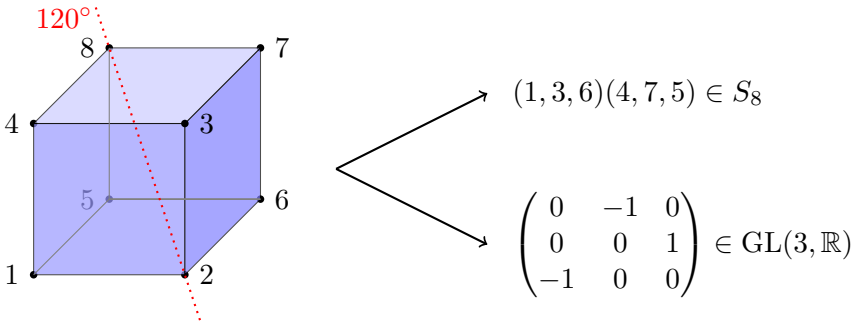
Representation theory

Lectures from summer semester 2023

Benjamin Sambale
Leibniz Universität Hannover

Version: April 4, 2026



Contents

Preface 3

1 Representations 3

2 Characters 7

3 Character Tables 12

4 Algebraic integers 17

5 Induced characters 19

6 Applications 21

7 Representations over number fields 24

8 Algebras 30

9 Modules 34

10 Semisimple modules 38

11 Indecomposable Modules 41

12 Group Algebras 45

13 Integral Representations 52

Exercises 57

Index 64

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

In *representation theory*, one realizes abstract mathematical objects such as maps, vector spaces, groups, rings, graphs etc. through concrete objects such as coordinate vectors, matrices or permutations. In linear algebra, this is easy: every n-dimensional vector space over a field K is isomorphic to K^n and every linear map corresponds to a matrix. From algebra, one knows Cayley's theorem: every (finite) group is isomorphic to a subgroup of a symmetric group (every group element thus corresponds to a permutation). In this lecture, we are interested in representations of finite groups by matrices over a field K. At the beginning, we often assume $K = \mathbb{C}$ for the sake of simplicity. One can then already answer many questions through the trace of the corresponding matrices. In Chapter 7, we replace $\mathbb{C}$ with a number field (i. e. a finite field extension of $\mathbb{Q}$). Finally, we consider fields with positive characteristic.

This script originated from a one-hour lecture in the summer semester 2023 at Leibniz Universität Hannover. This lecture is primarily aimed at Bachelor's and Master's students of mathematics. Knowledge of Algebra 1 is assumed. The first part roughly follows my notes on character theory. Subsequently, I have simplified the proof of Frobenius's theorem (existence of Frobenius kernels), so that induced characters are no longer needed for it. As a new application of induced characters, I have included Taunt's theorem instead. I thank Karl Böhlke, Lyon Wolfgang Dorgelo, Leon Eickhoff, Leon Lampe, Claude Sonnet (4.6), Frederik Tscherniak, Tim Wittenberg and Yasin Yilmaz for error corrections.

Literature:

- Sambale, Algebra notes, Character theory notes
- Isaacs, *Character theory of finite groups*, AMS Chelsea Publishing, Providence, RI, 2006
- Huppert, *Character theory of finite groups*, Expositions in Mathematics, Vol. 25, Walter de Gruyter GmbH & Co., Berlin, 1998
- Grove, *Groups and characters*, Pure and Applied Mathematics, John Wiley & Sons Inc., New York, 1997
- James und Liebeck, *Representations and characters of groups*, 2nd Edition, Cambridge University Press, Cambridge, 2001
- Lux und Pahlings, *Representations of groups*, Cambridge University Press, Cambridge, 2010
- Webb, *A Course in Finite Group Representation Theory*, Cambridge University Press, Cambridge, 2016

1 Representations

Remark 1.1.

(i) We use the usual number sets $\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

(ii) Let K always be a field and G a finite group.

Definition 1.2. Let $V \neq 0$ be a finite-dimensional K-vector space. A (K-)*representation* of G on V is a homomorphism $\Delta\colon G \to \mathrm{GL}(V)$. One calls $\dim V$ the *degree* of Δ. If Δ is injective, then Δ is called *faithful*. By choosing a basis of V, one obtains a corresponding *matrix representation* $\Delta'\colon G \to \mathrm{GL}(n, K)$.

Remark 1.3. If a representation $\Delta\colon G \to \mathrm{GL}(V)$ is given, we often write ${}^g v := \Delta(g)(v)$ for $g \in G$ and $v \in V$. This defines an action of G on V, i. e. ${}^1 v = v$ and ${}^{gh} v = {}^g({}^h v)$ hold for all $g, h \in G$ and $v \in V$. Additionally, the linearity ${}^g(v+w) = {}^g v + {}^g w$ holds. Conversely, every action of G on V corresponds to a homomorphism $G \to \mathrm{Sym}(V)$. If, in addition, linearity holds, then it is a homomorphism $G \to \mathrm{GL}(V)$, thus a representation. In this way, representations and linear actions correspond to each other.

Example 1.4.

(i) The *trivial* (matrix) representation $\mathbb{1}_G\colon G \to \mathrm{GL}(1, K) = K^\times = K \setminus \{0\}$ is given by $\mathbb{1}_G(g) = 1$ for $g \in G$.

(ii) For $n \in \mathbb{N}$ let S_n be the symmetric group of degree n. The map $\mathrm{sgn}\colon S_n \to \mathbb{Q}^\times$, $g \mapsto \mathrm{sgn}(g)$ is a $\mathbb{Q}$-representation of degree 1. The kernel of sgn is the alternating group A_n.

(iii) Let
$$D_{2n} = \langle \sigma, \tau : \sigma^n = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$$
be the *dihedral group* of order $2n$, i.e., the symmetry group of the regular n-gon. Then
$$\Delta(\sigma) := \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}, \qquad \Delta(\tau) := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
defines an $\mathbb{R}$-matrix representation of degree 2 ($\Delta(\sigma)$ is the rotation by $2\pi/n$ and $\Delta(\tau)$ the reflection across the x-axis).

(iv) For two K-representations $\Delta\colon G \to \mathrm{GL}(V)$ and $\Gamma\colon G \to \mathrm{GL}(W)$, $\Delta \oplus \Gamma\colon G \to \mathrm{GL}(V \times W)$ is also a K-representation with ${}^g(v, w) := ({}^g v, {}^g w)$ for $g \in G$, $v \in V$ and $w \in W$. With respect to a suitable basis, the corresponding matrix representation has block diagonal form:
$$(\Delta \oplus \Gamma)'(g) = \begin{pmatrix} \Delta'(g) & 0 \\ 0 & \Gamma'(g) \end{pmatrix}.$$

(v) If $\Delta\colon H \to \mathrm{GL}(V)$ is a representation and $f\colon G \to H$ is a group homomorphism, then $\Delta \circ f\colon G \to \mathrm{GL}(V)$ is also a representation. If $G \leq H$ and f is the inclusion map, one obtains the *restriction* $\Delta_G\colon G \to \mathrm{GL}(V)$, $g \mapsto \Delta(g)$. If $H = G/N$ with $N \trianglelefteq G$ and $f\colon G \to H$, $g \mapsto gN$ is the canonical epimorphism, then $\Delta \circ f$ is called the *inflation* of Δ.

(vi) If $\Delta\colon G \to \mathrm{GL}(V)$ is a representation and $N \trianglelefteq G$ with $N \subseteq \mathrm{Ker}(\Delta)$, one obtains by *deflation* a well-defined representation $\widehat{\Delta}\colon G/N \to \mathrm{GL}(V)$, $gN \mapsto \Delta(g)$. In particular, $\widehat{\Delta}\colon G/\mathrm{Ker}(\Delta) \to \mathrm{GL}(V)$ is a faithful representation.

(vii) Inflation and deflation are obviously inverse to each other.

Definition 1.5. Two representations $\Delta\colon G \to \mathrm{GL}(V)$ and $\Gamma\colon G \to \mathrm{GL}(W)$ are called *similar*, if an isomorphism $f\colon V \to W$ with $f \circ \Delta(g) = \Gamma(g) \circ f$ for all $g \in G$ exists. In this case, the following diagram is commutative:

$$\begin{array}{ccc} V & \xrightarrow{\Delta(g)} & V \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ W & \xrightarrow{\Gamma(g)} & W \end{array}$$

Accordingly, two matrix representations $\Delta\colon G \to \mathrm{GL}(n, K)$ and $\Gamma\colon G \to \mathrm{GL}(m, K)$ are similar if $n = m$ and there exists an $A \in \mathrm{GL}(n, K)$ with $A\Delta(g) = \Gamma(g)A$ for all $g \in G$.

Remark 1.6.

(i) Similarity is an equivalence relation. Similar representations have the same degree. One is usually only interested in representations up to similarity (just as for groups up to isomorphism).

(ii) In linear algebra, it is shown that two square matrices A, B describe the same map if and only if there exists an invertible matrix T with $AT = TB$. Thus, two matrix representations corresponding to the same representation of G are always similar.

(iii) The similarity classes of representations and matrix representations obviously correspond to each other. We will therefore often identify representations with their corresponding matrix representations in the following.

Definition 1.7. Let $\Delta\colon G \to \mathrm{GL}(V)$ be a representation. A subspace $U \leq V$ is called Δ-*invariant*, if ${}^gU := \{{}^gu : u \in U\} = U$ for all $g \in G$ holds. In this case, $\Delta'\colon G \to \mathrm{GL}(U)$, $g \mapsto \Delta(g)_{|U}$ is also a representation. If 0 and V are the only Δ-invariant subspaces, then Δ is *irreducible*. Otherwise, Δ is *reducible*.

Example 1.8.

(i) Representations of degree 1 are obviously irreducible.

(ii) Inflation and deflation of irreducible representations are again irreducible (the images do not change).

Theorem 1.9 (Maschke)**.** *Let* $\operatorname{char} K \nmid |G|$ (*e. g.* $\operatorname{char} K = 0$). *Let* $\Delta\colon G \to \mathrm{GL}(V)$ *be a representation and* $U \leq V$ *be* Δ*-invariant. Then* U *has a* Δ*-invariant complement* $W \leq V$*, i. e.* $V = U \oplus W$*.*

Proof. We first choose an arbitrary subspace X of V with $V = U \oplus X$ (basis extension theorem) and denote by $\pi\colon V \to V$, $u + x \mapsto u$ the projection onto U. Since $\operatorname{char} K \nmid |G|$,

$$\rho := \frac{1}{|G|} \sum_{g \in G} \Delta(g)^{-1} \circ \pi \circ \Delta(g) \in \mathrm{End}(V)$$

is well-defined and $W := \operatorname{Ker}(\rho) \leq V$. For $u \in U$ we have

$$\rho(u) = \frac{1}{|G|} \sum_{g \in G} \Delta(g)^{-1}(\pi(\underbrace{\Delta(g)(u)}_{\in U})) = \frac{1}{|G|} \sum_{g \in G} \underbrace{(\Delta(g)^{-1}\Delta(g))}_{=\mathrm{id}_V}(u) = u.$$

In particular, $U \cap W = 0$. For $v \in V$ we have $\rho(v) \in U$, thus

$$\rho(v - \rho(v)) = \rho(v) - \rho(\rho(v)) = \rho(v) - \rho(v) = 0,$$

i. e. $v - \rho(v) \in W$ and $v = \rho(v) + (v - \rho(v)) \in U + W$. Consequently, $V = U \oplus W$. For $w \in W$ and $g \in G$ it holds that

$$\rho({}^g w) = \left(\frac{1}{|G|} \sum_{h \in G} \Delta(h^{-1}) \circ \pi \circ \Delta(hg)\right)(w) = \left(\Delta(g) \circ \underbrace{\left(\frac{1}{|G|} \sum_{h \in G} \Delta(g^{-1}h^{-1}) \circ \pi \circ \Delta(hg)\right)}_{=\rho}\right)(w)$$

$$= {}^g\rho(w) = {}^g 0 = 0,$$

so ${}^g w \in \operatorname{Ker}(\rho) = W$. Thus W is Δ-invariant. □

Remark 1.10.

(i) Let Δ be a representation on V, and let $V = U \oplus W$ be a Δ-invariant decomposition. This yields subrepresentations $\Gamma_U \colon G \to \mathrm{GL}(U)$, $g \mapsto \Delta(g)_{|U}$ and $\Gamma_W \colon G \to \mathrm{GL}(W)$, $g \mapsto \Delta(g)_{|W}$. By choosing a suitable basis of V, Δ then has the form

$$\Delta(g) = \begin{pmatrix} \Gamma_U(g) & 0 \\ 0 & \Gamma_W(g) \end{pmatrix}$$

for all $g \in G$. Thus $\Delta = \Gamma_U \oplus \Gamma_W$. In the case $\operatorname{char} K \nmid |G|$, every representation can thus be written as a direct sum of irreducible representations.

(ii) If $\operatorname{char} K$ is a divisor of $|G|$, then there are representations for which Maschke's Theorem is false (Exercise 1).

Lemma 1.11 (Schur's Lemma)**.** *Let $\Delta \colon G \to \mathrm{GL}(n, K)$, $\Gamma \colon G \to \mathrm{GL}(m, K)$ be irreducible matrix representations and $0 \neq A \in K^{n \times m}$ with $A\Gamma(g) = \Delta(g)A$ for all $g \in G$. Then:*

(i) $n = m$ and A is invertible. In particular, Δ and Γ are similar.

(ii) If $\Delta = \Gamma$ and K is algebraically closed, then $A = \lambda 1_n$ for some $\lambda \in K^\times$.

Proof.

(i) For $g \in G$ and $v \in \operatorname{Ker}(A)$ we have

$$A\Gamma(g)v = \Delta(g)Av = 0,$$

thus $\Gamma(g)v \in \operatorname{Ker}(A)$. Therefore $\operatorname{Ker}(A)$ is a Γ-invariant subspace of K^m. Analogously, $\operatorname{Bild}(A)$ is a Δ-invariant subspace of K^n. From the irreducibility of Δ and Γ it follows that $\operatorname{Ker}(A) = 0$ and $\operatorname{Bild}(A) = K^n$. Therefore A is invertible and $n = m$.

(ii) Since K is algebraically closed, A has an eigenvalue λ. Then $(A - \lambda 1_n)\Gamma(g) = A\Gamma(g) - \lambda\Gamma(g) = \Delta(g)(A - \lambda 1_n)$ for all $g \in G$. Since $A - \lambda 1_n$ is not invertible, $A - \lambda 1_n = 0$ follows from (i). □

2 Characters

Remark 2.1. In the next chapters, let always $K = \mathbb{C}$. Because $\operatorname{char} K = 0 \nmid |G|$, Maschke's Theorem can be applied. According to the Fundamental Theorem of Algebra, $\mathbb{C}$ is algebraically closed. Thus one can also use the second part of Schur's Lemma.

Theorem 2.2. *Every irreducible representation of an abelian group has degree* 1.

Proof. Let G be abelian and $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ an irreducible matrix representation of G. Let $g \in G$ be fixed. For all $h \in G$ it then holds that $\Delta(g)\Delta(h) = \Delta(gh) = \Delta(hg) = \Delta(h)\Delta(g)$. According to Schur's Lemma, we thus have $\Delta(g) = \lambda_g 1_n$ for some $\lambda_g \in \mathbb{C}$. In particular, $\mathbb{C}(1, 0, \dots, 0)$ is a Δ-invariant subspace of $\mathbb{C}^n$. Since Δ is irreducible, it follows that $n = 1$. □

Definition 2.3. Let $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ be a matrix representation. The map

$$\chi\colon G \to \mathbb{C}, \qquad g \mapsto \operatorname{tr} \Delta(g)$$

is called the *character* of Δ (and of G). Here $\chi(1) = \operatorname{tr} \Delta(1) = \operatorname{tr} 1_n = n$ is the *degree* of χ (and of Δ). If Δ is irreducible (faithful, ...), then χ is also called *irreducible* (*faithful*, ...). We denote the set of irreducible characters of G by $\mathrm{Irr}(G)$. Note: Faithful characters are in general not injective (see Remark 2.15).

Remark 2.4. For $A = (a_{ij}) \in K^{n \times m}$ and $B = (b_{ij}) \in K^{m \times n}$ we have

$$\operatorname{tr}(AB) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} b_{ji} = \sum_{j=1}^{m} \sum_{i=1}^{n} b_{ji} a_{ij} = \operatorname{tr}(BA). \tag{2.1}$$

Lemma 2.5. *Similar matrix representations have the same character.*

Proof. Let $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ and $\Gamma\colon G \to \mathrm{GL}(n, \mathbb{C})$ be similar matrix representations. Then there exists an $A \in \mathrm{GL}(n, \mathbb{C})$ with $\Delta(g)A = A\Gamma(g)$ for all $g \in G$. From (2.1) it follows that

$$\operatorname{tr} \Delta(g) = \operatorname{tr}((A\Gamma(g))A^{-1}) = \operatorname{tr}(A^{-1}(A\Gamma(g))) = \operatorname{tr} \Gamma(g)$$

for all $g \in G$. □

Remark 2.6.

(i) Characters were originally introduced by Dirichlet for prime residue class groups $(\mathbb{Z}/n\mathbb{Z})^\times$ in order to prove his prime number theorem.[1]

(ii) Characters are the "shadows" of representations, i. e. on the one hand, information is lost by replacing the n^2 entries of a matrix with a single value, but on the other hand, enough information remains to read off properties of the group.

(iii) If $\Delta\colon G \to \mathrm{GL}(V)$ is a representation, one can assign a character to Δ by choosing a corresponding matrix representation. Due to Lemma 2.5, this does not depend on the choice of the basis of V.

[1] See Proof of Dirichlet's Prime Number Theorem

(iv) Obviously, representations of degree 1 coincide with their character. These characters are called *linear*. In particular, there is the *trivial* character $\mathbb{1}_G\colon G \to \mathbb{C}$ with $\mathbb{1}_G(g) = 1$ for $g \in G$.

(v) For every representation $\Delta\colon G \to \mathrm{GL}(V)$, $\det\Delta\colon G \to \mathbb{C}$, $g \mapsto \det\Delta(g)$ is a linear character. Since similar matrices have the same determinant, $\det\Delta$ depends only on the character χ of Δ. One can therefore define $\det\chi := \det\Delta$.

(vi) If Δ and Γ are representations with character χ and ψ respectively, then $\Delta \oplus \Gamma$ has the character $\chi + \psi$. Sums of characters are thus again characters.

Definition 2.7.

(i) One calls $g, h \in G$ *conjugate*, if an $x \in G$ with $xgx^{-1} = h$ exists. The elements conjugate to g form the *conjugacy class*

$$\mathrm{Cl}(g) := \{xgx^{-1} : x \in G\}$$

of g. Let the set of conjugacy classes of G be $\mathrm{Cl}(G)$. One calls $k(G) := |\mathrm{Cl}(G)|$ the *class number* of G. Let

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

be the *centralizer* of g in G. In algebra one shows $|\mathrm{Cl}(g)| = |G : \mathrm{C}_G(g)|$.

(ii) As is well known, the set of all mappings $G \to \mathbb{C}$ becomes a $\mathbb{C}$-vector space of dimension $|G|$ via

$$(\alpha + \beta)(g) := \alpha(g) + \beta(g), \qquad (\lambda \cdot \alpha)(g) := \lambda\alpha(g)$$

for $\alpha, \beta\colon G \to \mathbb{C}$, $g \in G$, $\lambda \in \mathbb{C}$. A mapping $\alpha\colon G \to \mathbb{C}$ is called a *class function*, if $\alpha(g) = \alpha(hgh^{-1})$ holds for all $g, h \in G$. Class functions are thus constant on conjugacy classes. The subspace $\mathrm{CF}(G)$ of all class functions obviously has dimension $|\mathrm{Cl}(G)|$.

Lemma 2.8. *The characters of G are class functions. In particular,* $\mathrm{Irr}(G) \subseteq \mathrm{CF}(G)$.

Proof. Let $\Delta\colon G \to \mathrm{GL}(V)$ be a representation with character χ. For $g, h \in G$ we have

$$\chi(hgh^{-1}) = \mathrm{tr}\,\Delta(hgh^{-1}) = \mathrm{tr}(\Delta(h)\Delta(g)\Delta(h)^{-1}) \overset{(2.1)}{=} \mathrm{tr}\,\Delta(g) = \chi(g). \qquad \square$$

Definition 2.9. Obviously,

$$(\chi, \psi)_G := \frac{1}{|G|}\sum_{g \in G} \chi(g)\overline{\psi(g)} \qquad (\chi, \psi \in \mathrm{CF}(G))$$

defines a scalar product of the $\mathbb{C}$-vector space $\mathrm{CF}(G)$.

Remark 2.10.

(i) If $g_1, \ldots, g_k \in G$ are representatives for the conjugacy classes of G, then

$$(\chi, \psi)_G = \frac{1}{|G|}\sum_{i=1}^{k} |G : \mathrm{C}_G(g_i)|\chi(g_i)\overline{\psi(g_i)} = \sum_{i=1}^{k} \frac{\chi(g_i)\overline{\psi(g_i)}}{|\mathrm{C}_G(g_i)|}. \tag{2.2}$$

Up to the factors $|\mathrm{C}_G(g_i)|^{-1}$, $(\chi, \psi)_G$ thus corresponds to the standard scalar product of $\mathbb{C}^k$.

(ii) For characters χ, ψ of G, according to Exercise 5, we also have

$$(\chi, \psi)_G = \frac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g^{-1}).$$

Lemma 2.11 (Schur Relations). *Let $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$, $\Gamma\colon G \to \mathrm{GL}(m, \mathbb{C})$ be irreducible matrix representations with $\Delta(g) = (\lambda_{ij}(g))$ and $\Gamma(g) = (\theta_{ij}(g))$ for $g \in G$.*

(i) If Δ and Γ are not similar, then

$$\sum_{g \in G} \lambda_{ii}(g)\theta_{jj}(g^{-1}) = 0$$

for all i, j.

(ii) It holds that

$$\sum_{g \in G} \lambda_{ii}(g)\lambda_{jj}(g^{-1}) = \frac{|G|}{n}\delta_{ij}.$$

Proof.

(i) Let $E_{ij} \in \mathbb{C}^{n \times m}$ be the matrix with a 1 at position (i, j) and zeros elsewhere. We set

$$F_{ij} := \sum_{g \in G} \Delta(g)E_{ij}\Gamma(g^{-1}).$$

For $h \in G$ we then have $\Delta(h)F_{ij}\Gamma(h^{-1}) = F_{ij}$, i. e. $\Delta(h)F_{ij} = F_{ij}\Gamma(h)$. If Δ and Γ are not similar, then $F_{ij} = 0$ follows from Schur's Lemma. In particular, F_{ij} is equal to 0 at position (i, j), i. e. (i) holds.

(ii) Now let $\Delta = \Gamma$. According to Schur, $F_{ij} = \rho_{ij} \cdot 1_n$ for some $\rho_{ij} \in \mathbb{C}$. For the entry of F_{ij} at position $(1, 1)$ it then holds that

$$\rho_{ij} = \sum_{g \in G} \lambda_{1i}(g)\lambda_{j1}(g^{-1}) = \sum_{h \in G} \lambda_{1i}(h^{-1})\lambda_{j1}(h) = \sum_{h \in G} \lambda_{j1}(h)\lambda_{1i}(h^{-1}) = \rho_{11}\delta_{ij}.$$

With $\rho := \rho_{11}\,(= \rho_{ii})$ it follows that

$$n\rho = \sum_{j=1}^{n} \sum_{g \in G} \lambda_{ij}(g)\lambda_{ji}(g^{-1}) = \sum_{g \in G} 1 = |G|$$

due to $\Delta(g)\Delta(g^{-1}) = 1_n$ for $g \in G$. Now (ii) results from the entry of F_{ij} at position (i, j). □

Theorem 2.12 (First Orthogonality Relation). *For $\chi, \psi \in \mathrm{Irr}(G)$ it holds that*

$$\boxed{(\chi, \psi)_G = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)} = \begin{cases} 1 & \text{if } \chi = \psi, \\ 0 & \text{if } \chi \neq \psi. \end{cases}}$$

Proof. Let Δ and Γ be irreducible representations of G with character χ and ψ respectively. First let $\chi \neq \psi$. According to Lemma 2.5, Δ and Γ are then not similar. We write $\Delta(g) = (\lambda_{ij}(g))$ and $\Gamma(g) = (\theta_{ij}(g))$ for $g \in G$. Then $\chi(g) = \sum \lambda_{ii}(g)$ and $\psi(g) = \sum \theta_{ii}(g)$. According to Lemma 2.11 it holds that

$$(\chi, \psi)_G = \frac{1}{|G|} \sum_{g \in G} \sum_{i,j} \lambda_{ii}(g)\theta_{jj}(g^{-1}) = 0.$$

Analogously,

$$(\chi, \chi)_G = \frac{1}{|G|} \sum_{g \in G} \sum_{i,j} \lambda_{ii}(g)\lambda_{jj}(g^{-1}) = \frac{\chi(1)}{|G|} \frac{|G|}{\chi(1)} = 1. \qquad \square$$

Remark 2.13. From Theorem 2.12 it follows easily that $\mathrm{Irr}(G)$ is a linearly independent subset of $\mathrm{CF}(G)$. In particular, $|\mathrm{Irr}(G)| \leq \dim_{\mathbb{C}} \mathrm{CF}(G) = |\mathrm{Cl}(G)| \leq |G| < \infty$.

Theorem 2.14. *Two representations are similar if and only if they have the same character.*

Proof. One direction is Lemma 2.5. Now let Δ and Γ be representations with the same character χ. We write $\Delta = \bigoplus_{i=1}^{n} \Delta_i$ and $\Gamma = \bigoplus_{i=1}^{m} \Gamma_i$ as sums of irreducible representations. Then χ also decomposes into

$$\chi = \sum_{i=1}^{n} \chi_{\Delta_i} = \sum_{i=1}^{m} \chi_{\Gamma_i}.$$

According to Remark 2.13, $n = m$ and $\chi_{\Delta_i} = \chi_{\Gamma_i}$ for $i = 1, \ldots, n$ given a suitable numbering. If Δ_i and Γ_i were not similar, one would obtain the contradiction $1 = (\chi_{\Delta_i}, \chi_{\Gamma_i})_G = 0$ as in the proof of Theorem 2.12. So let $A_i \in \mathrm{GL}(\chi_{\Delta_i}(1), \mathbb{C})$ with $A_i \Delta_i(g) = \Gamma_i(g) A_i$ for all $g \in G$. For

$$A := \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_n \end{pmatrix} \in \mathrm{GL}(\chi(1), \mathbb{C})$$

it then obviously holds that $A\Delta(g) = \Gamma(g)A$ for all $g \in G$, i. e. Δ and Γ are similar. $\square$

Remark 2.15.

