universal property, 244, 283, 330
Tensorprodukt
  universelle Eigenschaft, 340
topology
  compact, 497
  connected, 497
  totally disconnected, 497
torsion module, 172
trace map, 71, *126*
transcendence basis, 128
transcendence degree, 131
transcendental, 63
transitive, 29
Translation Theorem, 71
transposition, 21
triangle inequality, 396
triangular matrix, 20, 106
Tschirnhaus transformation, 94
Tsen, 344
Turyn, 441

U
UFD, 137
ultrafilter, 496
unit, 45
unit group, 45
Universal property
  universal enveloping algebra, 390
universal property
  path algebra, 359

V
valuation, 396
  additive, 397
  archimedean, 396
  complete, 396
  discrete, 398
  equivalent, 399
  euclidean, 396
  P-adic, 396
  p-adic, 396
  trivial, 396
  ultrametric, 396
valuation ideal, 398
valuation ring, 196, 398
van Lint, Tietäväinen, 442
variety, 261
  (ir)reducible, 262
  component, 263
  dimension, 263
vertex, 357
vertices
  adjacent, 359
  connected, 359
Vieta, 92
Voyager probe, 443

W
Wamsley, 509
Wedderburn, 157
Wedderburn-Malcev, 210, 493
Weierstraß normal form, 177
Weight, 435
weight, 371
well-ordering theorem, 115
Weston, 115
Weyl, 385
Wilson, 102
Witt algebra, 454
Witt's formula, 391

Y
Yoneda embedding, 320
Yoneda's Lemma, 320
Young diagram, 298
  conjugate, 298
Young subgroup, 298
Young tableau, 298

Z

Zariski closure, 261
Zariski topology, 237, 261
Zariski's Lemma, 260
zero divisor, 45
Zorn's Lemma, 115
Zsigmondy, 477
Zsigmondy prime, 476