(i) Let ρ be the regular character of G. According to Exercise 1, it holds that

$$\rho(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{otherwise.} \end{cases}$$

For $\chi \in \mathrm{Irr}(G)$ we therefore have

$$(\rho, \chi)_G = \frac{1}{|G|} \sum_{g \in G} \rho(g)\overline{\chi(g)} = \chi(1).$$

It follows that $\rho = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi$ and $\boxed{|G| = \rho(1) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2.}$

(ii) Let $C, D, E \in \mathrm{Cl}(G)$, $e \in E$ and $g \in G$. Then the map $(c,d) \mapsto (gcg^{-1}, gdg^{-1})$ is a bijection between $\{(c,d) \in C \times D : cd = e\}$ and $\{(c,d) \in C \times D : cd = geg^{-1}\}$. Therefore, the *class multiplication constant*

$$\gamma_{CDE} := \big|\{(c,d) \in C \times D : cd = e\}\big|$$

does not depend on the choice of $e \in E$.

Lemma 2.16. *For an irreducible representation Δ with character χ and $g \in C \in \mathrm{Cl}(G)$, it holds that*

$$\sum_{x \in C} \Delta(x) = \omega_\Delta(C)\,\mathrm{id}$$

with $\omega_\Delta(C) := \omega_\chi(C) := \frac{|C|}{\chi(1)}\chi(g)$.

Proof. Let $A := \sum_{x \in C} \Delta(x)$. For $y \in G$, it holds that $\Delta(y)A\Delta(y^{-1}) = \sum_{x \in C} \Delta(yxy^{-1}) = A$. From Schur's Lemma, it follows that $A = \omega_\Delta(C)\,\mathrm{id}$ for some $\omega_\Delta(C) \in \mathbb{C}$. Furthermore,

$$\omega_\Delta(C)\chi(1) = \operatorname{tr} A = \sum_{x \in C} \chi(x) = |C|\chi(g). \qquad \square$$

Theorem 2.17 (Second orthogonality relation)**.** *For $g, h \in G$, it holds that*

$$\boxed{\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = \begin{cases} |\mathrm{C}_G(g)| & \text{if } g \text{ and } h \text{ are conjugate,} \\ 0 & \text{otherwise.} \end{cases}}$$

Proof. Let $C, D \in \mathrm{Cl}(G)$ with $g \in C$ and $h^{-1} \in D$. Let $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ be an irreducible matrix representation with character χ. According to Lemma 2.16, it holds that

$$\begin{aligned} \omega_\chi(C)\omega_\chi(D)1_n &= \sum_{c \in C} \Delta(c) \sum_{d \in D} \Delta(d) = \sum_{c \in C} \sum_{d \in D} \Delta(cd) \overset{2.15}{=} \sum_{E \in \mathrm{Cl}(G)} \gamma_{CDE} \sum_{e \in E} \Delta(e) \\ &= \sum_{E \in \mathrm{Cl}(G)} \gamma_{CDE}\omega_\chi(E)1_n. \end{aligned}$$

From the definition of ω_χ one obtains

$$\chi(g)\overline{\chi(h)} = \sum_{E \in \mathrm{Cl}(G)} \frac{\gamma_{CDE}|E|}{|C||D|}\chi(1)\chi(e),$$

where $e \in E$ is chosen in each case. Let ρ be the regular character of G. Summing over χ yields

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = \sum_{E \in \mathrm{Cl}(G)} \frac{\gamma_{CDE}|E|}{|C||D|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(e) \overset{2.15}{=} \sum_{E \in \mathrm{Cl}(G)} \frac{\gamma_{CDE}|E|}{|C||D|}\rho(e) = \frac{\gamma_{CD\{1\}}|G|}{|C||D|}.$$

Obviously $\mathrm{Cl}(h) = D^{-1} = \{d^{-1} : d \in D\}$. If g and h are not conjugate, then $C \cap D^{-1} = \varnothing$ and $\gamma_{CD\{1\}} = 0$. Otherwise $\gamma_{CD\{1\}} = |C| = |D|$ and the assertion follows from $\frac{|G|}{|C|} = |\mathrm{C}_G(g)|$. $\square$

Theorem 2.18. $\mathrm{Irr}(G)$ *is an orthonormal basis of* $\mathrm{CF}(G)$*. In particular,* $\boxed{k(G) = |\mathrm{Irr}(G)|.}$

Proof. We already know that $\mathrm{Irr}(G)$ is linearly independent (Remark 2.13). According to the second orthogonality relation, for $g \in C \in \mathrm{Cl}(G)$ on the other hand

$$\varphi_C := \frac{1}{|\mathrm{C}_G(g)|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(g^{-1})\chi$$

is the characteristic function on C (i. e. $\varphi_C(x)$ is 1 if $x \in C$ and 0 otherwise). Since the characteristic functions form a basis of $\mathrm{CF}(G)$, $\mathrm{Irr}(G)$ is also a generating set. The orthonormality follows from the first orthogonality relation. □

Remark 2.19.

(i) Every class function $f \in \mathrm{CF}(G)$ can thus be uniquely written in the form

$$f = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi$$

with $a_\chi \in \mathbb{C}$. f is a character if and only if $a_\chi \in \mathbb{N}_0$ for all $\chi \in \mathrm{Irr}(G)$ and $a_\psi > 0$ for at least one $\psi \in \mathrm{Irr}(G)$ holds (Remark 2.6(vi)). If $a_\chi = (f, \chi)_G > 0$, then χ is called an *irreducible constituent* of f with *multiplicity* a_χ. Furthermore, $(f, f)_G = \sum_\chi a_\chi^2$ holds. In particular, a character χ is irreducible if and only if $(\chi, \chi)_G = 1$ holds.

(ii) In general, no canonical bijection between $\mathrm{Cl}(G)$ and $\mathrm{Irr}(G)$ is known.

3 Character Tables

Remark 3.1. Let $g_1, \ldots, g_k \in G$ be representatives for the conjugacy classes of G, and let $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$. The $k \times k$-matrix $C(G) := (\chi_i(g_j))_{i,j}$ is called the *character table* of G. Of course, C depends on the order of the elements and characters. Usually, one chooses $g_1 = 1$, $\chi_1 = \mathbb{1}_G$ and $\chi_1(1) \leq \chi_2(1) \leq \ldots \leq \chi_k(1)$. In this chapter, we want to calculate C for some groups. The first orthogonality relation can be written in the form

$$\sum_{i=1}^{k} \frac{1}{|\mathrm{C}_G(g_i)|} \chi_r(g_i)\overline{\chi_s(g_i)} = \delta_{rs}$$

(see (2.2)). This thus concerns the rows of C. The second orthogonality relation states that the columns of C are pairwise orthogonal with respect to the standard inner product of $\mathbb{C}^k$. In particular, C is invertible.

Definition 3.2. For matrices $A = (a_{ij}) \in K^{n\times n}$ and $B \in K^{m\times m}$, one calls

$$A \otimes B := \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{pmatrix} \in K^{nm\times nm}$$

the *Kronecker product* of A and B.

Lemma 3.3. *For $A, C \in K^{n\times n}$ and $B, D \in K^{m\times m}$, we have* $\boxed{(A \otimes B)(C \otimes D) = AC \otimes BD.}$

Proof.
$$(A \otimes B)(C \otimes D) = \Big(\sum_k a_{ik}Bc_{kj}D\Big)_{i,j} = \Big(\big(\sum_k a_{ik}c_{kj}\big)BD\Big)_{i,j} = AC \otimes BD. \qquad \square$$

Theorem 3.4. *Let $\Delta\colon G \to \mathrm{GL}(n,\mathbb{C})$ and $\Gamma\colon H \to \mathrm{GL}(m,\mathbb{C})$ be representations of groups G and H with characters χ and ψ, respectively. Then $\Delta \otimes \Gamma\colon G \times H \to \mathrm{GL}(nm,\mathbb{C})$, $(g,h) \mapsto \Delta(g) \otimes \Gamma(h)$ is a representation of $G \times H$ with character $(\chi \times \psi)(g,h) := \chi(g)\psi(h)$ for $g \in G$, $h \in H$.*

Proof. For $g_1, g_2 \in G$ and $h_1, h_2 \in H$, we have

$$\begin{aligned}(\Delta \otimes \Gamma)(g_1,h_1)(\Delta \otimes \Gamma)(g_2,h_2) &= (\Delta(g_1) \otimes \Gamma(h_1))(\Delta(g_2) \otimes \Gamma(h_2)) \overset{3.3}{=} \Delta(g_1)\Delta(g_2) \otimes \Gamma(h_1)\Gamma(h_2)\\ &= \Delta(g_1g_2) \otimes \Gamma(h_1h_2) = (\Delta \otimes \Gamma)(g_1g_2, h_1h_2).\end{aligned}$$

Therefore, $\Delta \otimes \Gamma$ is a representation of $G \times H$. Let $\Delta(g) = (a_{ij})$. Then we have

$$\begin{aligned}(\chi \times \psi)(g,h) &= \operatorname{tr}(\Delta(g) \otimes \Gamma(h)) = \sum_{i=1}^{n} \operatorname{tr}(a_{ii}\Gamma(h)) = \sum_{i=1}^{n} a_{ii} \operatorname{tr}(\Gamma(h))\\ &= \operatorname{tr}(\Delta(g)) \operatorname{tr}(\Gamma(h)) = \chi(g)\psi(h). \qquad \square\end{aligned}$$

Theorem 3.5. *For finite groups G, H, we have $\mathrm{Irr}(G \times H) = \{\chi \times \psi : \chi \in \mathrm{Irr}(G), \psi \in \mathrm{Irr}(H)\}$.*

Proof. Let $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_n\}$ and $\mathrm{Irr}(H) = \{\psi_1, \dots, \psi_m\}$. Then

$$\begin{aligned}(\chi_i \times \psi_j, \chi_k \times \psi_l)_{G\times H} &= \frac{1}{|G \times H|} \sum_{g\in G} \sum_{h \in H} \chi_i(g)\psi_j(h)\overline{\chi_k(g)\psi_l(h)}\\ &= \Big(\frac{1}{|G|}\sum_{g\in G} \chi_i(g)\overline{\chi_k(g)}\Big)\Big(\frac{1}{|H|}\sum_{h\in H} \psi_j(h)\overline{\psi_l(h)}\Big) = \delta_{ik}\delta_{jl}.\end{aligned}$$

Thus the characters $\chi_i \times \psi_j$ are irreducible and pairwise distinct. Because of

$$\sum_{i=1}^{n}\sum_{j=1}^{m} (\chi_i \times \psi_j)(1)^2 = \sum_{i=1}^{n} \chi_i(1)^2 \sum_{j=1}^{m} \psi_j(1)^2 = |G||H| = |G \times H|$$

one has found all irreducible characters of $G \times H$. $\square$

Corollary 3.6. *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 Δ and Γ be representations of G with character χ and ψ respectively. Then $G \to G \times G \to \mathrm{GL}(\chi(1)\psi(1),\mathbb{C})$, $g \mapsto (g,g) \mapsto (\Delta \otimes \Gamma)(g,g)$ is a representation of G with character $\chi\psi$. $\square$

Remark 3.7. For $\chi, \psi \in \mathrm{Irr}(G)$, $\chi\psi$ is not necessarily irreducible (choose $\chi(1) = \psi(1) > 1$ maximal).

Remark 3.8.

(i) Let $C(G) \in \mathbb{C}^{n\times n}$ and $C(H) \in \mathbb{C}^{m\times m}$ be the character tables of G and H respectively. Then $C(G) \otimes C(H)$ is the character table of $G \times H$ given a suitable ordering.

(ii) Let G be cyclic of order n (we write $G \cong C_n$). According to Exercise 2, the character table of G is given by $(e^{\frac{2\pi ikl}{n}})_{k,l=0}^{n-1}$ ($\mathrm{i} = \sqrt{-1}$). From algebra it is known that every abelian group G is the direct product of cyclic groups. With Theorem 3.5, the character table of G can thus be easily calculated.

Example 3.9. Let $G := \{1, x, y, z\,(= xy)\} \cong C_2 \times C_2 = C_2^2$ be the Klein four-group with $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_4\}$. Then

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{array}{c|cccc} C_2^2 & 1 & x & y & z \\ \hline \chi_1 & 1 & 1 & 1 & 1 \\ \chi_2 & 1 & -1 & 1 & -1 \\ \chi_3 & 1 & 1 & -1 & -1 \\ \chi_4 & 1 & -1 & -1 & 1 \end{array}$$

is the character table of G.

Definition 3.10. For $x, y \in G$, $[x, y] := xyx^{-1}y^{-1}$ is the *commutator* of x and y. Let

$$G' := \langle [x, y] : x, y \in G \rangle$$

be the *derived subgroup* of G.

Remark 3.11. For $\alpha \in \mathrm{Aut}(G)$ and $x, y \in G$ it is obvious that $\alpha([x, y]) = [\alpha(x), \alpha(y)] \in G'$. In particular, $G' \trianglelefteq G$ (choose $\alpha \in \mathrm{Inn}(G)$). For $xG', yG' \in G/G'$ we have

$$xG'yG' = xy\underbrace{[y^{-1}, x^{-1}]}_{\in G'}G' = yG'xG',$$

i. e. G/G' is abelian. Conversely, if $N \trianglelefteq G$ with G/N abelian, then $[x, y]N = xNyN(xN)^{-1}(yN)^{-1} = N$ for $x, y \in G$, i. e. $G' \subseteq N$. Therefore, G' is the smallest normal subgroup with an abelian factor group. The next theorem generalizes Theorem 2.2.

Theorem 3.12. *The linear characters of G are the inflations of* $\mathrm{Irr}(G/G')$.

Proof. Every linear character is a homomorphism $\chi\colon G \to \mathbb{C}^\times$. In particular, $G/\mathrm{Ker}(\chi)$ is abelian as a subgroup of $\mathbb{C}^\times$, i. e. $G' \subseteq \mathrm{Ker}(\chi)$. Thus, deflation yields a $\psi \in \mathrm{Irr}(G/G')$ and χ is the inflation of ψ. Conversely, the inflation of every $\chi \in \mathrm{Irr}(G/G')$ has degree 1 because of Theorem 2.2. □

Example 3.13. The alternating group A_4 possesses, with the Klein four-group

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

a normal 2-Sylow subgroup. The three involutions (elements of order 2) in V_4 are conjugate by a 3-cycle. According to Sylow, every element in $A_4 \setminus V_4$ is conjugate to $x := (1, 2, 3)$ or x^{-1}. On the other hand, x and x^{-1} cannot be conjugate, because otherwise the corresponding cosets in the abelian group $A_4/V_4 \cong C_3$ would also be conjugate. Thus 1, $(1, 2)(3, 4)$, $(1, 2, 3)$ and $(1, 3, 2)$ are representatives for the conjugacy classes of G. By inflation from A_4/V_4 one obtains three linear characters χ_1, χ_2, χ_3. For the remaining character χ_4 we have

$$\chi_4(1)^2 = |A_4| - \chi_1(1)^2 - \chi_2(1)^2 - \chi_3(1)^2 = 9,$$

hence $\chi_4(1) = 3$. The missing values of χ_4 result 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	σ	σ^{-1}
χ_3	1	1	σ^{-1}	σ
χ_4	3	-1	0	0

$$\sigma := e^{2\pi \mathrm{i}/3} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}.$$

Lemma 3.14. *Let $g \in G$ be of order k. For every representation Δ of G with character χ the following holds:*

(i) $\chi(g)$ *is the sum of* $\chi(1)$ *many* k*-th roots of unity.*

(ii) $|\chi(g)| \leq \chi(1)$.

(iii) $|\chi(g)| = \chi(1) \iff \Delta(g) \in \mathbb{C}^\times \mathrm{id}$.

(iv) $\chi(g) = \chi(1) \iff g \in \mathrm{Ker}(\Delta)$.

Proof.

(i) Let $n := \chi(1)$, and let $\epsilon_1, \ldots, \epsilon_n \in \mathbb{C}$ be the eigenvalues of $\Delta(g)$ (with multiplicities). Because of $(\Delta(g))^k = \Delta(g^k) = \Delta(1) = 1_n$, the ϵ_i are k-th roots of unity and $\chi(g) = \epsilon_1 + \ldots + \epsilon_n$.

(ii) We apply the Cauchy-Schwarz inequality to the vectors $v := (\epsilon_1, \ldots, \epsilon_n)$ and $w := (1, \ldots, 1)$:

$$|\chi(g)| = |\epsilon_1 + \ldots + \epsilon_n| = |\langle v, w\rangle| \leq \|v\|\|w\| = \sqrt{n}\sqrt{n} = n. \tag{3.1}$$

(iii) If equality holds in (3.1), then v and w are linearly dependent and it follows that $\epsilon := \epsilon_1 = \epsilon_2 = \ldots = \epsilon_n$. Since $\Delta(g)$ is diagonalizable (Exercise 4), the geometric multiplicity of the eigenvalue ϵ is equal to n, i. e. $\Delta(g) = \epsilon\,\mathrm{id}$. Conversely, if $\Delta(g) \in \mathbb{C}^\times \mathrm{id}$, then $|\chi(g)| = \chi(1)$ certainly follows.

(iv) If even $\chi(g) = \chi(1)$, then obviously $\epsilon = 1$ and $g \in \mathrm{Ker}(\Delta)$. The converse is also clear here. □

Definition 3.15. For a representation Δ with character χ, we set $\mathrm{Ker}(\chi) := \mathrm{Ker}(\Delta)$ and

$$\mathrm{Z}(\chi) := \mathrm{Z}(\Delta) := \{g \in G : |\chi(g)| = \chi(1)\}.$$

One calls $\mathrm{Z}(\chi)$ the *center* of χ (resp. Δ).

Example 3.16.

(i) If $g \in G$ is an involution and χ is a character of G, then $\chi(g) \in \mathbb{Z}$ and $\chi(g) \equiv \chi(1) \pmod 2$ by Lemma 3.14(i).

(ii) Let Δ be a representation of G with character χ and degree n. For $g \in G$ and $z \in \mathrm{Z}(\chi)$, it then holds that

$$\chi(zg) = \mathrm{tr}\big(\Delta(z)\Delta(g)\big) = \mathrm{tr}\Big(\frac{\chi(z)}{n} 1_n \Delta(g)\Big) = \frac{\chi(z)}{n}\,\mathrm{tr}\,\Delta(g) = \frac{\chi(z)\chi(g)}{\chi(1)}.$$

This is useful for completing rows of the character table. Exercise 6 provides a dual statement for the columns of $C(G)$.

Theorem 3.17. *For every character χ of G,* $\mathrm{Ker}(\chi)$ *and* $\mathrm{Z}(\chi)$ *are normal subgroups of G. In this case,* $\mathrm{Ker}(\chi) \leq \mathrm{Z}(\chi)$ *and* $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi)$ *is cyclic.*

Proof. Certainly $\mathrm{Ker}(\chi) \trianglelefteq G$ and $\mathrm{Ker}(\chi) \subseteq \mathrm{Z}(\chi)$. Let $\Delta\colon G \to \mathrm{GL}(V)$ be a representation with character χ. Because of $\mathbb{C}^\times \mathrm{id}_V \trianglelefteq \mathrm{GL}(V)$, $\mathrm{Z}(\chi) = \Delta^{-1}(\mathbb{C}^\times \mathrm{id}_V) \trianglelefteq G$. Furthermore, by the isomorphism theorem, $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi)$ is isomorphic to a finite subgroup H of $\mathbb{C}^\times \mathrm{id}_V \cong \mathbb{C}^\times$. Obviously, H consists precisely of the $|H|$-th roots of unity and is therefore cyclic. □

Remark 3.18.

(i) In this way, one can often construct normal subgroups, because every normal subgroup is the kernel of a character (Exercise 10).

(ii) Let $\mathrm{Cl}(G) = \{K_1, \ldots, K_k\}$, $g_i \in K_i$ and $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$. Then the matrix $\Omega := (\omega_{\chi_i}(K_j))_{i,j}$ differs from the character table $C(G)$ only by scalar multiplication of rows and columns. Therefore, like $C(G)$, Ω is also invertible.

Theorem 3.19. *The character table of G can be calculated from the class multiplication constants.*

Proof (Burnside-*algorithm*). Let $\mathrm{Cl}(G) = \{K_1, \ldots, K_n\}$ and $\gamma_{ijk} := \gamma_{K_iK_jK_k}$ be the class multiplication constant. Let $T_i := (\gamma_{ijk})_{j,k} \in \mathbb{Z}^{n\times n}$. Let $\Delta_1, \ldots, \Delta_n$ be the irreducible representations of G and $\omega_i := \omega_{\Delta_i}$ for $i = 1, \ldots, n$. As in the proof of Theorem 2.17, it holds that

$$\omega_l(K_i)\omega_l(K_j) = \sum_{k=1}^{n} \gamma_{ijk}\omega_l(K_k)$$

for $1 \leq i, j, l \leq n$. Consequently, $e_l := (\omega_l(K_k))_k \in \mathbb{C}^n$ is an eigenvector of T_i with eigenvalue $\omega_l(K_i)$.[2] According to Remark 3.18, $\{e_1, \ldots, e_n\}$ is a basis of $\mathbb{C}^n$. Every eigenspace of T_i is therefore spanned by some of the e_l. We intersect these eigenspaces with the eigenspaces of the T_j for $j \neq i$. The non-trivial intersections have the form

$$V_l := \{v \in \mathbb{C}^n : \forall i : T_i v = \omega_l(K_i)v\} \leq \mathbb{C}^n$$

for some $1 \leq l \leq n$ (note $e_l \in V_l$). Let $v_l \in V_l$ with $\sum_{l=1}^n v_l = 0$. Then it follows that

$$\sum_{l=1}^{n} \omega_l(K_i)v_l = T_i \sum_{l=1}^{n} v_l = 0$$

for $i = 1, \ldots, n$. Since the matrix $(\omega_l(K_i))_{l,i}$ is invertible according to Remark 3.18, it follows that $v_1 = \ldots = v_n = 0$ and $\sum_{l=1}^n V_l = \bigoplus_{l=1}^n V_l$. For dimension reasons, $V_l = \langle e_l \rangle$ for $l = 1, \ldots, n$. Because of $\omega_l(K_1) = 1$, e_l can be calculated from V_l. According to the first orthogonality relation, there exists only one vector e_l, say e_1, which consists only of positive numbers. It belongs to the trivial representation Δ_1. From this, the class lengths $|K_i| = \omega_1(K_i)$ for $i = 1, \ldots, n$ are obtained. Because of

$$\sum_{i=1}^{n} \frac{|\omega_l(K_i)|^2}{|K_i|} = \frac{1}{\chi_l(1)^2} \sum_{i=1}^{n} |K_i||\chi_l(g_i)|^2 = \frac{1}{\chi_l(1)^2} \sum_{g\in G} |\chi_l(g)|^2 = \frac{|G|}{\chi_l(1)^2}(\chi_l, \chi_l)_G = \frac{|G|}{\chi_l(1)^2}$$

one obtains $\chi_l(1)$ and subsequently also $\chi_l(g_i) = \frac{\chi_l(1)\omega_l(K_i)}{|K_i|}$ for $g_i \in K_i$. □

[2] The eigenvalues of T_i can indeed be calculated, but their assignment to ω_l is not unique.

Remark 3.20. As a rule, one does not need all matrices T_i to calculate the character table. If, for example, $\omega_l(K_i)$ as an eigenvalue of T_i has multiplicity 1, then e_l can be determined directly as a generator of the eigenspace. Optimizations of this kind lead to the *Dixon-Schneider algorithm*, which is frequently used in practice.

Theorem 3.21. *Let* $\mathrm{Cl}(G) = \{K_1, \ldots, K_n\}$ *and* $g_i \in K_i$. *Then*

$$\gamma_{ijk} = \frac{|K_i||K_j|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_k)}}{\chi(1)}$$

for $1 \leq i, j, k \leq n$. *The class multiplication constants can thus be determined from the character table.*

Proof. As in the proof of Theorem 3.19, $\omega_\chi(K_i)\omega_\chi(K_j) = \sum_{k=1}^n \gamma_{ijk}\omega_\chi(K_k)$. From this it follows that

$$\frac{|K_i||K_j|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_k)}}{\chi(1)} = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \omega_\chi(K_i)\omega_\chi(K_j)\chi(1)\overline{\chi(g_k)}$$

$$= \frac{1}{|G|} \sum_{l=1}^n \gamma_{ijl} \sum_{\chi \in \mathrm{Irr}(G)} \omega_\chi(K_l)\chi(1)\overline{\chi(g_k)} = \frac{1}{|G|} \sum_{l=1}^n \gamma_{ijl}|K_l| \sum_{\chi \in \mathrm{Irr}(G)} \chi(g_l)\overline{\chi(g_k)} \overset{2.17}{=} \gamma_{ijk}. \qquad \square$$

4 Algebraic integers

Definition 4.1. A number $\zeta \in \mathbb{C}$ is called an *algebraic integer*, if it is a root of a monic, integral polynomial, i.e., there exist numbers $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ with $\zeta^n + a_{n-1}\zeta^{n-1} + \ldots + a_1\zeta + a_0 = 0$.

Example 4.2.

(i) Integers are obviously algebraic integers and algebraic integers are algebraic.

(ii) Roots of unity are algebraic integers as roots of polynomials of the form $X^n - 1$.

Lemma 4.3. *If* $\alpha, \beta \in \mathbb{C}$ *are algebraic integers, then so are* $\alpha + \beta$ *and* $\alpha\beta$. (*The algebraic integers thus form a ring.*)

Proof. We write

$$\begin{aligned} \alpha^n &= a_{n-1}\alpha^{n-1} + \ldots + a_0, \\ \beta^m &= b_{m-1}\beta^{m-1} + \ldots + b_0 \end{aligned} \tag{4.1}$$

with $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1} \in \mathbb{Z}$. Let $S := \{\alpha^i\beta^j : i = 0, \ldots, n-1,\ j = 0, \ldots, m-1\}$ and $\gamma := \alpha + \beta$ (resp. $\alpha\beta$). For $s \in S$ there then exist numbers $c_{st} \in \mathbb{Z}$ with $\gamma s = \sum_{t \in S} c_{st} t$ (use (4.1)). For $A := (c_{st})_{s,t \in S} \in \mathbb{Z}^{nm \times nm}$ and $v := (s : s \in S) \in \mathbb{C}^{nm}$, we have $Av = \gamma v$. Thus γ is a root of the monic, integral, characteristic polynomial $\det(X1_{nm} - A)$. $\square$

Remark 4.4. If χ is a character of G, then $\chi(g)$ is an algebraic integer for $g \in G$ as a sum of roots of unity (Lemma 3.14).

Lemma 4.5. *If* $\zeta \in \mathbb{Q}$ *is algebraic-integral, then* $\zeta \in \mathbb{Z}$.

Proof. Let $\zeta = \frac{r}{s}$ with $r, s \in \mathbb{Z}$ and $\gcd(r,s) = 1$. By assumption, there exist $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ with

$$\frac{r^n}{s^n} = \frac{a_{n-1}r^{n-1}}{s^{n-1}} + \ldots + \frac{a_1 r}{s} + a_0.$$

Rearranging yields

$$r^n = s(a_{n-1}r^{n-1} + \ldots + a_1 r s^{n-2} + a_0 s^{n-1}).$$

Thus $s \mid r^n$. Because of $\gcd(r,s) = 1$, it follows that $s = \pm 1$ and $\zeta \in \mathbb{Z}$. □

Lemma 4.6. *For $C \in \mathrm{Cl}(G)$ and $\chi \in \mathrm{Irr}(G)$, $\omega_\chi(C)$ is algebraic-integral.*

Proof. As shown in the proof of Theorem 3.19, $\omega_\chi(C)$ is an eigenvalue of an integer matrix T. Thus $\omega_\chi(C)$ is algebraic-integral as a root of the monic, integer, characteristic polynomial of T. □

Theorem 4.7. *For $\chi \in \mathrm{Irr}(G)$,* $\boxed{\chi(1) \mid |G|.}$

Proof. Let $g_1, \ldots, g_k \in G$ be representatives for the conjugacy classes $K_1, \ldots, K_k$ of G. According to the first orthogonality relation, it then holds that

$$\frac{|G|}{\chi(1)} = \frac{1}{\chi(1)} \sum_{g \in G} \chi(g)\overline{\chi(g)} = \frac{1}{\chi(1)} \sum_{i=1}^{k} |K_i| \chi(g_i)\chi(g_i^{-1}) = \sum_{i=1}^{k} \omega_\chi(K_i)\chi(g_i^{-1}).$$

By Lemma 4.6, $\frac{|G|}{\chi(1)}$ is algebraic-integral. The claim now follows from Lemma 4.5. □

Example 4.8.

(i) Let G be a p-group with $|G| \geq p^2$. According to Remark 2.15 and Theorem 4.7, it holds that

$$0 \equiv |G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = |G/G'| + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1) > 1}} \chi(1)^2 \equiv |G/G'| \pmod{p^2}$$

and $|G/G'| \geq p^2$. In particular, G is abelian if $|G| = p^2$. By induction on $|G|$, one obtains that every p-group is solvable.

(ii) According to Algebra, the alternating group $G = A_5$ is non-abelian and simple. The permutations

$$1,\ (1,2)(3,4),\ (1,2,3),\ (1,2,3,4,5) \in G$$

have pairwise distinct orders and are therefore not conjugate. Let us assume that $g := (1,2,3,4,5)$ is conjugate to g^2. Let $x \in G$ with $xgx^{-1} = g^2$. Then $x^2 g x^{-2} = g^4 = g^{-1}$ and $x^4 g x^{-4} = g$. Therefore, the order of x must be divisible by 4. However, G possesses no element of order 4. Thus, g and g^2 are not conjugate and $k(G) \geq 5$. Let $\mathbb{1}_G \neq \chi \in \mathrm{Irr}(G)$. Because of $G' = G$, we have $\chi(1) > 1$. Let us assume $\chi(1) = 2$. Let $g := (1,2)(3,4) \in G$. According to Example 3.13, χ_{A_4} is the sum of two linear characters. But then $\chi(g) = 2 = \chi(1)$ would hold, in contradiction to $\mathrm{Ker}(\chi) = 1$. Thus $\chi(1) \geq 3$ holds. For the equation

$$60 = |G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = 1 + \sum_{\chi \neq \mathbb{1}_G} \chi(1)^2.$$

there are now two solutions: $60 = 1 + 3^2 + 3^2 + 4^2 + 5^2 = 1 + 3^2 + 3^2 + 3^2 + 4^2 + 4^2$. Suppose the second decomposition is correct (i. e. $k(G) = 6$). For $\chi(1) = 3$ resp. $\chi(1) = 4$, one obtains $\chi(g) = -1$ resp. $\chi(g) = 0$ from Example 3.13. This shows

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g) = 1 - 3 - 3 - 3 \neq 0$$

in contradiction to the second orthogonality relation. Therefore, $1, 3, 3, 4, 5$ are the character degrees of G and $k(G) = 5$. Since there is only one character of degree 4, it must be real. The restriction to A_4 thus yields the following entries of the character table:

A_5	1	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4,5)$	$(1,3,5,2,4)$
$\mathbb{1}_G$	1	1	1	1	1
χ_2	3	-1	0		
χ_3	3	-1	0		
χ_4	4	0	1		
χ_5	5	1	-1		

We complete the table in Example 5.8 and Example 7.14.

5 Induced characters

Remark 5.1. For $H \leq G$ and $\varphi \in \mathrm{CF}(G)$, the restriction $\varphi_H \colon H \to \mathbb{C}$ is obviously a class function of H. Conversely, we construct a class function on G from $\varphi \in \mathrm{CF}(H)$.

Definition 5.2. For $H \leq G$ and $\varphi \in \mathrm{CF}(H)$, let

$$\boxed{\varphi^G \colon G \to \mathbb{C}, \qquad x \mapsto \frac{1}{|H|} \sum_{\substack{g \in G \\ gxg^{-1} \in H}} \varphi(gxg^{-1}).}$$

One calls φ^G the class function *induced* by φ.

Theorem 5.3. *For $\varphi \in \mathrm{CF}(H)$, we have $\varphi^G \in \mathrm{CF}(G)$.*

Proof. For $x, y \in G$ we have

$$\varphi^G(yxy^{-1}) = \frac{1}{|H|} \sum_{\substack{g \in G \\ gyxy^{-1}g^{-1} \in H}} \varphi(gyxy^{-1}g^{-1}) = \frac{1}{|H|} \sum_{\substack{h \in G \\ hxh^{-1} \in H}} \varphi(hxh^{-1}) = \varphi^G(x). \qquad \square$$

Remark 5.4.

(i) One easily sees that induction is a linear map from $\mathrm{CF}(H)$ to $\mathrm{CF}(G)$.

(ii) If $|\langle x \rangle|$ is not a divisor of $|H|$, then no conjugate of x lies in H and it follows that $\varphi^G(x) = 0$. For $N \trianglelefteq G$, $\varphi \in \mathrm{CF}(N)$ and $x \in G \setminus N$, it likewise holds that $\varphi^G(x) = 0$.

(iii) For $H \leq G$, $\varphi \in \mathrm{CF}(H)$ and $x \in G$ we have

$$\varphi^G(x) = \frac{1}{|H|} \sum_{\substack{g \in G \\ g^{-1}xg \in H}} \varphi(g^{-1}xg) = \frac{1}{|H|} \sum_{gH \in G/H} \sum_{\substack{h \in H \\ h^{-1}g^{-1}xgh \in H}} \varphi(h^{-1}g^{-1}xgh)$$
$$= \frac{1}{|H|} \sum_{h \in H} \sum_{\substack{gH \in G/H \\ g^{-1}xg \in H}} \varphi(g^{-1}xg) = \sum_{\substack{gH \in G/H \\ xgH = gH}} \varphi(g^{-1}xg).$$

This is useful for practical calculation.

Theorem 5.5. *Let $K \leq H \leq G$, $\varphi \in \mathrm{CF}(G)$, $\mu \in \mathrm{CF}(H)$ and $\nu \in \mathrm{CF}(K)$. Then*

(i) $\boxed{(\nu^H)^G = \nu^G}$ (*Transitivity*).

(ii) $\boxed{\varphi\mu^G = (\varphi_H\mu)^G}$

(iii) $\boxed{(\varphi, \mu^G)_G = (\varphi_H, \mu)_H}$ (Frobenius reciprocity).

Proof.

(i) By Remark 5.4(iii) we have

$$(\nu^H)^G(x) = \sum_{\substack{gH \in G/H \\ xgH = gH}} \nu^H(g^{-1}xg) = \sum_{\substack{gH \in G/H \\ xgH = gH}} \sum_{\substack{hK \in H/K \\ g^{-1}xghK = hK}} \nu(h^{-1}g^{-1}xgh)$$
$$= \sum_{\substack{aK \in G/K \\ xaK = aK}} \nu(a^{-1}xa) = \nu^G(x)$$

for $x \in G$.

(ii) As in (i) we have

$$(\varphi\mu^G)(x) = \varphi(x) \sum_{\substack{gH \in G/H \\ xgH = gH}} \mu(g^{-1}xg) = \sum_{\substack{gH \in G/H \\ xgH = gH}} (\varphi_H\mu)(g^{-1}xg) = (\varphi_H\mu)^G(x)$$

for $x \in G$.

(iii) We have

$$(\varphi, \mu^G)_G = \frac{1}{|G|} \sum_{x \in G} \varphi(x) \sum_{\substack{gH \in G/H \\ xgH = gH}} \overline{\mu(g^{-1}xg)} = \frac{1}{|G|} \sum_{gH \in G/H} \sum_{\substack{x \in G \\ g^{-1}xg \in H}} \varphi(g^{-1}xg)\overline{\mu(g^{-1}xg)}$$
$$= \frac{1}{|G|} \sum_{gH \in G/H} \sum_{h \in H} \varphi(h)\overline{\mu(h)} = \frac{|G:H|}{|G|} \sum_{h \in H} \varphi(h)\overline{\mu(h)} = (\varphi_H, \mu)_H. \qquad \square$$

Remark 5.6. Frobenius reciprocity states that restriction and induction are adjoint maps between $\mathrm{CF}(G)$ and $\mathrm{CF}(H)$.

Theorem 5.7. *For every character ψ of $H \leq G$, ψ^G is a character of G of degree $|G:H|\psi(1)$.*

Proof. We write $\psi^G = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi$ with $a_\chi \in \mathbb{C}$. Then

$$a_\chi = (\chi, \psi^G)_G = (\chi_H, \psi)_H \in \mathbb{N}_0,$$

since χ_H is a character of H. Thus ψ^G is a character of G. By definition,

$$\psi^G(1) = \frac{1}{|H|} \sum_{g \in G} \psi(1) = |G : H| \psi(1). \qquad \square$$

Example 5.8.

(i) According to Remark 2.15, $\mathbb{1}_1^G$ is the regular character of G. In particular, φ^G is not necessarily irreducible if φ is irreducible. If φ is reducible, then φ^G must also be reducible due to the linearity of induction.

(ii) Let $G := A_5$ and $H := A_4$. According to Exercise 17, $\pi := (\mathbb{1}_H)^G$ is the permutation character of G on $\{1, \ldots, 5\}$, because H is the stabilizer of 5. For $g \in G$, $\pi(g)$ is the number of fixed points of g. Since G acts transitively, $\mathbb{1}_G$ is an irreducible constituent of π with multiplicity 1. Since G has no irreducible character of degree 2 according to Example 4.8, $\chi := \pi - \mathbb{1}_G$ is an irreducible character of degree 4. One obtains the missing values $\chi((1,2,3,4,5)) = -1 = \chi((1,3,5,2,4))$. Now let $\lambda \in \mathrm{Irr}(H)$ be a non-trivial linear character and $\psi := \lambda^G$. Because of $(\psi, \mathbb{1}_G)_G = (\lambda, \mathbb{1}_H)_H = 0$ and $\psi(1) = |G : H|\lambda(1) = 5$, ψ is also irreducible. Because $5 \nmid 12 = |H|$, no 5-cycle lies in H. This shows $\psi((1,2,3,4,5)) = 0 = \psi((1,3,5,2,4))$.

A_5	1	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4,5)$	$(1,3,5,2,4)$
$\mathbb{1}_G$	1	1	1	1	1
χ_2	3	-1	0		
χ_3	3	-1	0		
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

The missing values are calculated in Example 7.14.

6 Applications

Remark 6.1. William Burnside wrote the first book on group theory in 1897. Due to a lack of applications, the character theory developed by him and Frobenius was not yet mentioned therein. This changed with his proof of the $p^a q^b$-theorem. In the preface of the second edition published in 1911, he writes:

> *Very considerable advances in the theory of groups of finite order have been made since the appearance of the first edition of this book. In particular the theory of groups of linear substitutions has been the subject of numerous and important investigations by several writers; and the reason given in the original preface for omitting any account of it no longer holds good.*

Lemma 6.2. *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 $\alpha := \frac{\chi(g)}{\chi(1)}$. Because of $\gcd(\chi(1), |C|) = 1$, there exist $a, b \in \mathbb{Z}$ with $a\chi(1) + b|C| = 1$. With $\omega_\chi(C)$ and $\chi(g)$, also

$$\alpha = \frac{\chi(g)}{\chi(1)}\big(a\chi(1) + b|C|\big) = a\chi(g) + b\omega_\chi(C)$$

is algebraic-integral. Let $n := |\langle g \rangle|$. As a sum of n-th roots of unity, $\chi(g)$ lies in the cyclotomic field $\mathbb{Q}_n$. Let $\mathcal{G} := \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$. For $\sigma \in \mathcal{G}$, $\sigma(\alpha)$ is also algebraic-integral, because α and $\sigma(\alpha)$ are roots of the same integer polynomial. Therefore, $\beta := \prod_{\sigma\in\mathcal{G}} \sigma(\alpha)$ is also algebraic-integral (Lemma 4.3). Because of $\sigma(\beta) = \beta$ for all $\sigma \in \mathcal{G}$, β lies in the fixed field of $\mathcal{G}$, i. e. $\beta \in \mathbb{Q}$, since $\mathbb{Q} \subseteq \mathbb{Q}_n$ is a Galois extension. According to Lemma 4.5, $\beta \in \mathbb{Z}$. In the case $g \notin \mathrm{Z}(\chi)$, we have $|\alpha| < 1$ (Lemma 3.14). With $\chi(g)$, also $\sigma(\chi(g))$ is a sum of $m := \chi(1)$ many n-th roots of unity $\epsilon_1, \ldots, \epsilon_m$. It follows

$$|\sigma(\chi(g))| = |\epsilon_1 + \ldots + \epsilon_m| \leq |\epsilon_1| + \ldots + |\epsilon_m| = m$$

and $|\sigma(\alpha)| \leq 1$ for $\sigma \in \mathcal{G}$. Consequently, $|\beta| < 1$, i. e. $\beta = 0$. Thus $\alpha = 0$ and $\chi(g) = 0$. □

Theorem 6.3. *Let G be simple and non-abelian, $C \in \mathrm{Cl}(G)$ and $|C|$ a power of a prime p. Then $C = \{1\}$.*

Proof. We assume $C \neq \{1\}$ and choose $g \in C$ and $\chi \in \mathrm{Irr}(G) \setminus \{\mathbb{1}_G\}$. Since G is simple, $\mathrm{Ker}(\chi) = 1$. Since G is non-abelian, also $\mathrm{Z}(\chi) = 1$ (Theorem 3.17). In the case $p \nmid \chi(1)$, we have $\chi(g) = 0$ according to Lemma 6.2. Therefore,

$$\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ p\,\nmid\,\chi(1)}} \frac{\chi(1)}{p}\chi(g) = \frac{1}{p}\sum_{\mathbb{1}_G\neq\chi\in\mathrm{Irr}(G)} \chi(1)\chi(g) = \frac{1}{p}\left(\sum_{\chi\in\mathrm{Irr}(G)} \chi(1)\chi(g) - \mathbb{1}_G(1)\mathbb{1}_G(g)\right) = -\frac{1}{p} \in \mathbb{Q}\setminus\mathbb{Z}$$

is algebraic-integral. Contradiction. □

Theorem 6.4 (Burnside)**.** *Let $|G| = p^a q^b$ with primes p, q and $a, b \in \mathbb{N}_0$. Then G is solvable.*

Proof. Let G be a minimal counterexample and $N \lhd G$. If $N \neq 1$, then N and G/N would be solvable and therefore also G. Thus $N = 1$ and G is simple and non-abelian. Wlog. let $1 \neq P \in \mathrm{Syl}_p(G)$. According to algebra, there exists $g \in \mathrm{Z}(P) \setminus \{1\}$. Let C be the conjugacy class of g. Then

$$|C| = |G : \mathrm{C}_G(g)| \;\big|\; |G : P| = q^b$$

is a prime power. According to Theorem 6.3, $C = \{1\}$. Contradiction. □

Remark 6.5. Theorem 6.4 was one of the first applications of representation theory to the study of finite groups. Meanwhile, a (significantly more difficult) proof is also known that does not require representation theory.[3] However, for Theorem 6.3 and the following theorem, no such proof is known.[4]

Theorem 6.6 (Frobenius)**.** *Let $H \leq G$ with $gHg^{-1} \cap H = 1$ for all $g \in G \setminus H$. Then there exists $N \trianglelefteq G$ with $G = HN$ and $H \cap N = 1$.*

[3] see Section 10.2 in [H. Kurzweil, B. Stellmacher, *Theorie der endlichen Gruppen*, Springer, Berlin, 1998]
[4] see mathoverflow

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

$$xHx^{-1} \cap yHy^{-1} = x(H \cap x^{-1}yHy^{-1}x)x^{-1} = 1.$$

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 $N \cap H = 1$, then $|HN| = |H||N| = |G|$ 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

$$\begin{aligned} c_\chi := (\chi, \rho)_G &= \frac{1}{|G|}\sum_{g\in N} \chi(g)|H| = \frac{1}{|N|}\sum_{g\in G} \chi(g) - \frac{1}{|N|}\sum_{g\in H^*} \chi(g) \\ &= -\sum_{g\in H\setminus\{1\}} \chi(g) = \chi(1) - |H|(\chi_H, \mathbb{1}_H)_H \in \mathbb{Z}. \end{aligned}$$

We can assume $c_\chi \neq 0$. The Cauchy-Schwarz inequality applied to the vectors $(\chi(g) : g \in N)$ and $(1, \dots, 1)$ 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 that

$$1 = (\chi, \chi)_G = \frac{1}{|G|}\sum_{g\in N} |\chi(g)|^2 + \frac{1}{|G|}\sum_{g\in H^*} |\chi(g)|^2 \geq \frac{1}{|H|}\Big(c_\chi^2 + \sum_{g\in H\setminus\{1\}} |\chi(g)|^2\Big) > 0.$$

Because $c_\chi^2 - \chi(1)^2 = (c_\chi + \chi(1))(c_\chi - \chi(1))$, on the other hand,

$$\frac{1}{|H|}\Big(c_\chi^2 + \sum_{g\in H\setminus\{1\}} |\chi(g)|^2\Big) = \frac{1}{|H|}\big(c_\chi^2 - \chi(1)^2\big) + (\chi_H, \chi_H)_H = (\chi_H, \chi_H)_H - (c_\chi + \chi(1))(\chi_H, \mathbb{1}_H)_H \in \mathbb{Z}.$$

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 6.7. In the situation of Theorem 6.6 with $1 < H < G$, G is called a *Frobenius group* with *complement* H and *kernel* N.

Example 6.8. 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 $\langle\sigma\rangle$, because $\sigma^i\tau\sigma^{-i} = \sigma^{2i}\tau \neq \tau$ for $i = 1, \dots, n-1$. Further examples are constructed in Exercise 16.

Theorem 6.9 (Taunt)**.** *For every p-Sylow subgroup P of G, it holds that $G' \cap \mathrm{Z}(G) \cap P \leq P'$.*

Proof. As a subgroup of $\mathrm{Z}(G)$, $N := G' \cap \mathrm{Z}(G) \cap P$ is a normal subgroup of G. Let $\lambda \in \mathrm{Irr}(P)$ be a linear character. Since $\lambda^G(1) = |G : P|$ is not divisible by p, there exists an irreducible constituent χ of λ^G with $d := \chi(1) \not\equiv 0 \pmod{p}$. By Frobenius reciprocity, λ is a constituent of χ_P. Therefore, λ_N is an irreducible constituent of χ_N. Because $N \subseteq \mathrm{Z}(G)$, χ_N can have no other constituents according to Exercise 15. This shows $\chi_N = d\lambda_N$. For $\mu := \det \chi$, it follows that $\mu_N = \det(\chi_N) = \lambda_N^d$ (Remark 2.6). Because $\mu(1) = 1$, it holds that $N \leq G' \leq \mathrm{Ker}(\mu)$ and $\lambda_N^d = \mathbb{1}_N$. On the other hand, $\lambda(x)^{|N|} = \lambda(x^{|N|}) = \lambda(1) = 1$ for all $x \in N$, i. e. $\lambda_N^{|N|} = \mathbb{1}_N$. We choose $a, b \in \mathbb{Z}$ with $ad + b|N| = \gcd(d, |N|) = 1$. Then $\lambda_N = (\lambda_N^d)^a(\lambda_N^{|N|})^b = \mathbb{1}_N$. This shows $N \leq \mathrm{Ker}(\lambda)$. Theorem 3.12 and Exercise 10 applied to P/P' yield

$$N \leq \bigcap_{\substack{\lambda \in \mathrm{Irr}(P) \\ \lambda(1)=1}} \mathrm{Ker}(\lambda) = P'. \qquad \square$$

Example 6.10. Let G be a group of cube-free order (i. e. $|G|$ is not divisible by the third power of a prime number). According to Example 4.8, all Sylow subgroups P of G are abelian. By Taunt, it follows that $G' \cap \mathrm{Z}(G) \cap P = 1$. Since $G' \cap \mathrm{Z}(G) \cap P$ is a Sylow subgroup of $G' \cap \mathrm{Z}(G)$, it even holds that $G' \cap \mathrm{Z}(G) = 1$.

7 Representations over number fields

Remark 7.1. For the symbolic (i.e., exact) calculation of representations with the computer, it is necessary to approximate the field $\mathbb{C}$ by "smaller" fields.

(i) For the development of character theory so far, we have only used that $\mathbb{C}$ has characteristic 0 (Maschke), is algebraically closed (Schur's Lemma), and that complex conjugation exists (scalar product).[5] All statements therefore also hold for the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{C}$ ($\overline{\mathbb{Q}}$ is the set of algebraic numbers). In contrast to $\mathbb{C}$, $\overline{\mathbb{Q}}$ is indeed countable, but infinite-dimensional over $\mathbb{Q}$.

(ii) According to Lemma 3.14, the character values of G lie in the cyclotomic field $\mathbb{Q}_{|G|}$.[6] Brauer's deep induction theorem[7] implies that even every $\mathbb{C}$-representation of G can be realized over $\mathbb{Q}_{|G|}$. We prove a weaker statement with less effort.

(iii) A *number field* is a subfield $K \subseteq \mathbb{C}$ with $|K : \mathbb{Q}| = \dim_{\mathbb{Q}} K < \infty$. In this case, $\mathbb{Q} \subseteq K$ is an algebraic field extension and K lies in $\overline{\mathbb{Q}}$. Let $x_1, \ldots, x_n \in K$ be a $\mathbb{Q}$-basis of K. Let $\mu_i \in \mathbb{Q}[X]$ be the minimal polynomial of x_i for $i = 1, \ldots, n$. Then the splitting field $L \subseteq \mathbb{C}$ of $\mu_1 \ldots \mu_n$ is a Galois extension over $\mathbb{Q}$ with $K \subseteq L$. We can therefore assume, if necessary, that K itself is a Galois extension. As is well known, $\mathbb{Q} \subseteq \mathbb{Q}_n$ is a Galois extension for all $n \in \mathbb{N}$ (we have already used this in the proof of Lemma 6.2).

Theorem 7.2. *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. Let $\psi_1, \ldots, \psi_k$ be the characters of the irreducible $\overline{\mathbb{Q}}$-representations up to similarity. As in Theorem 2.18, $\{\psi_1, \ldots, \psi_k\}$ is an orthonormal basis of $\mathrm{CF}(G)$ and $k = k(G)$. Since every $\overline{\mathbb{Q}}$-representation

[5] We have not used that $\mathbb{C}$ is closed as a normed space.
[6] Even $\mathbb{Q}_{\exp(G)}$ with $\exp(G) := \mathrm{lcm}(|\langle g \rangle| : g \in G)$.
[7] see Theorem 6.7 in Character theory

is also a $\mathbb{C}$-representation, we have

$$\psi_i = \sum_{\chi \in \mathrm{Irr}(G)} a_{i,\chi}\chi$$

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 2.14). 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 such that every (irreducible) $\overline{\mathbb{Q}}$-representation has entries in K. □

Definition 7.3. 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 7.4.

(i) According to Theorem 7.2, every group possesses a splitting field with finite degree over $\mathbb{Q}$. According to Theorem 2.2, $\mathbb{Q}_n$ 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, cf. Exercise 19).

(ii) The companion matrix $B := \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ of the cyclotomic polynomial $\Phi_3 = X^2 + X + 1$ 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. Since the degree of Δ does not divide the group order, Δ cannot be absolutely irreducible (this also follows from Theorem 2.2).

Lemma 7.5. *Let $n, k \in \mathbb{N}$ and $k\mathbb{Z}^n \leq A \leq \mathbb{Z}^n$. Then $A \cong \mathbb{Z}^n$.*

Proof. Induction on n: In the case $n = 1$, $A = d\mathbb{Z} \cong \mathbb{Z}$ with $d \mid k$. Now let $n \geq 2$. Let $\pi\colon A \to \mathbb{Z}$, $(a_1, \ldots, a_n) \mapsto a_n$ be the projection onto the n-th coordinate. Let

$$B := \{(a_1, \ldots, a_{n-1}) \in \mathbb{Z}^{n-1} : (a_1, \ldots, a_{n-1}, 0) \in A\} \cong \mathrm{Ker}(\pi).$$

Then $k\mathbb{Z}^{n-1} \leq B \leq \mathbb{Z}^{n-1}$ holds. By induction it follows that $\mathrm{Ker}(\pi) \cong B \cong \mathbb{Z}^{n-1}$. Since $A/\mathrm{Ker}(\pi) \cong \pi(A) \leq \mathbb{Z}$ is cyclic, there exists $a = (a_1, \ldots, a_n) \in A$ with $A = \langle a \rangle + \mathrm{Ker}(\pi)$. Because of $k\mathbb{Z}^n \leq A$, $a_n \neq 0$. For all $m \in \mathbb{Z}\backslash\{0\}$, $ma \notin \mathrm{Ker}(\pi)$ therefore holds. Thus $\langle a \rangle \cap \mathrm{Ker}(\pi) = 0$ and $A = \langle a \rangle \oplus \mathrm{Ker}(\pi) \cong \mathbb{Z}^n$. □

Theorem 7.6 (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 $\mathrm{GL}(n, p)$.*

Proof. Obviously $M := \sum_{g \in G} g\mathbb{Z}^n \subseteq \mathbb{Q}^n$ is an abelian group containing $\mathbb{Z}^n = 1\mathbb{Z}^n$. If k is the lcm of all denominators of matrix entries from all $g \in G$, then $k\mathbb{Z}^n \subseteq kM \subseteq \mathbb{Z}^n$ holds. According to Lemma 7.5, $M \cong kM \cong \mathbb{Z}^n$. Let $\gamma\colon \mathbb{Z}^n \to M$ be a corresponding isomorphism of abelian groups. 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

$$(\gamma^{-1} g \gamma)(\mathbb{Z}^n) = (\gamma^{-1} g)(M) = \gamma^{-1}(M) = \mathbb{Z}^n.$$

An evaluation at the standard basis 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

$$\Gamma\colon G \to \mathrm{GL}(n,p), \qquad (a_{ij}) \mapsto (a_{ij} + p\mathbb{Z}),$$

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 of $g \equiv 1_n \pmod p$, we have $p \mid d$. According to 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 of $p > 2$, one obtains the contradiction

$$-A = \frac{p-1}{2}dA + \ldots + \frac{d^{p-1}}{p}A^p \equiv 0 \pmod p. \qquad \square$$

Corollary 7.7. *For every $n \in \mathbb{N}$, $\mathrm{GL}(n,\mathbb{Q})$ has, up to isomorphism, only finitely many finite subgroups.*

Proof. For every finite subgroup $G \leq \mathrm{GL}(n,\mathbb{Q})$, we have $|G| \leq |\mathrm{GL}(n,3)| \leq 3^{n^2}$ according to Theorem 7.6. $\square$

Remark 7.8. In Corollary 13.15 we will show that there are in fact only finitely many conjugacy classes of finite subgroups in $\mathrm{GL}(n,\mathbb{Q})$.

Example 7.9.

(i) The companion matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$ of $\Phi_6 = X^2 - X + 1$ has order 6. Because of $\mathrm{GL}(2,2) \cong S_3$, Theorem 7.6 cannot hold for $p = 2$ (cf. Exercise 31).

(ii) Let $G \leq \mathrm{GL}(n,\mathbb{Q})$. For $n = 1$ it is obvious that $G \leq \langle -1 \rangle$. As is well known,

$$|\mathrm{GL}(n,p)| = (p^n - 1)(p^n - p)\ldots(p^n - p^{n-1})$$

holds for every prime p. For $n = 2$ and $p = 3$ one obtains $|G| \mid 48$. According to Exercise 9,

$$Q_8 \cong \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\rangle \leq \mathrm{SL}(2,3)$$

is, however, not conjugate to any subgroup of $\mathrm{GL}(2,\mathbb{Q})$. Since $\mathrm{SL}(2,3)$ is the only subgroup of order 24 in $\mathrm{GL}(2,3)$ (without proof), it holds that $|G| \in \{1,2,3,4,6,8,12\}$. With the matrix from (i), it holds that

$$D_{12} \cong \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \leq \mathrm{GL}(2,\mathbb{Z}).$$

According to Example 1.4, D_8 is also isomorphic to a subgroup of $\mathrm{GL}(2,\mathbb{Z})$.

(iii) An $n \times n$-matrix of the form $(\epsilon_i \delta_{i\pi(j)})_{i,j}$ with $\pi \in S_n$ and $\epsilon_1, \ldots, \epsilon_n \in \{\pm 1\}$ is called a *generalized permutation matrix*. The generalized permutation matrices form a subgroup $M \leq \mathrm{GL}(n,\mathbb{Z})$ of order $2^n n!$. Feit has shown that for $n \geq 11$ there is no larger subgroup and every subgroup of order $2^n n!$ is conjugate to M.

(iv) With C_n and D_{2n} for $n \in \mathbb{N}$, $\mathrm{GL}(2,\mathbb{R})$ possesses infinitely many finite subgroups (Example 1.4). According to Exercise 32, these are, up to conjugation, the only such subgroups.

(v) For $G \leq \mathrm{GL}(n,\mathbb{C})$ there exists an abelian normal subgroup $A \trianglelefteq G$ such that $|G:A|$ is bounded by a function in n (JORDAN's theorem). For $n \geq 71$ it specifically holds that $|G:A| \leq (n+1)!$ with equality for $G = S_{n+1}$ (Exercise 18).

(vi) Minkowski's theorem cannot be generalized to number fields: FEIT has shown that Q_8 is isomorphic to a subgroup of $\mathrm{GL}(2,\mathbb{Q}(\sqrt{-35}))$, but not to a subgroup of $\mathrm{GL}(2,R)$, where $R = \mathbb{Z}[(1+\sqrt{-35})/2]$ is the ring of integers of $\mathbb{Q}(\sqrt{-35})$.[8] To show that Corollary 7.7 holds for number fields, we first generalize the complex conjugation of characters.

Theorem 7.10. *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 ${}^{\sigma}\mathrm{Cl}(g) := \mathrm{Cl}(g^k)$ 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 $\gcd(k,n) = 1$, there exists $k' \in \mathbb{Z}$ with $kk' \equiv 1 \pmod{n}$. Therefore $G \to G$, $g \mapsto g^k$ is a bijection with inverse map $g \mapsto g^{k'}$. 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

$$ {}^{\sigma\tau}\mathrm{Cl}(g) = \mathrm{Cl}(g^{kl}) = {}^{\sigma}(\mathrm{Cl}(g^l)) = {}^{\sigma}({}^{\tau}\mathrm{Cl}(g)). $$

Thus $\mathcal{G}$ acts on $\mathrm{Cl}(G)$.

(ii) Let K be a number field as in Theorem 7.2 and $\Delta\colon G \to \mathrm{GL}(d,K)$ a representation with character χ. According to Remark 7.1 we can assume that $\mathbb{Q} \subseteq K$ is a Galois extension containing $\mathbb{Q}_n$. Because of

$$ |\mathrm{Gal}(K|\mathbb{Q})/\mathrm{Gal}(K|\mathbb{Q}_n)| = \frac{|K:\mathbb{Q}|}{|K:\mathbb{Q}_n|} = |\mathbb{Q}_n:\mathbb{Q}| $$

the restriction $\mathrm{Gal}(K|\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ is surjective. Let $\hat{\sigma} \in \mathrm{Gal}(K|\mathbb{Q})$ 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 $\Delta(g)$. Then it holds that

$$ \chi(g^k) = \mathrm{tr}\,\Delta(g^k) = \zeta^{a_1 k} + \ldots + \zeta^{a_d k} = \sigma(\zeta^{a_1} + \ldots + \zeta^{a_d}) = \sigma(\chi(g)) $$

(cf. Exercise 5). One easily sees that $(\sigma,\chi) \mapsto {}^{\sigma}\chi$ defines an action. □

Corollary 7.11. *If $\chi \in \mathrm{Irr}(G)$ is the only irreducible character of degree d, then χ is integer-valued.*

Proof. For $\sigma \in \mathcal{G}$ it holds that ${}^{\sigma}\chi = \chi$. Therefore the values of χ lie in the fixed field $\mathbb{Q}$ of $\mathcal{G}$, since $\mathbb{Q} \subseteq \mathbb{Q}_n$ is a Galois extension. As algebraic integers, the values of χ are integers. □

[8] R is the set of algebraic integers in $\mathbb{Q}(\sqrt{-35})$.

Remark 7.12.

(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 ${}^{\sigma}\mathrm{Cl}(g) := \mathrm{Cl}(g^{k'})$ with $kk' \equiv 1 \pmod{n}$. Then $({}^{\sigma}\chi)({}^{\sigma}g) = \chi(g)$ holds.

(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 $g \in G$, we have ${}^{\alpha}\mathrm{Cl}(g) := \mathrm{Cl}(\alpha(g))$ and $({}^{\alpha}\chi)(g) = \chi(\alpha^{-1}(g))$. Again, one obtains $({}^{\alpha}\chi)({}^{\alpha}g) = \chi(g)$. Since $\mathrm{Inn}(G)$ lies in the kernel of both actions, it suffices to consider the actions of the outer automorphism group $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

(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 7.13 (Brauer's Permutation Lemma)**.** *Let G, H be finite groups such that G acts on $\mathrm{Cl}(H)$ and $\mathrm{Irr}(H)$. For all $g \in G$, $h \in H$ and $\chi \in \mathrm{Irr}(H)$, let $({}^{g}\chi)({}^{g}\mathrm{Cl}(h)) = \chi(h)$. Then the cycle types of g in $\mathrm{Sym}(\mathrm{Cl}(H))$ and $\mathrm{Sym}(\mathrm{Irr}(H))$ coincide. In particular,*

$$\big|\{C \in \mathrm{Cl}(H) : {}^{g}C = C\}\big| = \big|\{\chi \in \mathrm{Irr}(H) : {}^{g}\chi = \chi\}\big|$$

holds for all $g \in G$.

Proof. Let $\mathrm{Cl}(H) = \{K_1, \ldots, K_k\}$ and $\mathrm{Irr}(H) = \{\chi_1, \ldots, \chi_k\}$. Let $X := (\chi_i(K_j))_{i,j}$ be the character table of H. Let $g \in G$ be fixed. The action of g on $\mathrm{Irr}(H)$ (resp. $\mathrm{Cl}(H)$) is described by multiplication with a permutation matrix $P = (\delta_{i\sigma(j)})$ (resp. $Q = (\delta_{i\tau(j)})$ from the left (resp. right):

$$\begin{aligned} PX &= \Big(\sum_{l=1}^{k} \delta_{i\sigma(l)}\chi_l(K_j)\Big)_{i,j} = \big(\chi_{\sigma^{-1}(i)}(K_j)\big)_{i,j} = \big({}^{g^{-1}}\chi_i(K_j)\big)_{i,j} = \big(\chi_i({}^{g}K_j)\big)_{i,j} \\ &= \big(\chi_i(K_{\tau(j)})\big)_{i,j} = \Big(\sum_{l=1}^{k} \chi_i(K_l)\delta_{l\tau(j)}\Big)_{i,j} = XQ. \end{aligned}$$

According to the second orthogonality relation, X is invertible. It follows that $P = XQX^{-1}$, i. e. P and Q are similar. Let $(l_1, \ldots, l_n)$ be the cycle type of P. From Exercise 14, one obtains the eigenvalues of P:

$$\big\{e^{2\pi \mathrm{i} j/l_s} : s = 1, \ldots, n,\ j = 0, \ldots, l_s - 1\big\}$$

(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. □

Example 7.14.

(i) Let $|G|$ be odd. Suppose there exist $g, x \in G$ with $xgx^{-1} = g^{-1}$. Then $x^2gx^{-2} = g$. Since $n := |\langle x \rangle|$ is odd by Lagrange, there exist $a, b \in \mathbb{Z}$ with $an + 2b = 1$. It follows

$$g^{-1} = x^{an+2b}gx^{-an-2b} = x^{2b}gx^{-2b} = g = 1.$$

Therefore $g = 1$ is the only fixed point of the map $\mathrm{Cl}(G) \to \mathrm{Cl}(G)$, $\mathrm{Cl}(g) \mapsto \mathrm{Cl}(g^{-1})$. By Brauer's permutation lemma, $\mathbb{1}_G$ is the only fixed point of the map $\mathrm{Irr}(G) \to \mathrm{Irr}(G)$, $\chi \mapsto \overline{\chi}$. We choose

$\chi_1, \ldots, \chi_s \in \mathrm{Irr}(G)$ with $\mathrm{Irr}(G) = \{\mathbb{1}_G, \chi_1, \ldots, \chi_s, \overline{\chi_1}, \ldots, \overline{\chi_s}\}$. Because of $\chi_i(1) \mid |G|$, it holds that $\chi_i(1)^2 \equiv 1, 9 \pmod{16}$ and $2\chi_i(1)^2 \equiv 2 \pmod{16}$. This shows

$$|G| = 1 + \sum_{i=1}^{s} \big(\chi_i(1)^2 + \overline{\chi_i}(1)^2\big) \equiv 1 + 2s \equiv k(G) \pmod{16}.$$

(ii) In Example 5.8 we had constructed an (integer) part of the character table of $G = A_5$. Let $g = (1,2,3,4,5) \in G$. Because of $(2,5)(3,4)g(2,5)(3,4) = (1,5,4,3,2) = g^{-1}$, the entire character table of G is real. By Brauer's permutation lemma, there exist two Galois-conjugate characters $\chi, \psi \in \mathrm{Irr}(G)$ (of the same degree) with values in $\mathbb{Q}_5$. It must hold that $\chi(1) = \psi(1) = 3$. Since $\chi(g)$ is a sum of three 5-th roots of unity, wlog. $\chi(g) = 1 + \zeta + \zeta^{-1} = \frac{1+\sqrt{5}}{2}$ and $\psi(g) = 1 + \zeta^2 + \zeta^{-2} = \frac{1-\sqrt{5}}{2}$ with $\zeta = e^{2\pi \mathrm{i}/5}$. [9]

A_5	1	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4,5)$	$(1,3,5,2,4)$
$\mathbb{1}_G$	1	1	1	1	1
χ_2	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Theorem 7.15 (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 Lemma 3.14, 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 $\mathbb{Z}$. According to Lemma 3.14, $|\psi(g)| \leq dk$ holds for all $g \in G$. Therefore, ψ takes at most $2dk + 1$ many values, say $dk = x_0, \ldots, x_s$ with $s \leq 2dk$. Let $m_i := |\{g \in G : \psi(g) = x_i\}|$ for $0 \leq i \leq s$. Since χ is faithful, ψ is also faithful (Exercise 10). This shows $m_0 = 1$ according to Lemma 3.14. Since ψ^l is a character, it holds that

$$\sum_{i=0}^{s} m_i x_i^l = \sum_{g \in G} \psi(g)^l = |G|(\psi^l, \mathbb{1}_G)_G \equiv 0 \pmod{|G|}$$

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 adjugate matrix of 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,

$$|G| \leq \prod_{i<j} |x_j - x_i| \leq (2dk)^{\binom{s+1}{2}} \leq (2dk)^{\binom{2dk+1}{2}}.$$ □

[9] These values can also be calculated using the second orthogonality relation.

Corollary 7.16. *For $n \in \mathbb{N}$ and every number field K, $\mathrm{GL}(n, K)$ possesses only finitely many finite subgroups up to isomorphism.*

Proof. One applies Theorem 7.15 to the character of an embedding $G \to \mathrm{GL}(n, K)$. □

8 Algebras

Remark 8.1. In the next four chapters, we introduce ring-theoretic concepts that are useful for the study of representations over fields with positive characteristic. For this, let K be an arbitrary field.

Definition 8.2. An *algebra* over K (briefly a *K-algebra*) is a ring A (with identity) and at the same time a finite-dimensional K-vector space, such that the scalar multiplication and the ring multiplication are compatible, i. e.,

$$\lambda(ab) = (\lambda a)b = a(\lambda b)$$

holds for all $\lambda \in K$ and $a, b \in A$. One calls A a *division algebra* if $A^\times = A \setminus \{0\}$ holds, i. e., every element different from 0 is invertible.

- 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 subalgebra $K1_A$ of A.
- 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.

Example 8.3.

(i) If $K \subseteq L$ is a finite field extension, then L is a K-algebra, where ring and scalar multiplication are identical.

(ii) For $\varphi \in K[X] \setminus K$, $A := K[X]/(\varphi)$ is a commutative K-algebra with $\dim A = \deg \varphi$.

(iii) For every K-algebra A, the *center* $\mathrm{Z}(A) := \{a \in A : \forall b \in A : ab = ba\}$ is a commutative subalgebra.

(iv) If $A_1, \ldots, A_n$ are algebras over K, then so is the direct product $A_1 \times \ldots \times A_n$.

(v) If A is a K-algebra and $n \in \mathbb{N}$, then $A^{n\times n}$ is also a K-algebra. In particular, $K^{n\times n}$ is a K-algebra.

(vi) If one replaces the multiplication of an algebra A by $a * b := ba$, one obtains the *opposite* algebra A^o. The transposition provides an isomorphism $\varphi\colon (A^{n\times n})^o \cong (A^o)^{n\times n}$, $a \mapsto a^{\mathrm{t}}$, because

$$\varphi(a * b) = \varphi(ba) = (ba)^{\mathrm{t}} = \Big(\sum_{k=1}^{n} b_{jk}a_{ki}\Big)_{i,j} = \Big(\sum_{k=1}^{n} a_{ki} * b_{jk}\Big)_{i,j} = a^{\mathrm{t}} * b^{\mathrm{t}} = \varphi(a) * \varphi(b)$$

for $a, b \in A$. For algebras A, B, the identity is an isomorphism $(A \times B)^o \to A^o \times B^o$.

(vii) A commutative division algebra is a field. Wedderburn has shown that every finite division algebra is a field.

(viii) Every skew field R is a $\mathrm{Z}(R)$-division algebra, because $\mathrm{Z}(R)$ is a field in this case.

Lemma 8.4. *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 polynomial $\alpha \in K[X]\backslash K$ with $\alpha(x) = 0$. Since K is algebraically closed, α splits into linear factors, say $\alpha = (X - \lambda_1) \ldots (X - \lambda_n)$ with $\lambda_1, \ldots, \lambda_n \in K$. As a division algebra, D has no zero divisors. From $\alpha(x) = 0$ it follows that $x = \lambda_i 1_D$ for some $i \in \{1, \ldots, n\}$. Therefore $D = K1_D \cong K$. □

Definition 8.5. Let A be a K-algebra.

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

(ii) One calls A *simple*, if $\{0\}$ and A are the only ideals of A. As usual, we use the notation $0 := \{0\}$ for the zero ideal.

(iii) For $I, J \trianglelefteq A$, also $I + J := \{x + y : x \in I, y \in J\}$, $I \cap J$ and

$$IJ := \Big\{ \sum_{i=1}^{n} x_i y_j : n \in \mathbb{N}, x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J \Big\}$$

are ideals of A. Here $IJ \subseteq I \cap J \subseteq I \cup J \subseteq I + J$ holds.

(iv) For $I \trianglelefteq A$ let $I^0 := A$ and $I^{n+1} := I^n I$ for $n \in \mathbb{N}_0$. One calls I *nilpotent*, if an n with $I^n = 0$ exists.

Example 8.6.

(i) Let $f\colon A \to B$ be a homomorphism of algebras. For $J \trianglelefteq B$, the preimage $f^{-1}(J) \trianglelefteq A$. For $I \trianglelefteq A$, on the other hand, $f(I)$ is usually *not* an ideal of B.

(ii) Every division algebra is simple.

(iii) Let $0 \neq I \trianglelefteq A := K^{n \times n}$ and $x = (x_{ij}) \in I$ with $x_{st} \neq 0$. Let $E_{st} \in A$ be the matrix with a 1 at position (s, t) and zeros elsewhere. Then $E_{ij} = x_{st}^{-1} E_{is} x E_{tj} \in I$ for all $1 \leq i, j \leq n$. This shows $I = A$. Thus A is simple, but not a division algebra for $n \geq 2$.

(iv) Let $A \subseteq K^{n \times n}$ be the subalgebra of all upper triangular matrices. The triangular matrices with zeros on the main diagonal form a nilpotent ideal $I \trianglelefteq A$ with $I^n = 0 \neq I^{n-1}$.

Remark 8.7. Let $I \trianglelefteq A$, $x \in I$ and $\lambda \in K$. Then $\lambda x = (\lambda 1_A)x \in I$ holds. Therefore I is a K-vector space. As is well known, A/I is a ring and thus also a K-algebra.

Theorem 8.8.

(i) (Homomorphism Theorem) For every homomorphism $f\colon A \to B$ of algebras, $\mathrm{Ker}(f) \trianglelefteq A$ *and $f(A)$ is a subalgebra of B. Furthermore,*

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

is an isomorphism of algebras.

(ii) (1st Isomorphism Theorem) Let B be a subalgebra of A and $I \trianglelefteq A$. Then $B + I$ is a subalgebra of A, $I \trianglelefteq B + I$, $B \cap I \trianglelefteq B$ and

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

(iii) (*Correspondence Theorem*) *Let $I \trianglelefteq A$. Then the map $\{J \trianglelefteq A : I \subseteq J\} \to \{L \trianglelefteq A/I\}$, $J \mapsto J/I$ is a bijection.*

(iv) (*2nd Isomorphism Theorem*) *Let $I, J \trianglelefteq A$ with $I \subseteq J$. Then*

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

Proof. According to algebra, the map $F\colon A/\mathrm{Ker}(f) \to f(A)$, $a\mathrm{Ker}(f) \mapsto f(a)$ is at least a ring isomorphism. Obviously, F is also K-linear and thus an isomorphism of algebras. The isomorphism theorems are applications of the homomorphism theorem and therefore also hold for algebras. This also includes the well-definedness of the map $f(J) = J/I$ from the correspondence theorem. Since J is the union of the cosets J/I, f is injective. Now let $L \trianglelefteq A/I$ and $\pi\colon A \to A/I$, $a \mapsto a + I$ be the canonical epimorphism. Then $J := \pi^{-1}(L) \trianglelefteq A$ with $I \subseteq J$ and $f(J) = J/I = \pi(J) = L$. □

Lemma 8.9. *If $I, J \trianglelefteq A$ are nilpotent, then so is $I + J$.*

Proof. Let $n \in \mathbb{N}$ with $I^n = J^n = 0$. Every element of $(I+J)^{2n}$ has the form $z := (x_1+y_1)\dots(x_{2n}+y_{2n})$ with $x_1, \dots, x_{2n} \in I$ and $y_1, \dots, y_{2n} \in J$. By multiplying out, one obtains a sum of terms of the form $z_1 \dots z_{2n}$ with $z_1, \dots, z_{2n} \in I \cup J$. Wlog. at least n many of the z_i lie in I. Then $z_1 \dots z_{2n} \in I^n = 0$. This shows $z = 0$ and $(I + J)^{2n} = 0$. □

Definition 8.10. Let A be an algebra.

(i) The sum $\mathrm{J}(A)$ of all nilpotent ideals of A is called the (Jacobson) *radical* of A. For dimension reasons, $\mathrm{J}(A)$ is already the sum of finitely many nilpotent ideals. According to Lemma 8.9, $\mathrm{J}(A)$ is thus the largest nilpotent ideal of A.

(ii) A is called *semisimple*, if $\mathrm{J}(A) = 0$ holds.

(iii) A is called *local*, if $A/\mathrm{J}(A)$ is a division algebra.

Example 8.11.

(i) Because of $1 \in A^n$ for all $n \in \mathbb{N}$, $\mathrm{J}(A) \neq A$. Every simple algebra is thus semisimple. On the other hand, $K \times K$ is semisimple, but not simple, because $K \times 0 \trianglelefteq K \times K$. Note:

$$\text{field} \implies \text{division algebra} \implies \text{simple} \implies \text{semisimple}$$

(ii) If A is local, then $\mathrm{J}(A)$ is a maximal ideal of A according to the correspondence theorem. In this respect, local is the opposite of semisimple.

(iii) Let $A \subseteq K^{n\times n}$ be the algebra of upper triangular matrices with $n \geq 2$. Then $\mathrm{J}(A)$ consists of the triangular matrices with zeros on the main diagonal. The epimorphism $A \to K^n$, $(a_{ij}) \mapsto (a_{11}, \dots, a_{nn})$ has kernel $\mathrm{J}(A)$. In particular, $A/\mathrm{J}(A) \cong K^n$ is not a division algebra. Thus A is neither semisimple nor local.

(iv) The algebra $A := K[X]/(X^2)$ is local with $\mathrm{J}(A) = (X)/(X^2)$ and $A/\mathrm{J}(A) \cong K[X]/(X) \cong K$.

Lemma 8.12. *For algebras A, B and $n \in \mathbb{N}$ the following holds:*

(i) $A/\mathrm{J}(A)$ is semisimple.

(ii) $\boxed{\mathrm{Z}(A \times B) = \mathrm{Z}(A) \times \mathrm{Z}(B).}$

(iii) $\boxed{\mathrm{J}(A \times B) = \mathrm{J}(A) \times \mathrm{J}(B).}$

(iv) $\boxed{\mathrm{Z}(A^{n\times n}) = \mathrm{Z}(A)1_n \cong \mathrm{Z}(A).}$

(v) $\boxed{\mathrm{J}(A^{n\times n}) = \mathrm{J}(A)^{n\times n}.}$

Proof.

(i) According to the correspondence theorem, there exists an ideal $I \trianglelefteq A$ with $I/\mathrm{J}(A) = \mathrm{J}(A/\mathrm{J}(A))$. There exist $n, m \in \mathbb{N}$ with $\mathrm{J}(A)^n = 0$ and $I^m \subseteq \mathrm{J}(A)$. Therefore $I^{nm} = 0$ and $I = \mathrm{J}(A)$.

(ii) For $(a, b) \in A \times B$ we have

$$\begin{aligned}(a,b) \in \mathrm{Z}(A \times B) &\iff \forall x \in A, y \in B : (xa, yb) = (x,y)(a,b) = (a,b)(x,y) = (ax, by)\\ &\iff (a,b) \in \mathrm{Z}(A) \times \mathrm{Z}(B).\end{aligned}$$

(iii) We identify A with $A \times 0$ and B with $B \times 0$. Obviously, $\mathrm{J}(A)$ and $\mathrm{J}(B)$ are then nilpotent ideals of $A \times B$. This shows $\mathrm{J}(A) \times \mathrm{J}(B) = \mathrm{J}(A) + \mathrm{J}(B) \subseteq \mathrm{J}(A \times B) =: J$. For $(a, b) \in J$, we have $(a, 0) = (a, b)(1, 0) \in J \cap A$ and $(0, b) \in J \cap B$. Since $J \cap A$ and $J \cap B$ are nilpotent ideals of A and B respectively, it follows

$$(a, b) = (a, 0) + (0, b) \in J \cap A + J \cap B \subseteq \mathrm{J}(A) \times \mathrm{J}(B).$$

Thus $J \subseteq \mathrm{J}(A) \times \mathrm{J}(B)$ holds.

(iv) Certainly $\mathrm{Z}(A)1_n \subseteq \mathrm{Z}(A^{n\times n})$. Conversely, let $M = (a_{ij}) \in \mathrm{Z}(A^{n\times n})$. Then

$$(\delta_{jt}a_{is})_{i,j} = \Big(\sum_{k=1}^{n} a_{ik}\delta_{ks}\delta_{jt}\Big)_{i,j} = ME_{st} = E_{st}M = \Big(\sum_{k=1}^{n} \delta_{is}\delta_{kt}a_{kj}\Big)_{i,j} = (\delta_{is}a_{tj})_{i,j}$$

for all $1 \leq s, t \leq n$ and it follows $M \in A1_n$. Certainly $M \in \mathrm{Z}(A1_n) = \mathrm{Z}(A)1_n$ also holds.

(v) Let $J := \mathrm{J}(A)$. An induction on k shows $(J^{n\times n})^k \subseteq (J^k)^{n\times n}$. Thus $J^{n\times n}$ is nilpotent and $J^{n\times n} \subseteq \mathrm{J}(A^{n\times n})$. Conversely, let $a = (a_{ij})_{i,j} \in \mathrm{J}(A^{n\times n})$. Let $I = (a_{st}) \trianglelefteq A$ 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 $\mathrm{J}(A^{n\times n}) \subseteq J^{n\times n}$. □

Definition 8.13. An element e of an algebra A is called

- *idempotent*, if $e^2 = e$ holds.
- *nilpotent*, if $e^n = 0$ holds for some $n \in \mathbb{N}$.

Example 8.14.

(i) In every algebra A, 0 and 1 are idempotents.

(ii) If $e \in A$ is an idempotent, then so is $1 - e$, because $(1 - e)^2 = 1 - e - e + e^2 = 1 - e$. For $a \in A^\times$, aea^{-1} is also an idempotent, because $(aea^{-1})^2 = aea^{-1}aea^{-1} = ae^2a^{-1} = aea^{-1}$.

(iii) The matrices of the form E_{ii} are idempotents in $K^{n\times n}$.

(iv) Obviously, $\mathrm{J}(A)$ consists of nilpotent elements. On the other hand, $E_{12} \in K^{2\times 2}$ is nilpotent, but $\mathrm{J}(K^{2\times 2}) = 0$.

Lemma 8.15 (Lifting of units/idempotents)**.** *Let A be an algebra and $I \trianglelefteq A$ nilpotent. Then:*

(i) If $e + I \in (A/I)^\times$ is a unit, then so is $e \in A^\times$.

(ii) For every idempotent $\bar{e} \in A/I$, there exists an idempotent $e \in A$ with $e + I = \bar{e}$.

Proof (Koh).

(i) Let $a \in A$ with $ea \equiv 1 \pmod{I}$ and $b := 1 - ea \in I$. Since I is nilpotent, there exists an $n \in \mathbb{N}$ with $b^n = 0$. This shows

$$e \cdot a \sum_{k=0}^{n-1} b^k = (1-b) \sum_{k=0}^{n-1} b^k = 1 - b^n = 1.$$

An analogous calculation with $1 - ae$ yields $e \in A^\times$.

(ii) Let $a \in A$ 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 $a^{2n-i}(1-a)^j = 0$ for $0 \le i \le n$ and $n+1 \le j \le 2n$, it follows that $ef = 0$. This shows $e = e(e+f) = e^2 + ef = e^2$ and $e \equiv a^{2n} \equiv a \pmod{I}$. □

9 Modules

Remark 9.1. In this chapter, we investigate "vector spaces" over algebras instead of fields. Unlike in linear algebra, in this situation bases do not exist in general (see Example 9.3). Even if bases exist, they do not have to be of the same size. The theory thereby becomes more complicated, but also richer. Let A always be a K-algebra.

Definition 9.2. An *A-module* is a finite-dimensional K-vector space M with an operation $A \times M \to M$, $(a, m) \mapsto am$ such that for $a, b \in A$, $m, n \in M$ and $\lambda \in K$:

- $a(m+n) = am + an$.
- $(a+b)m = am + bm$.
- $(ab)m = a(bm)$.
- $1_A m = m$.
- $\lambda m = (\lambda 1_A)m$

Example 9.3.

(i) The *trivial* A-module $0 := \{0\}$.

(ii) If A is a field, then the A-modules are exactly the A-vector spaces.

(iii) Through the ordinary multiplication $A \times A \to A$, $(a, b) \mapsto ab$, A becomes an A-module, which is called the *regular* A-module.

(iv) For A-modules M, N, $M \times N$ is also an A-module.

(v) For $n, m \in \mathbb{N}$, $K^{n\times m}$ is a $K^{n\times n}$-module with respect to matrix multiplication. In particular, $K^n := K^{n\times 1}$ is a $K^{n\times n}$-module. For every $x \in K^n$ and $A := K^{n\times n}$, $Ax = K^n$ holds (linear algebra), i. e. $\{x\}$ is a generating set of K^n. On the other hand, there exists an $a \in A \setminus \{0\}$ with $ax = 0$, i. e. $\{x\}$ is linearly dependent. This shows that K^n has no basis as an A-module.

Remark 9.4. Let M be an A-module, $a \in A$ and $m \in M$. Then, as in linear algebra, it holds that

$$a0_M = a(0_M + 0_M) = a0_M + a0_M = 0_M,$$
$$0_A m = (0_A + 0_A)m = 0_A m + 0_A m = 0_M.$$

Definition 9.5.

- A subset N of an A-module M is called a *submodule* of M if N with the restricted operations is itself an A-module. As with groups, we then write $N \leq M$ or $N < M$ if $N \neq M$.
- If 0 and $M \neq 0$ are the only submodules, then M is called *simple*.

Example 9.6.

(i) As usual, intersections and sums of submodules are again submodules.

(ii) Let $A = K^{n\times n}$ and $M = K^n$. For $x, y \in M \setminus \{0\}$, there exists an $a \in A$ with $ax = y$ (linear algebra). Therefore, M is a simple A-module. In contrast to vector spaces, simple modules are thus not necessarily 1-dimensional.

(iii) For A-modules $N \leq M$, the quotient space M/N is also an A-module with $a(m + N) := am + N$ for $a \in A$, $m + N \in M/N$.

(iv) For submodules $U, V, W \leq M$ with $U \leq W$, the Dedekind *identity* holds:

$$\boxed{U + (V \cap W) = (U + V) \cap W.}$$

Definition 9.7. A map $f\colon M \to N$ for A-modules M, N is called a *homomorphism* (or *A-linear*) if $f(ax + y) = af(x) + f(y)$ holds for $a \in A$ and $x, y \in M$. The set of all homomorphisms is denoted by $\mathrm{Hom}_A(M, N)$. As usual, one defines mono-, epi-, endo-, iso- and automorphisms. Deviating from groups and algebras, we write $M \simeq N$ or more precisely $M \simeq_A N$ for the isomorphism of modules.

Remark 9.8.

(i) Let $f\colon M \to N$ be a homomorphism of A-modules. For $m \in M$ and $\lambda \in K$ it holds that

$$f(\lambda m) = f((\lambda 1_A)m) = (\lambda 1_A)f(m) = \lambda f(m),$$

i. e. f is K-linear.

(ii) For every homomorphism $f\colon M \to N$ of A-modules, $\operatorname{Ker}(f) \leq M$ and $f(M) \leq N$. The homomorphism theorem, the correspondence theorem, and the isomorphism theorems hold for modules just as they do for vector spaces.

(iii) If $f\colon M \to N$ is a bijective homomorphism, then $f^{-1}\colon N \to M$ is also a homomorphism, because

$$f^{-1}(am) = f^{-1}\big(af(f^{-1}(m))\big) = f^{-1}\big(f(af^{-1}(m))\big) = af^{-1}(m)$$

for $m \in M$ and $a \in A$.

(iv) If $f, g\colon M \to N$ are A-linear, then so are $f+g\colon M \to N$, $m \mapsto f(m)+g(m)$ and $\lambda f\colon M \to N$, $m \mapsto \lambda f(m)$ for $\lambda \in K$. This makes $\operatorname{Hom}_A(M,N)$ into a K-vector space (but usually not an A-module). In the case $M = N$, we also have $f \circ g \in \operatorname{Hom}_A(M,M) =: \operatorname{End}_A(M)$. 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 $f, g, h \in \operatorname{End}_A(M)$. In this way, $\operatorname{End}_A(M)$ becomes a K-algebra with identity element id_M. One calls $\operatorname{End}_A(M)$ the *endomorphism algebra* of M.

(v) Let M be an A-module. For $a \in A$, $f_a\colon M \to M$, $m \mapsto am$ is a homomorphism of vector spaces (but not of A-modules). Because of $f_{a+b} = f_a + f_b$ and $f_{ab} = f_a \circ f_b$ for $a, b \in A$, $f\colon A \to \operatorname{End}_K(M)$, $a \mapsto f_a$ is a homomorphism of algebras. One calls f a *representation* of A. By choosing a basis, one obtains a corresponding *matrix representation* $A \to K^{n\times n}$.

Lemma 9.9. *For simple A-modules $M \not\simeq N$, it holds that* $\operatorname{Hom}_A(M,N) = 0$ *and* $\operatorname{End}_A(M)$ *is a division algebra.*

Proof. For $f \in \operatorname{Hom}_A(M,N)$, $\operatorname{Ker}(f)$ and $f(M)$ are submodules of M and N, respectively. In the case $\operatorname{Ker}(f) = 0$, we would have $M \simeq f(M) = N$. Thus $\operatorname{Ker}(f) = M$ and $f = 0$. In the case $M = N$, either $f = 0$ or f is bijective. Therefore $\operatorname{End}_A(M)$ is a division algebra. □

Definition 9.10. Let M be an A-module. A sequence of submodules $0 = M_0 < M_1 < \ldots < M_n = M$ is called a *composition series* of M if the factors M_i/M_{i-1} are simple for $i = 1, \ldots, n$.

Theorem 9.11 (Jordan-Hölder)**.** *Every A-module possesses a composition series. If $0 = M_k < \ldots < M_0 = M$ and $0 = N_l < \ldots < N_0 = M$ are composition series of M, then $k = l$ and there exists a $\pi \in S_k$ with $M_{i-1}/M_i \cong N_{\pi(i)-1}/N_{\pi(i)}$ for $i = 1, \ldots, k$. One calls $M_0/M_1, \ldots, M_{k-1}/M_k$ the* composition factors *of M.*

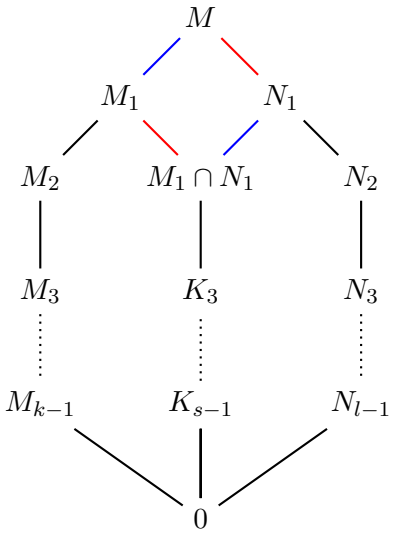
Proof. Induction on $\dim M$: In the case $M = 0$, the composition series consists only of M. Now let $M \neq 0$ and $L < M$ be a maximal submodule. By induction, L has a composition series $0 = L_0 < \ldots < L_n = L$. Obviously, $L_0 < \ldots < L_n < M$ is then a composition series of M.

Now for the uniqueness: In the case $M_1 = N_1$, the assertion follows by induction. So let $M_1 \neq N_1$. Since M/M_1 is simple, $M = M_1 + N_1$. The first isomorphism theorem shows

$$M/M_1 = (N_1 + M_1)/M_1 \simeq N_1/(N_1 \cap M_1), \qquad M/N_1 = (M_1 + N_1)/N_1 \simeq M_1/(M_1 \cap N_1). \tag{9.1}$$

Let $0 = K_s < \ldots < K_2 = M_1 \cap N_1$ be an arbitrary composition series. By induction, the composition series $M_k < \ldots < M_1$ and $K_s < \ldots < K_2 < M_1$ then have the same length (i. e. $k = s$) and their factors are isomorphic (up to the order). Now the composition series $0 = K_k < \ldots < K_2 < N_1$ and $0 = N_l < \ldots < N_1$ also have the same length with isomorphic factors. Thus $k = s = l$ and according to (9.1), the composition series

$$M_k < \ldots < M_0,$$
$$K_k < \ldots < K_2 < M_1 < M_0,$$
$$K_k < \ldots < K_2 < N_1 < N_0,$$
$$N_k < \ldots < N_0$$



have isomorphic factors. □

Corollary 9.12. *Every simple A-module is isomorphic to a composition factor of the regular A-module. In particular, there are at most* $\dim A$ *many simple A-modules up to isomorphism.*

Proof. Let M be a simple A-module and $m \in M \setminus \{0\}$. Then the map $\varphi\colon A \to M$, $a \mapsto am$ is an epimorphism. By the homomorphism theorem, $M \simeq A/\mathrm{Ker}(\varphi)$. One can now extend a composition series of $\mathrm{Ker}(\varphi)$ with M to a composition series of A. The second statement follows because every simple module is at least 1-dimensional. □

Definition 9.13. For an A-module M, one calls

$$\mathrm{Ann}(M) := \{a \in A : aM = 0\} \trianglelefteq A$$

the *annihilator* of M.

Remark 9.14. If $\varphi\colon M \to N$ is an isomorphism of A-modules, then

$$\mathrm{Ann}(N) = \{a \in A : a\varphi(M) = 0\} = \{a \in A : \varphi(aM) = 0\} = \{a \in A : aM = 0\} = \mathrm{Ann}(M).$$

Theorem 9.15. *If $M_1, \ldots, M_k$ are the simple A-modules up to isomorphism, then*

$$\mathrm{J}(A) = \mathrm{Ann}(M_1) \cap \ldots \cap \mathrm{Ann}(M_k).$$

Proof. For every A-module M and every ideal $I \trianglelefteq A$,

$$IM := \Big\{\sum_{i=1}^{n} x_i m_i : n \in \mathbb{N},\ x_1, \ldots, x_n \in I,\ m_1, \ldots, m_n \in M\Big\} \leq M.$$

In particular, $\mathrm{J}(A)M_i \leq M_i$. Let $\mathrm{J}(A)^s = 0$. In the case $\mathrm{J}(A)M_i = M_i$, it would follow that $0 = \mathrm{J}(A)^s M_i = \mathrm{J}(A)^{s-1} M_i = \ldots = M_i$. Thus $\mathrm{J}(A)M_i = 0$ for $i = 1, \ldots, k$, since M_i is simple. This shows $\mathrm{J}(A) \subseteq \mathrm{Ann}(M_1) \cap \ldots \cap \mathrm{Ann}(M_k) =: I$.

Let $0 = A_0 < \ldots < A_l = A$ be a composition series of the regular A-module. Since A/A_{l-1} is isomorphic to some M_i, we have $I(A/A_{l-1}) = 0$, i. e. $IA \subseteq A_{l-1}$ according to Remark 9.14. Analogously, $I^2 A \subseteq IA_{l-1} \subseteq A_{l-2}$ and finally $I^l = I^l A = 0$. Therefore I is nilpotent and $I \subseteq \mathrm{J}(A)$. □

10 Semisimple modules

Remark 10.1. As is well known, every finite-dimensional vector space is a direct sum of simple (i. e. 1-dimensional) subspaces. We investigate modules with the corresponding property. Again, let A always be a K-algebra.

Theorem 10.2. *For an A-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 submodule $V \leq M$ with $M = U \oplus V$.

If applicable, M is called semisimple.

Proof.

(1) $\Rightarrow$ (3): Let $M = M_1 + \ldots + M_k$ with simple submodules $M_1, \ldots, M_k \leq M$. Let $V \leq M$ with $U \cap V = 0$, such that $\dim V$ is as large as possible (if necessary $V = 0$). Assume $U \oplus V < M$. Then there exists $1 \leq i \leq k$ with $M_i \not\subseteq U+V$. From the simplicity of M_i, it follows that $M_i \cap (U+V) = 0$. Let $u = v + m \in U \cap (V + M_i)$ with $v \in V$ and $m \in M_i$. Then $u - v = m \in M_i \cap (U + V) = 0$ and $u = v \in U \cap V = 0$. This shows $U \cap (V + M_i) = 0$ in contradiction to the choice of V. Thus $M = U \oplus V$.

(3) $\Rightarrow$ (2): Let $U := U_1 \oplus \ldots \oplus U_k$ be a direct sum of simple submodules $U_1, \ldots, U_k \leq M$, such that $\dim U$ is as large as possible. Assume $U < M$. Then there exists $V \leq M$ with $M = U \oplus V$. For dimensional reasons, there exists a simple submodule $N \leq M$ with $N \leq V$. But then $U + N = U \oplus N$ in contradiction to the choice of U.

(2) $\Rightarrow$ (1): Trivial. □

Example 10.3.

(i) Every simple A-module is semisimple.

(ii) If $M = M_1 \oplus \ldots \oplus M_k$ is a decomposition into simple modules, then $0 < M_1 < M_1 \oplus M_2 < \ldots < M$ is a composition series of M. Therefore $M_1, \ldots, M_k$ are the composition factors of M.

(iii) If $M_1, \ldots, M_k$ are semisimple A-modules, then so is $M_1 \times \ldots \times M_k$.

(iv) Let $A = K^{2\times 2}$. Then the regular A-module is semisimple as a sum of the simple modules $\left\{\left(\begin{smallmatrix} * & 0 \\ * & 0 \end{smallmatrix}\right)\right\} \simeq K^2 \simeq \left\{\left(\begin{smallmatrix} 0 & * \\ 0 & * \end{smallmatrix}\right)\right\}$ (Example 9.6). Note: As an algebra A is simple, but as a module it is not.

(v) Let A be the algebra of upper triangular 2×2-matrices. Then K^2 is not semisimple, because the submodule $K\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ has no complement.

Lemma 10.4. *Submodules and factor modules of semisimple A-modules are semisimple.*

Proof. Let M be a semisimple A-module and $N \leq M$. For $L \leq N$ there exists an $L_1 \leq M$ with $M = L \oplus L_1$. Then $N = L + (L_1 \cap N)$ with $L \cap (L_1 \cap N) = (L \cap L_1) \cap N = 0$ by Dedekind. Therefore $L_1 \cap N$ is a complement of L in N and N is semisimple. For a simple submodule $S \leq M$, $(S+N)/N \simeq S/(S \cap N)$ is simple or trivial. Thus, with M, M/N is also a sum of simple submodules. Hence M/N is semisimple. □

Theorem 10.5. *For every algebra A the following statements are equivalent:*

(1) A is semisimple.

(2) The regular A-module is semisimple.

(3) Every A-module is semisimple.

Proof.

(1) ⇒ (2): Let $M_1, \ldots, M_n$ be the simple A-modules up to isomorphism. Let $x_1, \ldots, x_k \in M_i$ be a K-basis of M_i. Then $A \to M_i^k$, $a \mapsto a(x_1, \ldots, x_k)$ is a homomorphism with kernel $\mathrm{Ann}(M_i)$. As a submodule of M_i^k, $A/\mathrm{Ann}(M_i)$ is semisimple by Lemma 10.4. By Theorem 9.15 the map

$$A \to \bigtimes_{i=1}^{n} A/\mathrm{Ann}(M_i), \qquad a \mapsto (a + \mathrm{Ann}(M_i))_{1 \leq i \leq n}$$

is a monomorphism. Therefore the regular A-module is also semisimple.

(2) ⇒ (3): Let M be an A-module with K-basis $m_1, \ldots, m_k \in M$. Then $A^k \to M$, $(a_1, \ldots, a_k) \mapsto a_1 m_1 + \ldots + a_k m_k$ is an epimorphism. Since A^k is semisimple, M must also be semisimple by Lemma 10.4.

(3) ⇒ (1): Since the regular A-module is semisimple, there exist simple A-modules $M_1, \ldots, M_k$ with $A = M_1 \oplus \ldots \oplus M_k$. Let $1 = m_1 + \ldots + m_k$ with $m_i \in M_i$. For $x \in \mathrm{J}(A) \subseteq \mathrm{Ann}(M_1) \cap \ldots \cap \mathrm{Ann}(M_k)$ we have $x = x1 = xm_1 + \ldots + xm_k = 0$. Therefore $\mathrm{J}(A) = 0$ and A is semisimple. □

Lemma 10.6. *For A-modules M, M', N, N', the following hold:*

(i) $\boxed{\mathrm{End}_A(A) \cong A^o.}$

(ii) $\boxed{\mathrm{End}_A(M^n) \cong \mathrm{End}_A(M)^{n \times n}}$ *for $n \in \mathbb{N}$.*

(iii) $\mathrm{Hom}_A(M,N) = 0 = \mathrm{Hom}_A(N,M) \implies \mathrm{End}_A(M \times N) \cong \mathrm{End}_A(M) \times \mathrm{End}_A(N)$.

(iv) $\mathrm{Hom}_A(M, N \times N') \simeq_K \mathrm{Hom}_A(M,N) \times \mathrm{Hom}_A(M,N')$.

(v) $\mathrm{Hom}_A(M \times M', N) \simeq_K \mathrm{Hom}_A(M,N) \times \mathrm{Hom}_A(M',N)$.

Proof.

(i) Obviously, the map

$$\Phi \colon \mathrm{End}_A(A) \to A^o, \qquad f \mapsto f(1)$$

is K-linear. Because of $(f \circ g)(1) = f(g(1)) = f(g(1) \cdot 1) = g(1)f(1)$, Φ is a homomorphism of algebras. Because of $f(a) = f(a1) = af(1)$ for $a \in A$, f is already uniquely determined by $f(1)$. Therefore, Φ is injective. Conversely, let $a \in A$ be arbitrary. Then the map $f_a \colon A \to A$, $b \mapsto ba$ is a homomorphism with $f_a(1) = a$. This shows the surjectivity of Φ.

(ii) For $i = 1, \dots, n$, the maps

$$\begin{aligned} \pi_i \colon M^n &\to M, & (m_1, \dots, m_n) &\mapsto m_i, \\ \rho_i \colon M &\to M^n, & m &\mapsto (0, \dots, 0, \underset{i}{m}, 0, \dots, 0) \end{aligned}$$

are A-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 $\Phi \colon \mathrm{End}_A(M^n) \to \mathrm{End}_A(M)^{n \times n}$, $f \mapsto (\pi_i f \rho_j)_{i,j=1}^n$. Then $\Phi(\mathrm{id}) = (\pi_i \rho_j)_{i,j} = 1_n$ and $\Phi(f + g) = \Phi(f) + \Phi(g)$ for $f, g \in \mathrm{End}_A(M^n)$. 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 homomorphism of algebras. 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 $(f_{ij})_{i,j} \in \mathrm{End}_A(M)^{n \times n}$ be given. Then $f := \sum_{i,j=1}^{n} \rho_i f_{ij} \pi_j \in \mathrm{End}_A(M^n)$ 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) Similarly to (ii), let $\Phi \colon \mathrm{End}_A(M \times N) \to \mathrm{End}_A(M) \times \mathrm{End}_A(N)$, $f \mapsto (\pi_1 f \rho_1, \pi_2 f \rho_2)$. It is easily shown that Φ is a homomorphism of algebras. Let $\Phi(f) = 0$. Because of

$$\pi_1 f \rho_2 \in \mathrm{Hom}_A(N, M) = 0 \qquad \pi_2 f \rho_1 \in \mathrm{Hom}_A(M, N) = 0$$

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 $(f_1, f_2) \in \mathrm{End}_A(M) \times \mathrm{End}_A(N)$, let $f \colon = \rho_1 f_1 \pi_1 + \rho_2 f_2 \pi_2 \in \mathrm{End}_A(M \times N)$. 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 surjective.

(iv) It is easily shown that the maps

$$\begin{aligned} \mathrm{Hom}_A(M, N \times N') &\to \mathrm{Hom}_A(M, N) \times \mathrm{Hom}_A(M, N'), & f &\mapsto (\pi_1 f, \pi_2 f), \\ \mathrm{Hom}_A(M, N) \times \mathrm{Hom}_A(M, N') &\to \mathrm{Hom}_A(M, N \times N'), & (g_1, g_2) &\mapsto \rho_1 g_1 + \rho_2 g_2 \end{aligned}$$

are mutually inverse isomorphisms of K-vector spaces.

(v) Analogous. □

Theorem 10.7 (Artin-Wedderburn)**.** *An algebra A is semisimple if and only if there exist division algebras $D_1, \ldots, D_k$ and $n_1, \ldots, n_k \in \mathbb{N}$ with*

$$\boxed{A \cong D_1^{n_1 \times n_1} \times \ldots \times D_k^{n_k \times n_k}}.$$

If applicable, $n_1, \ldots, n_k$ are the multiplicities and $\dim(D_1)n_1, \ldots, \dim(D_k)n_k$ are the dimensions of the simple modules as composition factors of the regular A-module.

Proof. Let A be semisimple. According to Theorem 10.5, $A \simeq M_1^{n_1} \oplus \ldots \oplus M_k^{n_k}$ holds with pairwise non-isomorphic simple A-modules $M_1, \ldots, M_k$. According to Lemma 9.9, $\mathrm{Hom}_A(M_i, M_j) = 0$ for $i \neq j$ and $D_i := \mathrm{End}_A(M_i)^o$ is a division algebra for $i = 1, \ldots, k$. From Lemma 10.6 it follows that $\mathrm{Hom}_A(M_i^{n_i}, M_j^{n_j}) \simeq_K \mathrm{Hom}_A(M_i, M_j)^{n_i n_j} = 0$ and

$$\begin{aligned} A &\cong \mathrm{End}_A(A)^o \cong \mathrm{End}_A(M_1^{n_1} \times \ldots \times M_k^{n_k})^o \cong (\mathrm{End}_A(M_1^{n_1}) \times \ldots \times \mathrm{End}_A(M_k^{n_k}))^o \\ &\cong (\mathrm{End}_A(M_1)^{n_1 \times n_1} \times \ldots \times \mathrm{End}_A(M_k)^{n_k \times n_k})^o \\ &\overset{8.3}{\cong} (\mathrm{End}_A(M_1)^{n_1 \times n_1})^o \times \ldots \times (\mathrm{End}_A(M_k)^{n_k \times n_k})^o \overset{8.3}{\cong} D_1^{n_1 \times n_1} \times \ldots \times D_k^{n_k \times n_k}. \end{aligned}$$

Conversely, let $A \cong D_1^{n_1 \times n_1} \times \ldots \times D_k^{n_k \times n_k}$. According to Lemma 8.12,

$$\mathrm{J}(A) \cong \mathrm{J}(D_1)^{n_1 \times n_1} \times \ldots \times \mathrm{J}(D_k)^{n_k \times n_k} = 0,$$

i. e. A is semisimple. As in Example 9.6, one shows that $D_i^{n_i}$ is a simple $D_i^{n_i \times n_i}$-module. Then certainly

$$M_{i,j} := 0 \times \ldots \times 0 \times \begin{pmatrix} 0 & *_j & 0 \\ \vdots & \vdots & \vdots \\ 0 & *_j & 0 \end{pmatrix} \times 0 \times \ldots \times 0$$

is a simple submodule of the regular A-module with dimension $\dim(D_i)n_i$. Furthermore, A is the direct sum of these modules, where $M_{i,1} \simeq \ldots \simeq M_{i,n_i}$. For $i \neq j$, $M_{i,1} \not\simeq M_{j,1}$ holds because the annihilators are different (Remark 9.14). Thus $M_{i,1}$ occurs with multiplicity n_i in the regular A-module. □

Remark 10.8. Because of $D_1^{n_1 \times n_1} \trianglelefteq D_1^{n_1 \times n_1} \times \ldots \times D_k^{n_k \times n_k}$, it holds: A is simple if and only if there exists a division algebra D and $n \in \mathbb{N}$ with $A \cong D^{n \times n}$. This special case was proven by Wedderburn.

11 Indecomposable Modules

Remark 11.1. Furthermore, let A be a K-algebra. If an A-module M is not semisimple, one can still decompose M into smallest possible submodules $M = M_1 \oplus \ldots \oplus M_k$. We investigate the properties of such a decomposition.

Definition 11.2. Let $M \neq 0$ be an A-module. M is called *decomposable* if there exist submodules $M_1, M_2 < M$ with $M = M_1 \oplus M_2$. Otherwise, M is called *indecomposable*.

Example 11.3.

(i) Every simple module is indecomposable.

(ii) The 2-dimensional module K^2 of $A = \left\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\right\}$ from Example 10.3 is indecomposable, since otherwise it would be semisimple.

Theorem 11.4. *For every algebra A, the following statements are equivalent:*

(1) A is local.

(2) Every element in A is invertible or nilpotent.

(3) 0 and 1 are the only idempotents of A.

Proof.

(1) $\Rightarrow$ (2): Every element in $\mathrm{J}(A)$ is nilpotent. Let $a \in A \setminus \mathrm{J}(A)$. Since $A/\mathrm{J}(A)$ is a division algebra, $a + \mathrm{J}(A) \in (A/\mathrm{J}(A))^\times$. By Lemma 8.15, $a \in A^\times$ holds.

(2) $\Rightarrow$ (3): Let $e = e^2 \in A$. In the case $e \in A^\times$, $e = eee^{-1} = ee^{-1} = 1$. Otherwise, $e^n = 0$ for some $n \in \mathbb{N}$. Then it follows that $e = e^2 = \ldots = e^n = 0$.

(3) $\Rightarrow$ (1): By Lemma 8.15, the semisimple algebra $A/\mathrm{J}(A)$ possesses only the idempotents 0 and 1. However, every component $D^{n\times n}$ in the Artin-Wedderburn decomposition of $A/\mathrm{J}(A)$ yields (at least) n idempotents $E_{11}, \ldots, E_{nn}$ according to Example 8.14. Therefore, $A/\mathrm{J}(A)$ itself must be a division algebra. □

Lemma 11.5 (Fitting)**.** *Let M be an A-module and $f \in \mathrm{End}_A(M)$. Then there exists a $k \in \mathbb{N}$ with $M = \mathrm{Ker}(f^k) \oplus f^k(M)$.*

Proof. For dimension reasons, the sequences $\mathrm{Ker}(f) \subseteq \mathrm{Ker}(f^2) \subseteq \ldots$ and $f(M) \supseteq f^2(M) \supseteq \ldots$ become constant. 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. The assertion follows from

$$\dim_K(\mathrm{Ker}(f^k) \oplus f^k(M)) = \dim \mathrm{Ker}(f^k) + \dim f^k(M) = \dim \mathrm{Ker}(f^k) + \dim(M/\mathrm{Ker}(f^k)) = \dim M. \quad \square$$

Theorem 11.6. *An A-module $M \neq 0$ is indecomposable if and only if $\mathrm{End}_A(M)$ is local.*

Proof. Let M be indecomposable. Suppose $E := \mathrm{End}_A(M)$ possesses an idempotent $e \notin \{0, 1\}$. By Fitting, $M = e(M) \oplus \mathrm{Ker}(e)$ holds. Because $e \neq 0$, $\mathrm{Ker}(e) < M$. Since M is indecomposable, it follows that $e(M) = M$, i. e. e is invertible. But then $e = 1$. Thus E is local by Theorem 11.4.

Conversely, let E be local and $M = M_1 \oplus M_2$. Let $\pi_1 \colon M \to M$, $m_1 + m_2 \mapsto m_1$ be the projection onto M_1. Obviously $\pi_1 \in E$ is an idempotent and $\pi_1 \in \{0, \mathrm{id}_M\}$ follows from Theorem 11.4. This shows $M_2 = M$ or $M_1 = M$, i. e. M is indecomposable. □

Corollary 11.7. *An algebra A is local if and only if the regular A-module is indecomposable.*

Proof. Follows from $\mathrm{End}_A(A) \cong A^o$ (Lemma 10.6). □

Theorem 11.8 (Krull-Schmidt)**.** *Every A-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. The existence follows easily by induction on $\dim M$. 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

$$\mathrm{id}_{N_1} = \rho_{|N_1} = \rho \circ (\pi_1 + \ldots + \pi_k)_{|N_1} = (\rho \circ \pi_1)_{|N_1} + \ldots + (\rho \circ \pi_k)_{|N_1}.$$

Not all summands on the right side can lie in $\mathrm{J}(\mathrm{End}_A(N_1))$. According to Theorem 11.6 and Theorem 11.4, at least one summand, say $\tau := (\rho \circ \pi_1)_{|N_1}$, is invertible. In particular, $(\pi_1)_{|N_1}$ is injective and $\rho_{|M_1}$ is surjective. For $\sigma := \pi_1 \circ \tau^{-1} \circ \rho_{|M_1} \in \mathrm{End}_A(M_1)$, it clearly holds that

$$\sigma^2 = \pi_1 \circ \tau^{-1} \circ \rho \circ \pi_1 \circ \tau^{-1} \circ \rho_{|M_1} = \sigma \neq 0.$$

From Theorem 11.6 and Theorem 11.4 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 11.9. For a K-algebra A, let

$$\gamma(A) := K\{ab - ba : a, b \in A\}$$

be the *commutator space* of A.

Remark 11.10. Attention: $\gamma(A)$ is neither an ideal nor a subring of A.

Lemma 11.11. *For K-algebras A, B, the following holds:*

(i) $\gamma(A \times B) = \gamma(A) \times \gamma(B)$.

(ii) For $I \trianglelefteq A$, $\gamma(A/I) = (\gamma(A) + I)/I$ holds.

(iii) For $n \in \mathbb{N}$, $\gamma(K^{n\times n}) = \{M \in K^{n\times n} : \mathrm{tr}\, M = 0\}$ holds. In particular, $\dim_K(K^{n\times n}/\gamma(K^{n\times n})) = 1$.

Proof.

(i) Certainly $\gamma(A) \times \gamma(B) = (\gamma(A) \times 0) + (0 \times \gamma(B)) \subseteq \gamma(A \times B)$ holds. 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 $a, b \in K^{n\times n}$ we have $\mathrm{tr}(ab - ba) = \mathrm{tr}(ab) - \mathrm{tr}(ba) \overset{(2.1)}{=} 0$, 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

$$E_{st} = E_{s1}E_{1t} - E_{1t}E_{s1} \in \gamma(K^{n\times n}),$$
$$E_{ss} - E_{tt} = E_{st}E_{ts} - E_{ts}E_{st} \in \gamma(K^{n\times n}).$$

Apparently 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 homomorphism theorem for tr. □

Lemma 11.12. *Let A be a K-algebra and $p := \operatorname{char} K > 0$. 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) $\mathrm{J}(A) + \gamma(A) = \left\{a \in A : \exists n \in \mathbb{N}_0 : a^{p^n} \in \gamma(A)\right\}$, *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 $c_1, \dots, c_p \in \{a, b\}$.[10] 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

$$a^p \equiv (bc)^p + (-cb)^p \equiv (bc)^p - (cb)^p \equiv b(c \dots bc) - (cb \dots c)b \equiv 0 \pmod{\gamma(A)}.$$

(iii) Let $a \equiv b \pmod{\gamma(A)}$. According to (i) and (ii), it holds that $a^p - b^p \equiv (a-b)^p \equiv 0 \pmod{\gamma(A)}$. For arbitrary $a, b \in A$, it is therefore $(a+b)^{p^2} \equiv (a^p + b^p)^p \equiv a^{p^2} + b^{p^2} \pmod{\gamma(A)}$ and inductively $(a+b)^{p^n} \equiv a^{p^n} + b^{p^n} \pmod{\gamma(A)}$ for $n \in \mathbb{N}$. This shows that

$$T := \{a \in A : \exists n \in \mathbb{N}_0 : a^{p^n} \in \gamma(A)\}$$

is a vector space with $\gamma(A) \subseteq T$. Since $\mathrm{J}(A)$ is nilpotent, $\mathrm{J}(A) \subseteq T$ holds, thus $\mathrm{J}(A) + \gamma(A) \subseteq T$. According to Artin-Wedderburn and Lemma 8.4, $A/\mathrm{J}(A) \cong K^{n_1 \times n_1} \times \dots \times K^{n_k \times n_k}$. Together with Lemma 11.11, it follows that

$$(\gamma(A) + \mathrm{J}(A))/\mathrm{J}(A) = \gamma(A/\mathrm{J}(A)) \cong \gamma(K^{n_1 \times n_1}) \times \dots \times \gamma(K^{n_k \times n_k}) \tag{11.1}$$

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 $T = \gamma(A) + \mathrm{J}(A)$. □

Corollary 11.13. *Let K be algebraically closed with characteristic $p > 0$. Then*

$$\dim A/(\gamma(A) + \mathrm{J}(A)) = \dim \mathrm{Z}(A/\mathrm{J}(A))$$

is the number of simple A-modules up to isomorphism.

Proof. According to Exercise 22, every simple A-module is also a simple $A/\mathrm{J}(A)$-module. According to Artin-Wedderburn and (11.1), $\dim A/(\gamma(A) + \mathrm{J}(A))$ is the number of simple A-modules. The second equation follows from Lemma 8.12. □

[10] Since a and b are not necessarily commutable, one must not use the binomial formula.

12 Group Algebras

Remark 12.1. In Chapter 2, we have seen that $\mathbb{C}$-representations of a group G are essentially determined by their character. Over fields with characteristic $p > 0$, this is in general false, because the character of a representation of the form $\Delta \oplus \ldots \oplus \Delta$ with p summands is the zero map. In this chapter, we introduce an algebra that contains all representation-theoretic information of G.

Definition 12.2. Let KG be the set of all mappings $G \to K$. By

$$\begin{aligned}(\alpha + \beta)(g) &:= \alpha(g) + \beta(g) \qquad (\alpha, \beta \in KG,\ g \in G),\\ (\alpha\beta)(g) &:= \sum_{h \in G} \alpha(h)\beta(h^{-1}g) \qquad (\textit{convolution}),\\ (\lambda\alpha)(g) &:= \lambda\alpha(g) \qquad (\lambda \in K)\end{aligned}$$

KG becomes a K-algebra. The associativity of the 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 like with polynomials:

$$\sum_{g \in G} \alpha_g g \cdot \sum_{g \in G} \beta_g g = \sum_{g,h \in G} \alpha_g \beta_h gh = \sum_{g \in G} \Big(\sum_{h \in G} \alpha_h \beta_{h^{-1}g} \Big) g.$$

By identifying $g \in G$ with $1_K g$, we can regard 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.

Example 12.3. For $x := (1,2) + (1,3) \in \mathbb{F}_2 S_3$ we have

$$x^2 = (1,2)^2 + (1,2)(1,3) + (1,3)(1,2) + (1,3)^2 = 1 + (1,3,2) + (1,2,3) + 1 = (1,3,2) + (1,2,3).$$

Remark 12.4.

(i) Every representation $\Delta\colon G \to \mathrm{GL}(V)$ of G can be linearly extended to a representation

$$\hat{\Delta}\colon KG \to \mathrm{End}_K(V), \qquad \sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g \Delta(g)$$

of KG. In this way, V becomes a KG-module (Remark 9.8). Conversely, from a KG-module $V \neq 0$, one obtains a representation of G by restriction.

(ii) Representations $\Delta\colon G \to \mathrm{GL}(V)$ and $\Gamma\colon G \to \mathrm{GL}(W)$ are similar if and only if there exists a vector space isomorphism $f\colon V \to W$ with $f \circ \Delta(g) = \Gamma(g) \circ f$ for all $g \in G$. For $v \in V$, this means $f(gv) = gf(v)$, i.e., f is an isomorphism of KG-modules. Therefore, the similarity classes of representations of G and the isomorphism classes of KG-modules correspond to each other. Note: The trivial representation $\mathbb{1}_G$ corresponds to the 1-dimensional module K. In contrast to

arbitrary algebras, we will refer to K in this context as the *trivial module*. The existence of this module distinguishes group algebras from arbitrary algebras. For example, $K^{2\times 2}$ is not isomorphic to any group algebra.

(iii) Let Δ be a representation corresponding to the KG-module V. The Δ-invariant subspaces are then precisely the submodules of V. Therefore, Δ is irreducible if and only if V is simple.

Theorem 12.5 (Maschke)**.** *KG is semisimple if and only if* $\operatorname{char} K$ *does not divide* $|G|$.

Proof. Let $\operatorname{char} K \nmid |G|$. According to Theorem 1.9, every KG-module is semisimple. According to Theorem 10.5, the algebra KG is also semisimple. If $|G|$ is divisible by $\operatorname{char} K$, then KG is not semisimple according to Exercise 1. □

Example 12.6.

(i) Let $\operatorname{char} K \nmid |G|$. Artin-Wedderburn yields division algebras $D_1, \ldots, D_k$ and $n_1, \ldots, n_k \in \mathbb{N}$ with $KG \cong D_1^{n_1\times n_1} \times \ldots \times D_k^{n_k\times n_k}$. Because of the trivial module, one can assume $D_1^{n_1\times n_1} = K$. Furthermore,

$$|G| = \dim_K KG = \sum_{i=1}^{k} \dim(D_i^{n_i\times n_i}) = \sum_{i=1}^{k} \dim(D_i) n_i^2.$$

If K is algebraically closed, then $D_i \cong K$ for $i = 1, \ldots, k$ according to Lemma 8.4. One then obtains $|G| = n_1^2 + \ldots + n_k^2$ as in Remark 2.15. If G is abelian, then $D_1, \ldots, D_k$ are fields and $n_1 = \ldots = n_k = 1$.

(ii) If G is abelian of order n, then $\mathbb{C}G \cong \mathbb{C}^n$ according to Remark 12.4. The isomorphism type of G can therefore not be determined from $\mathbb{C}G$.

(iii) According to Example 7.4, C_3 has an irreducible $\mathbb{R}$-representation of degree 2. Since C_3 is abelian, it follows easily that $\mathbb{R}C_3 \cong \mathbb{R} \times \mathbb{C}$. Since the $\mathbb{Q}$-representations of D_6 and D_8 are absolutely irreducible, we have $\mathbb{Q}S_3 \cong \mathbb{Q}D_6 \cong \mathbb{Q}^{2\times 2} \times \mathbb{Q}^2$ and $\mathbb{Q}D_8 \cong \mathbb{Q}^{2\times 2} \times \mathbb{Q}^4$. Without proof, it should be mentioned: $\mathbb{R}Q_8 \cong \mathbb{R}^4 \times \mathbb{H}$.

(iv) For $G = \langle g \rangle \cong C_n$, $\mathbb{Q}[X] \to \mathbb{Q}G$, $X \mapsto g$ is an epimorphism of algebras with kernel $(X^n - 1)$. As is well known, $X^n - 1 = \prod_{d|n} \Phi_d$, where Φ_d are the (irreducible) cyclotomic polynomials. Since the Φ_d are pairwise coprime,

$$\mathbb{Q}[X]/(X^n - 1) \to \prod_{d\,|\,n} \mathbb{Q}[X]/(\Phi_d), \qquad \alpha + (X^n - 1) \mapsto (\alpha + (\Phi_d))_d$$

is an isomorphism (Chinese Remainder Theorem for rings). Finally, $\mathbb{Q}[X]/(\Phi_d) \cong \mathbb{Q}_d$ is the d-th cyclotomic field. Overall, one obtains the Artin-Wedderburn decomposition

$$\mathbb{Q}G \cong \prod_{d\,|\,n} \mathbb{Q}_d.$$

The number of simple $\mathbb{Q}G$-modules is therefore the number of divisors of n.

Theorem 12.7 (Burnside)**.** *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.

(1) ⇒ (2): By Schur's Lemma, it holds that

$$\mathrm{C}_{K^{n\times n}}(\Delta(G)) = K^{n\times n} \cap \mathrm{C}_{\mathbb{C}^{n\times n}}(\Delta(G)) = K^{n\times n} \cap \mathbb{C}1_n = K1_n.$$

(2) ⇒ (1): If Δ is reducible as a $\mathbb{C}$-representation, then there exists a $\mathbb{C}$-basis with $\Delta(g) = \left(\begin{smallmatrix} \Delta_1(g) & 0 \\ 0 & \Delta_2(g) \end{smallmatrix}\right)$ for $g \in G$ and $\mathbb{C}$-representations Δ_1, Δ_2. Then, however, $\left(\begin{smallmatrix} \Delta_1(1) & 0 \\ 0 & 0 \end{smallmatrix}\right) \in \mathrm{C}_{K^{n\times n}}(\Delta(G)) \setminus K1_n$ (note that (2) does not depend on the choice of basis).

(1) ⇒ (3): If matrices are linearly independent over $\mathbb{C}$, then they are all the more so over K. Therefore, it holds that

$$\dim_{\mathbb{C}} \Delta(\mathbb{C}G) = \dim \mathrm{Span}_{\mathbb{C}} \Delta(G) \leq \dim \mathrm{Span}_K \Delta(G) = \dim_K \Delta(KG).$$

Thus, we can assume $K = \mathbb{C}$. Let $V := \mathbb{C}^n$ be the $\mathbb{C}G$-module belonging to Δ. Then $\mathrm{Ann}(V)$ is the kernel of $\Delta\colon \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(V) \cong \mathbb{C}^{n\times n}$. In particular, $\dim \mathbb{C}G/\mathrm{Ann}(V) \leq n^2$. Let $V = V_1, \ldots, V_k$ be the simple $\mathbb{C}G$-modules up to isomorphism. According to Theorem 9.15, $\mathbb{C}G \to \bigtimes_{i=1}^k \mathbb{C}G/\mathrm{Ann}(V_i)$ is a monomorphism. Because of

$$|G| = \dim \mathbb{C}G \leq \sum_{i=1}^{n} \dim \mathbb{C}G/\mathrm{Ann}(V_i) \leq \sum_{i=1}^{k} \dim(V_i)^2 \overset{2.15}{=} |G|$$

Δ must be surjective.

(3) ⇒ (1): Suppose 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). □

Definition 12.8. For a conjugacy class C of G, let $C^+ := \sum_{g\in C} g \in KG$ be the *class sum* of C.

Theorem 12.9. *The class sums form a K-basis of* $\mathrm{Z}(KG)$. *In particular,* $\boxed{\dim_K \mathrm{Z}(KG) = k(G).}$

Proof. For $g \in G$ and $C \in \mathrm{Cl}(G)$ 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 conjugacy classes are disjoint, the class sums are linearly independent. □

Remark 12.10.

(i) According to Theorem 12.9, $\mathrm{Z}(KG)$ consists exactly of the class functions $G \to K$.

(ii) For $C, D \in \mathrm{Cl}(G)$ we have

$$C^+D^+ = \sum_{c\in C}\sum_{d\in D} cd = \sum_{E\in\mathrm{Cl}(G)}\sum_{e\in E} |\{(c,d)\in C\times D : cd = e\}|e = \sum_{E\in\mathrm{Cl}(G)} \gamma_{CDE}E^+$$

with the class multiplication constants defined in Remark 2.15.

(iii) Let $\mathrm{char}\, K \nmid |G|$ and $KG \cong D_1^{n_1\times n_1} \times \ldots \times D_k^{n_k\times n_k}$ be the Artin-Wedderburn decomposition. From Lemma 8.12 it follows that

$$k(G) = \dim \mathrm{Z}(KG) = \dim \mathrm{Z}(D_1) + \ldots + \dim \mathrm{Z}(D_k).$$

If K is algebraically closed, one obtains $k(G) = k$ as in the case $K = \mathbb{C}$ (Theorem 2.18). In the following, we determine k if $\mathrm{char}\, K \mid |G|$.

Definition 12.11. Let p be a prime number. An element $x \in G$ is called a *p-element* or *p'-element*, if $|\langle x\rangle|$ is a p-power or is not divisible by p, respectively. Let G_p or $G_{p'}$ be the set of p-elements or p'-elements of G, respectively. Then $G_p \cap G_{p'} = \{1\}$ holds, but $G \neq G_p \cup G_{p'}$ in general. A class $C \in \mathrm{Cl}(G)$ is called a *p-conjugacy class* or *p'-conjugacy class*, if $C \subseteq G_p$ or $C \subseteq G_{p'}$ (note: conjugate elements have the same order).

Lemma 12.12. *Every element $x \in G$ can be uniquely written in the form $x = x_px_{p'} = x_{p'}x_p$ 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 $|\langle x\rangle| = p^am$ 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 $x_{p'} := x^{\alpha p^a} \in G_{p'}$ we have $x = x^{\alpha p^a+\beta m} = x_px_{p'} = x_{p'}x_p$.

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 $y^{-1}x_p = zx_{p'}^{-1} \in G_p \cap G_{p'} = \{1\}$, i. e. $y = x_p$ and $z = x_{p'}$. □

Remark 12.13. For $x, g \in G$ we have $(gxg^{-1})_p = gx_pg^{-1}$ and $(gxg^{-1})_{p'} = gx_{p'}g^{-1}$.

Definition 12.14. For $x \in G$ let

$$\mathrm{Sec}_{p'}(x) := \big\{y \in G : \mathrm{Cl}(y_{p'}) = \mathrm{Cl}(x_{p'})\big\} \subseteq G$$

be the *p'-section* of x. According to Remark 12.13, $\mathrm{Sec}_{p'}(x)$ is a union of conjugacy classes of G.

Example 12.15. For $x \in G_p$ we have $\mathrm{Sec}_{p'}(x) = G_p$. For $g := (1,2) \in S_3$ we have $\mathrm{Sec}_{3'}(g) = \mathrm{Cl}(g) = \{g, (1,3), (2,3)\}$.

Lemma 12.16. *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) $$\gamma(KG) + \mathrm{J}(KG) = \Big\{\sum_{g\in G}\alpha_g g : \forall x \in G_{p'} : \sum_{s\in\mathrm{Sec}_{p'}(x)}\alpha_s = 0\Big\}.$$

Proof.

(i) Let Γ be the right-hand side of the equation. For $g, h \in G$, we have $gh - hg = gh - g^{-1}(gh)g \in \Gamma$. For $\alpha = \sum_{g\in G} \alpha_g g$ and $\beta = \sum_{h\in G} \beta_h h$, it follows that

$$\alpha\beta - \beta\alpha = \sum_{g,h\in G} \alpha_g\beta_h(gh - hg) \in \Gamma.$$

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 $c = gx_Cg^{-1}$. Then $c - x_C = (gx_C)g^{-1} - g^{-1}(gx_C) \in \gamma(KG)$ and

$$\sum_{g\in G} \alpha_g g = \sum_{C\in \mathrm{Cl}(G)} \Big(\sum_{c\in C} \alpha_c c - x_C \underbrace{\sum_{c\in C} \alpha_c}_{=0}\Big) = \sum_{C\in \mathrm{Cl}(G)} \sum_{c\in C} \alpha_c(c - x_C) \in \gamma(KG).$$

(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 $g \in \mathrm{Sec}_{p'}(x_i)$, we have $g_{p'} \equiv x_i \pmod{\gamma(KG)}$ by (i). From Lemma 11.12 it follows that

$$\alpha^{p^k} \equiv \sum_{g\in G} \alpha_g^{p^k} g_{p'} \equiv \sum_{i=1}^{l} x_i \sum_{s\in \mathrm{Sec}_{p'}(x_i)} \alpha_s^{p^k} \equiv \sum_{i=1}^{l} x_i \Big(\sum_{s\in \mathrm{Sec}_{p'}(x_i)} \alpha_s\Big)^{p^k} \pmod{\gamma(KG)}. \tag{12.1}$$

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 Lemma 11.12. Conversely, if $\alpha^{p^n} \in \gamma(KG)$ for some $n \in \mathbb{N}$, then there exists a $k \geq \max\{a, n\}$ with $p^k \equiv 1 \pmod m$. Then $\sum_{s\in \mathrm{Sec}_{p'}(x_i)} \alpha_s = 0$ follows from (12.1) for $i = 1, \ldots, l$. □

Theorem 12.17 (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. Obviously, the number l of p'-conjugacy classes coincides with the number of p'-sections. Lemma 12.16 describes $\gamma(KG) + \mathrm{J}(KG)$ as the solution of a system of linear equations with l linearly independent rows. Therefore, $\dim KG/(\gamma(KG) + \mathrm{J}(KG)) = l$ and the assertion follows from Corollary 11.13. □

Example 12.18. The algebraic closure $K := \overline{\mathbb{F}_p}$ of $\mathbb{F}_p$ has characteristic $p > 0$.

(i) Let G be abelian and $|G| = p^a m$ with $p \nmid m$. Then $G = G_p \times G_{p'}$ and $m = |G_{p'}|$ is the number of simple KG-modules. One obtains these modules as inflations of $G_{p'} \cong G/G_p$. This holds more generally if G_p is the unique p-Sylow subgroup of G (Example 12.22).

(ii) The trivial module is the only simple KG-module if and only if $\{1\}$ is the only p'-conjugacy class of G. This holds if and only if G is a p-group. This statement remains true if K is not algebraically closed (see proof of Theorem 12.21).

(iii) For $p \in \{2,3\}$, KS_3 has exactly two simple modules in each case. The non-trivial module for $p = 3$ is the *alternating* module K with $\sigma \cdot 1_K = \operatorname{sgn}(\sigma)1_K$ for $\sigma \in S_3$ (inflation of $C_2 \cong S_3/A_3$). In particular, both simple modules are 1-dimensional here, although S_3 is not abelian (cf. Theorem 2.2). For $p = 2$,

$$V := \{x \in K^3 : x_1 + x_2 + x_3 = 0\} \leq K^3$$

is the non-trivial simple module (with $\dim V = 2$), where S_3 permutes the coordinates.

Remark 12.19.

(i) The determination of 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 $\overline{\mathbb{F}_2}S_{20}$-modules. These dimensions also do not divide the group order in general. For example, there are simple $\overline{\mathbb{F}_3}S_7$-modules of dimension 13.

(ii) In the situation of Theorem 12.17, one can assign to each KG-module a so-called *Brauer character* $\varphi\colon G_{p'} \to \mathbb{C}$. The set of irreducible Brauer characters then forms a basis for the space of all class functions on $G_{p'}$.

(iii) The number of simple $\mathbb{Q}G$-modules is the number of conjugacy classes of cyclic subgroups of G (without proof).

(iv) Let r be the number of conjugacy classes of the form $C = C^{-1}$ and $2s$ the number of conjugacy classes $C \neq C^{-1}$ of G. Then $r + s$ is the number of simple $\mathbb{R}G$-modules (without proof). If $|G|$ is odd, then $r = 1$ and there are exactly $(k(G) + 1)/2$ simple $\mathbb{R}G$-modules.

(v) According to Corollary 9.12, KG has only finitely many simple modules up to isomorphism for every field K. We will see that the situation for indecomposable modules is different.

Lemma 12.20. *Let G be a non-cyclic p-group. Then there exists $N \trianglelefteq G$ with $G/N \cong C_p \times C_p$.*

Proof. Induction on $|G|$. Since G is not cyclic, $|G| \geq p^2$ holds. In the case $|G| = p^2$, G is abelian according to Example 4.8 and the claim holds with $N := 1$. Let $|G| > p^2$ and $Z := \mathrm{Z}(G) \neq 1$ (Algebra 1). If G/Z is not cyclic, then by induction there exists a normal subgroup $N/Z \trianglelefteq G/Z$ with

$$G/N \cong (G/Z)/(N/Z) \cong C_p \times C_p.$$

Now let G/Z be cyclic, say $G/Z = \langle gZ \rangle$. Then every element of G has the form $g^i z$ with $i \in \mathbb{Z}$ and $z \in Z$. This implies that G is abelian. Let $x \in G$ be of order p. By induction we can assume that $G/\langle x \rangle$ is cyclic, say $G = \langle x, y \rangle$. For $N := \langle y^p \rangle \trianglelefteq G$, it now holds that $G/N \cong C_p \times C_p$. □

Theorem 12.21. *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 modules up to isomorphism. These have 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) First, assume that G is not a p-group. By Cauchy (or Sylow), 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. By Theorem 11.4, 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 p-power. 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 $M = Ka \simeq K$. By Theorem 9.15, $KG/\mathrm{J}(KG) = KG/\mathrm{Ann}(M) \cong \mathrm{End}_K(M) \cong K$. Therefore, 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 $J_k(1)$.[11] Since V is indecomposable, it follows that $W = 0$ 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 turn the vector space $V := K^k$ into a KG-module via $gv := J_k(1)v$ for $v \in V$. Due to the uniqueness of the Jordan normal form, V is indecomposable.

(iii) By Lemma 12.20, there exists $N \trianglelefteq G$ with $G/N \cong C_p \times C_p$. 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 $u \in U$ (inflation). We can therefore assume $G = \langle g, h\rangle \cong C_p \times C_p$.

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 $\alpha, \beta \in \mathrm{End}_K(V_{2d})$ 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 $J = J_d(0) \in K^{d\times d}$ be the Jordan block for the eigenvalue 0 with ones below the main diagonal. Because $f(gv) = gf(v)$ for $v \in V_{2d}$, f commutes with α and β, i. e.

$$\begin{pmatrix} 0 & 0 \\ A & B\end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1_d & 0\end{pmatrix}\begin{pmatrix} A & B \\ C & D\end{pmatrix} = \alpha M = M\alpha = \begin{pmatrix} A & B \\ C & D\end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1_d & 0\end{pmatrix} = \begin{pmatrix} B & 0 \\ D & 0\end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 \\ JA & JB\end{pmatrix} = \begin{pmatrix} 0 & 0 \\ J & 0\end{pmatrix}\begin{pmatrix} A & B \\ C & D\end{pmatrix} = \beta M = M\beta = \begin{pmatrix} A & B \\ C & D\end{pmatrix}\begin{pmatrix} 0 & 0 \\ J & 0\end{pmatrix} = \begin{pmatrix} BJ & 0 \\ DJ & 0\end{pmatrix}.$$

It follows that $A = D$, $B = 0$ and $AJ = JA$. In particular, M is a lower triangular matrix. With $A = (a_{ij})$, specifically:

$$\begin{pmatrix} a_{12} & \cdots & a_{1,d-1} & 0 \\ \vdots & & \vdots & \vdots \\ a_{d2} & \cdots & a_{d,d-1} & 0\end{pmatrix} = AJ = JA = \begin{pmatrix} 0 & \cdots & 0 \\ a_{11} & \cdots & a_{1d} \\ \vdots & & \vdots \\ a_{d-1,1} & \cdots & a_{d-1,d}\end{pmatrix}.$$

[11] see lecture notes Linear Algebra.

It follows that $a_{11} = \ldots = a_{dd}$. In the case $a_{11} \neq 0$, f is invertible, and otherwise f is nilpotent. Thus $\mathrm{End}_{KG}(V_{2d})$ is local (Theorem 11.4) and V_{2d} is indecomposable (Theorem 11.6).

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. □

Example 12.22. Let K be algebraically closed with $\mathrm{char}\, K = p$. Let $P := G_p \trianglelefteq G$ be the unique p-Sylow subgroup of G. By inflation from G/P, one obtains $k(G/P)$ non-isomorphic simple KG-modules (Remark 12.10). Conversely, let V be an arbitrary simple KG-module. By restriction, V is also a KP-module. According to Theorem 12.21, V possesses a trivial KP-submodule (for example, the second to last term of a composition series). In particular, $W := \{v \in V : \forall x \in P : xv = v\} \neq 0$. For $g \in G$, $x \in P$ and $w \in W$, it holds that

$$x(gw) = g(\underbrace{g^{-1}xg}_{\in P})w = gw.$$

This shows $gw \in W$ and $W \leq V$. Since V is simple, it follows that $W = V$, i. e. P acts trivially on V. The deflation of V is therefore a simple $K[G/P]$-module. Consequently, the simple KG-modules and the simple $K[G/P]$-modules correspond to each other via inflation and deflation. In particular, $k(G/P)$ is the number of p'-conjugacy classes of G.

Remark 12.23. HIGMAN has shown that the number of indecomposable KG-modules for an arbitrary finite group G is finite if and only if G has cyclic p-Sylow subgroups ($p = \mathrm{char}\, K$). If applicable, one says: KG has *finite representation type*.

13 Integral Representations

Remark 13.1. After having studied representations over $\mathbb{C}$, over number fields, and over fields of positive characteristic, we will entirely dispense with the field axioms in this chapter. In the simplest case, $\mathbb{Z}$ plays the role of the field. As in the last chapter, one defines the group *ring* $\mathbb{Z}G$. However, a $\mathbb{Z}G$-module generally does not possess a basis. For example, every finite abelian group A is a trivial $\mathbb{Z}G$-module and every element $a \in A$ is linearly dependent because of $|A|a = 0$. We therefore investigate a family of $\mathbb{Z}G$-modules which, by definition, possess a basis.

Definition 13.2.

- A homomorphism of the form $G \to \mathrm{GL}(n, \mathbb{Z})$ is called an *integral* representation.
- A free abelian group $\mathfrak{A}$ is called a *G-lattice*, if an action $G \times \mathfrak{A} \to \mathfrak{A}$ with ${}^g(x+y) = {}^gx + {}^gy$ exists. As with modules, we write gx instead of ${}^gx$. A G-invariant subgroup $\mathfrak{B} \leq \mathfrak{A}$ is called a *sublattice*, if $\mathfrak{A}/\mathfrak{B}$ is torsion-free. If $\mathfrak{A}$ possesses no proper, non-trivial sublattices, then $\mathfrak{A}$ is called *simple*.

Remark 13.3.

(i) We always assume that G-lattices have finite rank.

(ii) If $\Delta\colon G \to \mathrm{GL}(n,\mathbb{Z})$ is an integral representation, then $\mathfrak{A} := \mathbb{Z}^n$ becomes a G-lattice as usual via $ga = \Delta(g)a$ for $a \in \mathfrak{A}$ and $g \in G$. Conversely, the action of G on a lattice $\mathfrak{A}$ describes an integral representation Δ. A change of basis on $\mathfrak{A}$ replaces Δ by $g \mapsto S\Delta(g)S^{-1}$ for some $S \in \mathrm{GL}(n,\mathbb{Z})$. The well-known diagonalization arguments for matrices over fields are therefore not available here.

(iii) If $\mathfrak{B}$ is a sublattice of $\mathfrak{A}$, then $\mathfrak{A}/\mathfrak{B}$ is clearly also a G-lattice.

(iv) Let $b_1, \ldots, b_n$ be a basis of a G-lattice $\mathfrak{A}$. Then every element $a \in \mathfrak{A}$ can be uniquely written in the form $a = z_1b_1 + \ldots + z_nb_n$ with $z_1, \ldots, z_n \in \mathbb{Z}$. One can extend $\mathfrak{A}$ to a $\mathbb{Q}$-vector space V by allowing $z_1, \ldots, z_n \in \mathbb{Q}$. The action of G extends to V, so that one obtains a $\mathbb{Q}G$-module. This construction is called the *tensor product* of $\mathbb{Q}$ and $\mathfrak{A}$, written $V = \mathbb{Q} \otimes_{\mathbb{Z}} \mathfrak{A} = \mathbb{Q} \otimes \mathfrak{A}$. Obviously $\operatorname{rk}\mathfrak{A} = \dim V$.

(v) Conversely, let a $\mathbb{Q}G$-module V be given. According to Minkowski, there exists a basis $b_1, \ldots, b_n$ of V with respect to which G acts by integral matrices. Therefore $\mathfrak{A} := \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n$ is a G-lattice with $\mathbb{Q} \otimes \mathfrak{A} = V$.

(vi) Note that simple G-lattices $\mathfrak{A}$ can certainly possess proper G-invariant subgroups such as $2\mathfrak{A} = \{2a : a \in \mathfrak{A}\}$.

Lemma 13.4. *Let $\mathfrak{A}$ be a G-lattice and $V := \mathbb{Q} \otimes \mathfrak{A}$. Then the maps $\mathfrak{B} \to \mathbb{Q} \otimes \mathfrak{B}$ and $U \mapsto U \cap \mathfrak{A}$ are mutually inverse bijections between the set of sublattices of $\mathfrak{A}$ and the set of submodules of V. In particular, $\mathfrak{A}$ is simple if and only if V is simple.*

Proof. If $\mathfrak{B}$ is a sublattice of $\mathfrak{A}$, then $\mathbb{Q} \otimes \mathfrak{B} \leq V$. Conversely, let $U \leq V$. Then $\mathfrak{B} := \mathfrak{A} \cap U$ is a G-invariant subgroup of $\mathfrak{A}$. Let $a \in \mathfrak{A} \setminus \mathfrak{B}$. Suppose there exists an $m \in \mathbb{N}$ with $ma \in \mathfrak{B}$. Then $a = \frac{1}{m}ma \in \mathfrak{A} \cap U = \mathfrak{B}$. Thus $\mathfrak{A}/\mathfrak{B}$ is torsion-free. This shows that $\mathfrak{B}$ is a sublattice of $\mathfrak{A}$.

For a sublattice $\mathfrak{B}$, it is obvious that $\mathfrak{B} \subseteq \mathfrak{A} \cap (\mathbb{Q} \otimes \mathfrak{B})$. According to the fundamental theorem of finitely generated abelian groups, one can extend a basis $b_1, \ldots, b_k$ of $\mathfrak{B}$ to a basis of $\mathfrak{A}$. The elements in $\mathfrak{A} \cap (\mathbb{Q} \otimes \mathfrak{B})$ with respect to this basis are exactly the integer linear combinations of $b_1, \ldots, b_k$. Thus $\mathfrak{B} \subseteq \mathfrak{A} \cap (\mathbb{Q} \otimes \mathfrak{B})$.

For $U \leq V$, let $W := \mathbb{Q} \otimes (\mathfrak{A} \cap U) \leq U$. Let $b_1, \ldots, b_k$ be a $\mathbb{Q}$-basis of U. Then there exists an $m \in \mathbb{N}$ with $mb_i \in \mathfrak{A}$ for $i = 1, \ldots, k$. This shows $\dim W = \dim U$ and $W = U$. Therefore, the specified maps are inverse to each other. Consequently, they must be bijections. □

Remark 13.5. Let $\mathfrak{A}$ be a G-lattice with sublattice $\mathfrak{B}$. According to the fundamental theorem of finitely generated abelian groups, one can extend a basis of $\mathfrak{B}$ to a basis of $\mathfrak{A}$. The action of G on $\mathfrak{A}$ with respect to this basis is described by integer block matrices of the form $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)$. Here A describes the action on $\mathfrak{B}$ and C the action on $\mathfrak{A}/\mathfrak{B}$. According to Maschke, U has a complement W in V. Now $\mathfrak{C} := \mathfrak{A} \cap W$ is a sublattice of $\mathfrak{A}$, but in general $\mathfrak{B} + \mathfrak{C} < \mathfrak{A}$ holds. As a rule, $\mathfrak{B}$ has no complement in $\mathfrak{A}$.

Example 13.6. The group $G := \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right) \rangle \cong C_2$ acts on the lattice $\mathfrak{A} := \mathbb{Z}^2$ by matrix-vector multiplication. Obviously $\mathfrak{B} := \mathbb{Z}(1,0)^{\mathrm{t}}$ and $\mathfrak{C} := \mathbb{Z}(1,-2)^{\mathrm{t}}$ are sublattices with $\mathfrak{B} + \mathfrak{C} < \mathfrak{A}$. One easily sees that $\mathfrak{B}$ has no complement in $\mathfrak{A}$, i. e. $\mathfrak{A}$ is not semisimple or $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$ is not diagonalizable in $\mathrm{GL}(2,\mathbb{Z})$ (but in $\mathrm{GL}(2,\mathbb{Q})$).

Definition 13.7. Let $\mathfrak{A}$ and $\mathfrak{B}$ be G-lattices. A map $f\colon \mathfrak{A} \to \mathfrak{B}$ is called a *homomorphism*, if $f(gx + y) = gf(x) + f(y)$ holds for all $g \in G$ and $x, y \in \mathfrak{A}$. As usual, one defines mono-, epi- and isomorphisms. If an isomorphism exists, then $\mathfrak{A}$ and $\mathfrak{B}$ are called *isomorphic* and one writes $\mathfrak{A} \cong \mathfrak{B}$.

Lemma 13.8. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be G-lattices. Then there exist, up to isomorphism, only finitely many lattices $\mathfrak{C}$ with sublattice $\mathfrak{A}$ and $\mathfrak{C}/\mathfrak{A} \cong \mathfrak{B}$.*

Proof. As in Remark 13.5, we choose a basis of $\mathfrak{C}$ with respect to which the corresponding representation $\Delta\colon G \to \mathrm{GL}(n,\mathbb{Z})$ has the form $\Delta(g) = \left(\begin{smallmatrix} A_g & B_g \\ 0 & C_g \end{smallmatrix}\right)$ for $g \in G$. The matrices $A_g \in \mathrm{GL}(k,\mathbb{Z})$ and $C_g \in \mathrm{GL}(l,\mathbb{Z})$ are given up to integral similarity by $\mathfrak{A}$ and $\mathfrak{B}$. It suffices to show that there are only finitely many possibilities for B_g up to similarity. For $g, h \in G$ we have

$$\begin{pmatrix} A_{gh} & B_{gh} \\ 0 & C_{gh} \end{pmatrix} = \Delta(gh) = \Delta(g)\Delta(h) = \begin{pmatrix} A_gA_h & A_gB_h + B_gC_h \\ 0 & C_gC_h \end{pmatrix},$$

i. e. $A_gB_h = B_{gh} - B_gC_h$. As in the proof of Maschke, we use an averaging argument: For

$$M := \frac{1}{|G|} \sum_{x \in G} B_x C_x^{-1} \in \frac{1}{|G|}\mathbb{Z}^{k \times l}$$

it holds that

$$\begin{aligned} A_gM &= \frac{1}{|G|} \sum_{x \in G} A_gB_xC_x^{-1} = \frac{1}{|G|} \sum_{x \in G} (B_{gx} - B_gC_x)C_x^{-1} = \frac{1}{|G|} \sum_{x \in G} B_{gx}C_x^{-1} - B_g \\ &= \frac{1}{|G|} \sum_{y \in G} B_yC_y^{-1}C_g - B_g = MC_g - B_g. \end{aligned}$$

It follows that $B_g = MC_g - A_gM$. It thus suffices to restrict the possibilities for M. Let $E \in \mathbb{Z}^{k \times l}$ be arbitrary and $S = \left(\begin{smallmatrix} 1_k & E \\ 0 & 1_l \end{smallmatrix}\right)$. We can replace $\Delta(g)$ by

$$S^{-1}\Delta(g)S = \begin{pmatrix} 1_k & -E \\ 0 & 1_l \end{pmatrix} \begin{pmatrix} A_g & A_gE + B_g \\ 0 & C_g \end{pmatrix} = \begin{pmatrix} A_g & A_gE + B_g - EC_g \\ 0 & C_g \end{pmatrix}.$$

Subsequently, $B_g = (M + E)C_g - A_g(M + E)$ holds. By a suitable choice of E, one can achieve in this way that all entries of M lie between 0 and 1. Since these entries, on the other hand, lie in $\frac{1}{|G|}\mathbb{Z}$, there are only finitely many possibilities for M. □

Example 13.9. According to Example 13.6, $\mathbb{Z}^2$ and $\mathbb{Z}(1,0)^{\mathrm{t}} + \mathbb{Z}(1,-2)^{\mathrm{t}}$ are two non-isomorphic G-lattices with the same simple components.

Theorem 13.10 (Minkowski's linear forms theorem)**.** *Let $A \in \mathbb{Z}^{n \times n}$ and $d_1, \ldots, d_n \in \mathbb{R}_+$ with $d_1 \ldots d_n \geq |\det(A)|$. Then there exists an $x \in \mathbb{Z}^n \setminus \{0\}$ with $|(Ax)_i| < d_i$ for $i = 1, \ldots, n$.*

Proof (RADO). According to the Hermite normal form[12] there exists an $S \in \mathrm{GL}(n, \mathbb{Z})$ such that AS is a lower triangular matrix. If x satisfies the assertion for AS instead of A, then $S^{-1}x$ is a solution for A. We can therefore assume that A itself is a lower triangular matrix. Then $d_1 \dots d_n \geq |\det(A)| = |a_{11} \dots a_{nn}|$. For integers $0 \leq \alpha_i < |a_{ii}|$ and $0 \leq \delta_i \leq d_i$ we consider the system of equations $Ax = \alpha + \delta$. We show by induction on n that for a given $\delta \in \mathbb{Z}^n$ there exists exactly one $\alpha \in \mathbb{Z}^n$ such that the system has an integer solution x. In the case $n = 1$, α_1 and x_1 are uniquely determined by

$$\alpha_1 = a_{11}x_1 - \delta_1 \equiv -\delta_1 \pmod{|a_{11}|}$$

. Let $n \geq 2$ and $B := A_{nn}$. Inductively, there exist unique $\alpha_1, \dots, a_{n-1}$ such that $x_1, \dots, x_{n-1}$ is an integer solution of $Bx = \alpha + \delta$. Now α_n and x_n are uniquely determined by

$$\alpha_n = a_{n1}x_1 + \dots + a_{nn}x_n - \delta_n \equiv a_{n1}x_1 + \dots + a_{n,n-1}x_{n-1} - \delta_n \pmod{|a_{nn}|}$$

(because $a_{in} = 0$ for $i < n$, x_n only appears in this equation).

Apparently there are $(\lfloor d_1 \rfloor + 1) \dots (\lfloor d_n \rfloor + 1) > d_1 \dots d_n$ possible vectors δ, but only $|a_{11} \dots a_{nn}| \leq d_1 \dots d_n$ possible α. For at least one α there must therefore exist $\delta \neq \delta'$ such that $Ay = \alpha + \delta$ and $Az = \alpha + \delta'$ have integer solutions $y \neq z$. Now $x := y - z \neq 0$ satisfies the assertion, because $|(Ax)_i| = |\delta_i - \delta'_i| \leq d_i$. □

Remark 13.11. The linear forms theorem can be easily transferred to real matrices A.[13] However, we do not need this generalization.

Theorem 13.12 (JORDAN-ZASSENHAUS)**.** *For each $n \in \mathbb{N}$ there exist, up to isomorphism, only finitely many G-lattices of rank n.*

Proof (GASCHÜTZ). According to Lemma 13.8, it suffices to show that up to isomorphism, only finitely many *simple* G-lattices of rank n exist. Since there are only finitely many (simple) $\mathbb{Q}G$-modules of dimension n up to isomorphism, we can fix such a module $V = \mathbb{Q}^n$ and examine G-lattices $\mathfrak{A} \subseteq V$. According to Remark 13.3, there exists a basis $a_1, \dots, a_n$ of V such that the corresponding representation $\Delta\colon G \to \mathrm{GL}(V)$ is realized by integral matrices. Let $\mathfrak{A} = \mathbb{Z}a_1 + \dots + \mathbb{Z}a_n$ be the corresponding lattice. We determine a constant $c \in \mathbb{N}$ depending only on Δ, such that every G-lattice of rank n contained in V is isomorphic to a lattice $\mathfrak{C} \supseteq \mathfrak{A}$ with $|\mathfrak{C} : \mathfrak{A}| \leq c$. Because of $\mathfrak{A} \subseteq \mathfrak{C} \subseteq \frac{1}{c}\mathfrak{A}$ and $\frac{1}{c}\mathfrak{A}/\mathfrak{A} \cong (\mathbb{Z}/c\mathbb{Z})^n$, there are only finitely many possibilities for $\mathfrak{C}$.

Let $\mathfrak{B} \subseteq V$ be a G-lattice of rank n. By replacing $\mathfrak{B}$ with $d\mathfrak{B} \cong \mathfrak{B}$ for a suitable d, one can assume $\mathfrak{B} \subseteq \mathfrak{A}$. Since $\mathfrak{A}$ and $\mathfrak{B}$ are free abelian groups of the same rank, $D := |\mathfrak{A} : \mathfrak{B}| < \infty$ holds. A basis $b_1, \dots, b_n$ of $\mathfrak{B}$ can be written in the form $b_i := \sum_{j=1}^n \beta_{ji}a_j$ with $B = (\beta_{ij}) \in \mathbb{Z}^{n \times n}$. As is well known (Algebra), $|\det(B)| = D$ holds. According to the linear forms theorem?!, there exists an $x \in \mathbb{Z}^n \setminus \{0\}$ with $|(Bx)_i| \leq \sqrt[n]{D}$ for $i = 1, \dots, n$. For $s := Bx \in \mathbb{Z}^n$, it holds that

$$t := \sum_{i=1}^n s_i a_i = \sum_{i=1}^n \sum_{j=1}^n x_j \beta_{ij} a_i = \sum_{j=1}^n x_j b_j \in \mathfrak{B}.$$

Wlog. let $s_1 \neq 0$. Let $\varphi \in \mathrm{End}(V)$ with $\varphi(a_1) = t$ and $\varphi(a_i) = 0$ for $i = 2, \dots, n$. Then

$$\psi := \sum_{g \in G} \Delta(g) \circ \varphi \circ \Delta(g)^{-1}$$

[12] See notes on linear algebra.
[13] See notes on linear algebra.

is an endomorphism of $\mathbb{Q}G$-modules with $\psi(\mathfrak{A}) \subseteq \mathfrak{B}$. Because of $\operatorname{tr}(\psi) = \sum_{g \in G} \operatorname{tr}(\varphi) = |G| s_1 \neq 0$, we have $\psi \neq 0$. According to Schur's Lemma, ψ is an automorphism. Let $M \in \mathrm{GL}(n, \mathbb{Q})$ be the matrix of ψ with respect to $a_1, \ldots, a_n$. Then $|\mathfrak{A} : \psi(\mathfrak{A})| = |\det(M)|$ holds. Every entry of M is a linear combination of $s_1, \ldots, s_n$ with coefficients that depend only on Δ. According to the Leibniz formula for determinants, $\det(M)$ is a linear combination of terms of the form $s_{i_1} \ldots s_{i_n}$ with $1 \leq i_1, \ldots, i_n \leq n$ and coefficients that depend only on Δ. By the choice of s, $|s_{i_1} \ldots s_{i_n}| \leq D$ holds. The triangle inequality shows $|\mathfrak{A} : \psi(\mathfrak{A})| = |\det(M)| \leq cD = c|\mathfrak{A} : \mathfrak{B}|$ for a constant c. For $\mathfrak{C} := \psi^{-1}(\mathfrak{B}) \cong \mathfrak{B}$, it now holds that $\mathfrak{A} = \psi^{-1}(\psi(\mathfrak{A})) \subseteq \psi^{-1}(\mathfrak{B}) = \mathfrak{C}$ and

$$|\mathfrak{C} : \mathfrak{A}| = |\mathfrak{B} : \psi(\mathfrak{A})| = \frac{|\mathfrak{A} : \psi(\mathfrak{A})|}{|\mathfrak{A} : \mathfrak{B}|} \leq c,$$

as claimed. □

Example 13.13.

(i) Let $G := \langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle \cong S_3$ with the natural representation on $V := \mathbb{Q}^2$. Obviously $\mathfrak{A} := \mathbb{Z}^2$ and $\mathfrak{B} := \mathbb{Z}(1, -1)^{\mathrm{t}} + \mathbb{Z}(2, 1)^{\mathrm{t}}$ are simple G-lattices in V. Suppose there exists an isomorphism $\varphi \colon \mathfrak{A} \to \mathfrak{B}$. Since V is absolutely irreducible, $\varphi = k \operatorname{id}$ for some $k \in \mathbb{Z}$ by Theorem 12.7. Then, however,

$$3 = \det \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} = |\mathfrak{A} : \mathfrak{B}| = |\mathfrak{A} : \varphi(\mathfrak{A})| = |\mathbb{Z}^2 : k\mathbb{Z}^2| = k^2.$$

Thus $\mathfrak{A} \ncong \mathfrak{B}$. In Exercise 42 it is shown that there are no further non-isomorphic G-lattices in V. Since V is the only simple $\mathbb{Q}G$-module of dimension 2, there are generally no further simple G-lattices of rank 2.

(ii) Let $\zeta := e^{2\pi \mathrm{i}/n} \in \mathbb{C}$. Then $G = \langle \zeta \rangle \cong C_n$ acts by multiplication on $K := \mathbb{Q}(\zeta) = \mathbb{Q}_n \cong \mathbb{Q}^{\varphi(n)}$. The G-lattices in K are the so-called *fractional* ideals. Let $\varphi \colon \mathfrak{A} \to \mathfrak{B}$ be an isomorphism between such lattices. Then $\varphi(\zeta x) = \zeta \varphi(x)$ for $x \in \mathfrak{A}$. Since K is generated by ζ, it even holds that $\varphi(\lambda x) = \lambda \varphi(x)$ for all $\lambda \in K$. Let $a \in \mathfrak{A} \setminus \{0\}$ and $c := \varphi(a)/a \in K$. For all $x \in \mathfrak{A}$ it holds that

$$a\varphi(x) = \varphi(ax) = \varphi(xa) = x\varphi(a),$$

i. e. $\varphi(x) = cx$ and $\mathfrak{B} = c\mathfrak{A}$. Conversely, $\mathfrak{A}$ is isomorphic to all multiples. In particular, $\mathfrak{A}$ is isomorphic to an ideal of the ring of integers

$$\mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\zeta + \ldots + \mathbb{Z}\zeta^{\varphi(n)-1}.$$

The number of isomorphism classes of lattices is called the *class number* $h(K)$ of K. $h(K) = 1$ holds if and only if $\mathbb{Z}[\zeta]$ is a principal ideal domain. This is equivalent to

$$n \in \{1, \ldots, 22, 24, \ldots, 28, 30, 32, \ldots, 36, 38, 40, 42, 44, 45, 48, 50, 54, 60, 66, 70, 84, 90\}$$

(only 30 different fields because of $\mathbb{Q}_{2q} = \mathbb{Q}_q$ for odd q). On the other hand, $h(\mathbb{Q}_{23}) = 3$ (without proof).

(iii) For arbitrary $\mathbb{Z}G$-modules, the Jordan-Zassenhaus theorem is false, since with $\mathbb{Z}/k\mathbb{Z}$ for $k \in \mathbb{N}$ there are already infinitely many (trivial) $\mathbb{Z}G$-modules of rank 1.

Remark 13.14.

(i) The Jordan-Zassenhaus theorem holds more generally for the ring of integers $\mathbb{Z}_K$ of a number field K, instead of $\mathbb{Z}$. In fact, one can replace KG by a semisimple K-algebra.

(ii) The next theorem improves Corollary 7.7.

Corollary 13.15. *For every n, $\mathrm{GL}(n,\mathbb{Q})$ and $\mathrm{GL}(n,\mathbb{Z})$ possess only finitely many conjugacy classes of finite groups.*

Proof. According to Theorem 7.6, it suffices to prove the statement for $\mathrm{GL}(n,\mathbb{Z})$. According to Corollary 7.7, we can fix the isomorphism class of a finite group $G \leq \mathrm{GL}(n,\mathbb{Z})$. According to Jordan-Zassenhaus, there exist only finitely many non-isomorphic G-lattices $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$. Let $\Delta_i \colon G \to \mathrm{GL}(n,\mathbb{Z})$ be a representation associated with $\mathfrak{A}_i$ and $G_i := \Delta(G)$ for $i = 1, \ldots, k$. Let $\varphi \colon G \to H \leq \mathrm{GL}(n,\mathbb{Z})$ be an arbitrary isomorphism. Then $\mathfrak{B} := \mathbb{Z}^n$ becomes a G-lattice via $gz := \varphi(g)z$ for $z \in \mathfrak{B}$. Wlog. there exists an isomorphism $\gamma \colon \mathfrak{A}_1 \to \mathfrak{B}$. With respect to a suitable basis, γ can be realized by a matrix $A \in \mathrm{GL}(n,\mathbb{Z})$. In this case,

$$Agx = \gamma(gx) = g\gamma(x) = \varphi(g)Ax$$

holds for all $x \in \mathfrak{A}$. It follows that $A^{-1}gA = \varphi(g)$ and $A^{-1}GA = H$. □

Example 13.16. We determine the conjugacy classes of subgroups of order 2 in $\mathrm{GL}(2,\mathbb{Z})$. Let $A \in \mathrm{GL}(2,\mathbb{Z})$ be of order 2. Since there is no simple $\mathbb{Q}G$-module of dimension 2, every G-lattice of rank 2 possesses a sublattice of rank 1 according to Lemma 13.4. We can therefore assume $A = \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$. From $A^2 = 1_2$ it follows that $a, c \in \{\pm 1\}$ and $(a+c)b = 0$. In the case $a = c$, b must be 0. Then one obtains $A = -1_2$ in its own conjugacy class $\{A\}$. Now let $ac = -1$. For $b = 0$, two matrices arise which are transformed into each other by conjugation with $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. So let $b \neq 0$. Because of

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a & 0 \\ -2b^{-1} & a \end{pmatrix} = \begin{pmatrix} -1 & ab \\ -2b^{-1}c & -1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ -2b^{-1} & a \end{pmatrix}\begin{pmatrix} c & b \\ 0 & a \end{pmatrix}$$

one can assume $a = 1 = -c$. Because of

$$\begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+s \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b+2s \\ 0 & -1 \end{pmatrix}$$

for $s \in \mathbb{Z}$, one can assume $b = 1$. In total, one obtains three matrices -1_2, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$, which are not conjugate according to Example 13.6.

Remark 13.17. For infinite groups G, Corollary 13.15 does not hold (Exercise 43). However, the following variant holds: If $A \in \mathrm{GL}(n,\mathbb{Z})$ is diagonalizable in $\mathrm{GL}(n,\mathbb{C})$, then the $\mathrm{GL}(n,\mathbb{Q})$-conjugacy class of A splits into finitely many conjugacy classes in $\mathrm{GL}(n,\mathbb{Z})$. This is because $\mathbb{Q}(A) := \{\gamma(A) : \gamma \in \mathbb{Q}[X]\} \subseteq \mathbb{Q}^{n\times n}$ is a semisimple algebra (see Remark 13.14).

Exercises

Exercise 1 (2 + 2 + 3 points)**.** Let G be a finite group and K a field. Let V be a K-vector space with basis $\{v_g : g \in G\}$. For $g, x \in G$, let $\Delta(g) \colon V \to V$, $v_x \mapsto v_{gx}$ be linear.

(a) Show that $\Delta \colon G \to \mathrm{GL}(V)$ is a faithful representation of G.

(b) Calculate the character of Δ.

(c) Let $\operatorname{char} K$ be a divisor of $|G|$ and $s := \sum_{g\in G} v_g \in V$. Show that Ks is a Δ-invariant subspace that possesses no Δ-invariant complement in V.

One calls Δ the *regular* representation of G.

Exercise 2 (2 points)**.** Determine the irreducible $\mathbb{C}$-representations of a finite cyclic group.

Exercise 3 ($2+2$ points)**.** Let $n \in \mathbb{N}$ be even and $G = D_{2n} = \langle \sigma, \tau \rangle$ the dihedral group of order $2n$. Show:

(a) For all $\epsilon, \mu \in \{\pm 1\}$, there exists a representation Δ of G with $\Delta(\sigma) = \epsilon$ and $\Delta(\tau) = \mu$.

(b) There are (at least) $\frac{n-2}{2}$ pairwise non-similar irreducible $\mathbb{R}$-representations of G of degree 2.

Exercise 4 (2 points)**.** Let Δ be a $\mathbb{C}$-matrix representation of a finite group G, and let $g \in G$. Show that $\Delta(g)$ is diagonalizable.
Hint: One can use the minimal polynomial or Theorem 2.2 of the lecture.

Exercise 5 ($2+2+2$ points)**.** Let Δ be a $\mathbb{C}$-matrix representation of G with character χ.

(a) Show that $\overline{\Delta}$ with $\overline{\Delta}(g) := \overline{\Delta(g)}$ for $g \in G$ is also a matrix representation of G. Here, $\overline{\Delta(g)}$ is the complex conjugate of $\Delta(g)$.

(b) Δ is irreducible if and only if $\overline{\Delta}$ is irreducible.

(c) $\overline{\Delta}$ has character $\overline{\chi}$ with $\overline{\chi}(g) := \overline{\chi(g)} = \chi(g^{-1})$ for $g \in G$.
Hint: One can use Exercise 4.

Exercise 6 (2 points)**.** Let $\chi, \psi \in \mathrm{Irr}(G)$ with $\chi(1) = 1$. Show: $\chi\psi \in \mathrm{Irr}(G)$.

Exercise 7 (2 points)**.** Determine the character table of D_{4n} for $n \in \mathbb{N}$.

Exercise 8 ($2+2+2$ points)**.** Let $\Delta \colon G \to \mathrm{GL}(n, \mathbb{R})$ be a representation. Show:

(a) $S := \sum_{g \in G} \Delta(g)\Delta(g)^{\mathrm{t}}$ is symmetric and positive definite.

(b) There exists $T \in \mathrm{GL}(n, \mathbb{R})$ with $T^2 = S$.
Hint: Spectral theorem.

(c) $T^{-1}\Delta(x)T$ is an orthogonal matrix for all $x \in G$.

Remark: Every $\mathbb{R}$-representation is thus similar to an *orthogonal* representation $G \to \mathrm{O}(n, \mathbb{R})$.

Exercise 9 ($2+2+3$ points)**.** Let

$$Q_8 := \left\langle \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle \leq \mathrm{GL}(2, \mathbb{C})$$

be the *quaternion group*. Show:

(a) $|Q_8| = 8$, $Q_8' = \langle -1_2 \rangle$ and $Q_8/Q_8' \cong C_2 \times C_2$.

(b) Determine the character table of Q_8 and compare it with D_8 (Exercise 7).

(c) Show that the embedding $Q_8 \hookrightarrow \mathrm{GL}(2,\mathbb{C})$ is not similar to any $\mathbb{R}$-representation, although the character is real-valued.
Hint: Exercise 8.
Remark: It follows that $Q_8 \ncong D_8$.

Exercise 10 $(2+2+2+2$ points$)$**.** Show:

(a) For characters χ, ψ of G, it holds: $\mathrm{Ker}(\chi+\psi) = \mathrm{Ker}(\chi) \cap \mathrm{Ker}(\psi)$.

(b) Every normal subgroup of G is the kernel of a character.

(c) $\bigcap_{\chi \in \mathrm{Irr}(G)} \mathrm{Ker}(\chi) = 1$.

(d) $\bigcap_{\chi \in \mathrm{Irr}(G)} \mathrm{Z}(\chi) = \mathrm{Z}(G)$.

Exercise 11 (3 points)**.** Determine the character table of S_3 using the Burnside algorithm (Theorem 3.19).

Exercise 12 (2 points)**.** Find a monic, integer polynomial with root $\sqrt{2} + \sqrt[3]{3}$.

Exercise 13 (3 points)**.** Let A be an abelian subgroup of G and $\chi \in \mathrm{Irr}(G)$. Show:

$$\chi(1) \leq |G : A|.$$

Hint: Frobenius reciprocity.

Exercise 14 (3 points)**.** A *permutation matrix* has the form $P = (\delta_{i\pi(j)})_{i,j} \in \mathbb{Z}^{n\times n}$, where $\pi \in S_n$ and δ_{ij} is the Kronecker delta. Determine the eigenvalues of P depending on π.

Exercise 15 $(2+1+3+2$ points$)$**.** Let $N \trianglelefteq G$, $g \in G$ and ψ be a character of N. Show:

(a) The map ${}^g\psi \colon N \to \mathbb{C}$, $x \mapsto \psi(g^{-1}xg)$ is a character of N.

(b) G acts on $\mathrm{Irr}(N)$ via $(g,\psi) \mapsto {}^g\psi$.

(c) (Clifford) For $\chi \in \mathrm{Irr}(G)$ there exist $e \in \mathbb{N}$ and $\psi \in \mathrm{Irr}(N)$ with

$$\chi_N = e \sum_{gG_\psi \in G/G_\psi} {}^g\psi,$$

where G_ψ is the stabilizer of ψ in G.
Remark: e is called the *ramification index* of χ w.r.t. N.

(d) $\psi^G \in \mathrm{Irr}(G)$ holds if and only if $\psi \in \mathrm{Irr}(N)$ and $G_\psi = N$.

Exercise 16 (3 points)**.** Let F be a finite field with $|F| > 2$. For $a \in F^\times$ and $b \in F$ let $\varphi_{a,b} \colon F \to F$, $x \mapsto ax + b$. Show that

$$\mathrm{Aff}(F) := \{\varphi_{a,b} : a \in F^\times, b \in F\} \leq \mathrm{Sym}(F)$$

is a Frobenius group.

Exercise 17 (2 + 2 + 2 + 2 points)**.** As is well known, every action of G on a set Ω induces a homomorphism $\varphi\colon G \to S_n$ with $n = |\Omega|$. Show:

(a) The map $\tau\colon S_n \to \mathrm{GL}(n,\mathbb{C})$, $\pi \mapsto (\delta_{i\pi(j)})_{i,j=1}^n$ is a monomorphism. In particular, $\Delta := \tau \circ \varphi\colon G \to \mathrm{GL}(n,\mathbb{C})$ is a representation of G. (One calls Δ a *permutation representation*.)

(b) For the character χ of Δ, $\chi(g) := |\{\omega \in \Omega : {}^g\omega = \omega\}|$ holds for $g \in G$. (One calls χ a *permutation character*.)

(c) Let $\omega_1, \ldots, \omega_m \in \Omega$ be representatives for the orbits of the action. Then

$$\chi = \sum_{i=1}^{m} \mathbb{1}_{G_{\omega_i}}^G,$$

where G_ω is the stabilizer of $\omega \in \Omega$ in G.

(d) $m = (\mathbb{1}_G, \chi)_G$ holds. In particular, $\chi - \mathbb{1}_G$ is a character of G if $n > 1$.

Exercise 18 (2 points)**.** Show that S_n is isomorphic to a subgroup of $\mathrm{GL}(n-1,\mathbb{Z})$ for $n \geq 2$.

Exercise 19 (2 + 2 + 2 points)**.** Show:

(a) Permutations of the same cycle type in S_n are conjugate.

(b) If $g, h \in S_n$ with $\langle g \rangle = \langle h \rangle$, then g and h are conjugate.

(c) The character table of S_n is integer-valued.
Hint: Brauer's permutation lemma.

Exercise 20 (3 points)**.** Show that

$$\mathbb{H} := \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$$

as a subalgebra of $\mathbb{C}^{2\times 2}$ is an $\mathbb{R}$-division algebra. $\mathbb{H}$ is called *quaternion algebra* after Hamilton.
Remark: Frobenius showed that $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$ are the only division algebras over $\mathbb{R}$.

Exercise 21 (2 + 2 points)**.** Let A be a simple algebra. Show:

(a) $\mathrm{Z}(A)$ is a field.

(b) Any two simple A-modules are isomorphic.

Exercise 22 (2 points)**.** Let A be an algebra. Show that every simple A-module is isomorphic to a direct factor of $A/\mathrm{J}(A)$. In particular, the number of isomorphism classes of simple A-modules is bounded by $\dim A/\mathrm{J}(A)$.
Remark: This improves Corollary 9.12 and is further improved in Corollary 11.13.

Exercise 23 $(1+3+2+2$ points$)$**.** Let K be a field.

(a) Show that the matrices of the form

$$\begin{pmatrix} * & * & * \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix}$$

form a subalgebra A of $K^{3\times 3}$.

(b) Check whether A is commutative, semisimple or local.

(c) Determine a composition series of the regular A-module.

(d) How many simple modules does A have up to isomorphism?

The following exercises were not assigned:

Exercise 24 (2+2+2+2 points)**.** Let G, H be finite, abelian groups. Show:

(a) $\widehat{G} := \mathrm{Irr}(G)$ is an abelian group with respect to multiplication. (One calls $\widehat{G}$ the *character group* of G.)

(b) $\widehat{\widehat{G}} \cong G$
Hint: Think of the bidual space. Do not use (d).

(c) $\widehat{G \times H} \cong \widehat{G} \times \widehat{H}$.

(d) $\widehat{G} \cong G$.

Exercise 25 (2 points)**.** Let $x \in \mathbb{C}$ be algebraic. Show that x is an algebraic integer if and only if the minimal polynomial of x lies in $\mathbb{Z}[X]$.

Exercise 26 (2 points)**.** Show $\gamma_{CDE} = \gamma_{DCE}$ for all $C, D, E \in \mathrm{Cl}(G)$.

Exercise 27 (3 points)**.** Let $A \in K^{n\times n}$ and $B \in K^{m\times m}$. Show for the Kronecker product $\det(A \otimes B) = \det(A)^m \det(B)^n$.
Hint: Gaussian elimination.

Exercise 28 (2 points)**.** Let $N \trianglelefteq G$ and $\chi \in \mathrm{Irr}(G)$. Show that $(\chi_N)^G = \chi\rho$ holds, where ρ is the inflation of the regular character of G/N.

Exercise 29 (3 points)**.** Let $H \leq G$ and Δ be a representation of H with character χ. Let $t_1, \ldots, t_m$ be a transversal for the left cosets of H in G. For $g \in G$ let $\dot{\Delta}(g) := \Delta(g)$ if $g \in H$ and $0 \in \mathbb{Z}^{\chi(1)\times\chi(1)}$ otherwise. For $g \in G$ we define the block matrix

$$\Delta^G(g) := \begin{pmatrix} \dot{\Delta}(t_1^{-1}gt_1) & \cdots & \dot{\Delta}(t_1^{-1}gt_m) \\ \vdots & \ddots & \vdots \\ \dot{\Delta}(t_m^{-1}gt_1) & \ldots & \dot{\Delta}(t_m^{-1}gt_m) \end{pmatrix}.$$

Show that Δ^G is a representation of G with character χ^G.

Exercise 30 (2 points)**.** Let $H \leq G$ with $\gcd(|H|, |G : H|) = 1$. Show $G' \cap \mathrm{Z}(G) \cap H \leq H'$.
Remark: This generalizes the theorem of Taunt.
Hint: Every group is generated by Sylow subgroups.

Exercise 31 (2 points)**.** Let $G \leq \mathrm{GL}(n, \mathbb{Q})$ be finite. Show that there exists a normal subgroup $N \cong C_2^k$ (with $k \in \mathbb{N}_0$) of G such that G/N is isomorphic to a subgroup of $\mathrm{GL}(n, 2)$.

Exercise 32 (3 points)**.** Let $G \leq \mathrm{GL}(2, \mathbb{R})$ be finite. Show: If $G \leq \mathrm{SL}(2, \mathbb{R})$, then G is cyclic and otherwise a dihedral group.
Hint: Exercise 8.

Exercise 33 (Bonus task, +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}					

Hint: Example 3.16.

Exercise 34 (3 points)**.** Let K be a field and $n \in \mathbb{N}$. For a relation $R \subseteq \{1, \ldots, n\}^2$ let

$$A_R := \big\{(a_{ij}) \in K^{n \times n} : (i, j) \notin R \Longrightarrow a_{ij} = 0\big\}.$$

Show that A_R is a K-algebra if and only if R is reflexive ($\forall i : (i, i) \in R$) and transitive ($(i, j), (j, k) \in R \Rightarrow (i, k) \in R$).
Remark: For the equality relation R one obtains the diagonal matrices and for the less-than-or-equal relation one obtains the upper triangular matrices.

Exercise 35 (3 points)**.** Let A be an algebra. Show that A-modules M and N are isomorphic if and only if $\mathrm{Ann}(M) = \mathrm{Ann}(N)$ holds.

Exercise 36 ($2 + 2 + 2$ points)**.** Let $e \neq 0$ be an idempotent of a K-algebra A. Show:

(a) eAe is a K-algebra, but in general not a subalgebra of A.

(b) $\mathrm{J}(eAe) = e\mathrm{J}(A)e$.

(c) $\mathrm{End}_A(Ae) \cong (eAe)^o$, where Ae is the submodule of the regular A-module generated by e.

Addition: Does $\mathrm{Z}(eAe) = e\mathrm{Z}(A)e$ also hold?

Exercise 37 (2 + 2 points)**.** Let A be an algebra and $N \leq M$ A-modules. Show:

(a) (NAKAYAMA's Lemma) From $M = N + \mathrm{J}(A)M$ it follows that $M = N$.

(b) $\mathrm{J}(M) := \mathrm{J}(A)M$ is the intersection of all maximal submodules of M.

Hint: Proof of Theorem 9.15.

Exercise 38 (2 + 3 points)**.** Show for every finite group G:

(a) For $\chi \in \mathrm{Irr}(G)$, $\omega_\chi \colon \mathrm{Z}(\mathbb{C}G) \to \mathbb{C}$, $C^+ \mapsto \omega_\chi(C)$ is a homomorphism of algebras.

(b) Every homomorphism $\mathrm{Z}(\mathbb{C}G) \to \mathbb{C}$ has the form ω_χ for some $\chi \in \mathrm{Irr}(G)$.

Exercise 39 (3 points)**.** Determine the Artin-Wedderburn decomposition of $\mathbb{R}C_n$ for $n \in \mathbb{N}$.

Exercise 40 (4 points)**.** Show that a number field K is a splitting field for the finite group G if and only if there exist $n_1, \ldots, n_k \in \mathbb{N}$ with $KG \cong K^{n_1 \times n_1} \times \ldots \times K^{n_k \times n_k}$.
Hint: Theorem 12.7.

Exercise 41 (3 points)**.** Let K be an algebraically closed field of characteristic $p > 0$ and G a finite group. Show that KG has, up to isomorphism, exactly $|G : G'|_{p'}$ modules of dimension 1 (where $|G : G'|_{p'}$ is the largest divisor of $|G : G'|$ coprime to p).

Exercise 42 (2 + 3 + 3 + 3 points)**.** Let $G := \langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle \cong S_3$ with the natural representation on $V := \mathbb{Q}^2$. Let $\mathfrak{A} := \mathbb{Z}^2 \subseteq V$ be a G-lattice. Recapitulate the proof of Jordan-Zassenhaus in this situation:

(a) Show $M = 3s_1 1_2$. Thus one can choose $c = 9$.

(b) Construct all subgroups in $\mathfrak{A}/9\mathfrak{A}$.

(c) Which of these are G-lattices ($\mathfrak{A}$, $3\mathfrak{A}$, $9\mathfrak{A}$, $\mathfrak{B}$, $3\mathfrak{B}$).

(d) Show that there are exactly six isomorphism classes of (not necessarily simple) G-lattices of rank 2.
Hint: Example 13.16

Exercise 43 (2 points)**.** Show that the matrices $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ with $a \in \mathbb{N}$ are conjugate in $\mathrm{GL}(2, \mathbb{Q})$, but are pairwise not conjugate in $\mathrm{GL}(2, \mathbb{Z})$.

Index

Symbols

$(\chi, \psi)_G$, 8
$[x, y]$, 14
$\mathbb{1}_G$, 4
$\mathrm{Aff}(F)$, 59
A_n, 4
$\mathrm{Ann}(M)$, 37
A^o, 30
C^+, 47
$\mathrm{CF}(G)$, 8
$C(G)$, 12
$\mathrm{C}_G(g)$, 8
$\mathrm{Cl}(G)$, 8
$\mathrm{Cl}(g)$, 8
C_n, 14
D_{2^n}, 4
$\Delta \oplus \Gamma$, 4
Δ_H, 4
$\det \chi$, 8
E_{ij}, 9
$\mathrm{End}_A(M)$, 36
G', 14
$\gamma(A)$, 43
γ_{CDE}, 11
$\mathbb{H}$, 60
$\mathrm{Hom}_A(M, N)$, 35
$\mathrm{Irr}(G)$, 7
$\mathrm{J}(M)$, 63
$k(G)$, 8
$\mathrm{Ker}(\chi)$, 15
$K^\times$, 4
$M \simeq N$, 35
$\omega_\chi(C)$, 11
φ^G, 19
Q_8, 58
$\mathbb{Q}_n$, 22
$\mathrm{Sec}_{p'}(x)$, 48
sgn, 4
S_n, 4
$\mathrm{Z}(A)$, 30
$\mathrm{Z}(\chi)$, 15
$\overline{\mathbb{Q}}$, 24

A

action, 4
algebra, 30
  local, 32
  opposite, 30
  semisimple, 32
  simple, 31
algebraic integer, 17
annihilator, 37
Artin-Wedderburn, 41

B

Brauer, 49
Brauer character, 50
Brauer's Induction Theorem, 24
Brauer's Permutation Lemma, 28
Burnside, 46
Burnside algorithm, 16
Burnside's $p^a q^b$-theorem, 22

C

center, 30
centralizer, 8
character, 7
  center, 15
  degree, 7
  faithful, 7
  induced, 20
  irreducible, 7
  linear, 8
  trivial, 8
character group, 61
character sudoku, 62
character table, 12
  D_{4n}, 58
  A_4, 15
  A_5, 29
  abelian group, 14
  $C_2 \times C_2$, 14
  C_n, 14
  Q_8, 58
  S_n, 60
class function, 8
  induced, 19
class multiplication constant, 11
class number
  of a group, 8
  of a number field, 56
class sum, 47
Clifford, 59
commutator, 14
commutator space, 43
composition factor, 36
composition series, 36
conjugacy class, 8
constituent
  irreducible, 12
  multiplicity, 12
Correspondence Theorem, 32

D

Dedekind identity, 35
deflation, 4
degree, 4

Δ-invariant, 5
derived subgroup, 14
dihedral group, 4
direct product, 30
Dirichlet, 7
division algebra, 30
Dixon-Schneider algorithm, 17

E
element
  conjugate, 8
  idempotent, 33
  nilpotent, 33
endomorphism algebra, 36

F
Feit, 26, 27
Fitting, 42
Frobenius, 22, 60
Frobenius group, 23
Frobenius reciprocity, 20

G
Galois conjugate, 28
Gaschütz, 55
G-lattice, 52
  homomorphism, 54
  isomorphic, 54
  simple, 52
group algebra, 45

H
Hamilton, 60
Higman, 52
homomorphism
  of algebras, 30
  of modules, 35
homomorphism Theorem
  for algebras, 31
homomorphism theorem
  for modules, 36

I
ideal, 31
  fractional, 56
  nilpotent, 31
idempotent, 33
  lifting, 34
inflation, 4
involution, 14
isomorphism theorems
  for algebras, 31
  for modules, 36

J
Jacobson radical, 32
Jordan, 27
Jordan-Hölder, 36
Jordan-Zassenhaus, 55

K
K-representation, 4
Knapp-Schmid, 23
Koh, 34
Kronecker product, 12
Krull-Schmidt, 42

M
Maschke, 5, 46
matrix representation, 4
Minkowski, 25
Minkowski's linear forms theorem, 54
module, 34
  (in)decomposable, 41
  regular, 35
  semisimple, 38
  simple, 35
  trivial, 35, 46

N
Nakayama's Lemma, 63
nilpotent, 33
number field, 24

O
orthogonality relation
  first, 9
  second, 11

P
p-conjugacy class, 48
p-element, p'-element, 48
p-factor, p'-factor, 48
p'-section, 48
permutation character, 60
permutation matrix, 59
  generalized, 26
permutation representation, 60

Q
quaternion algebra, 60
quaternion group, 58

R
radical, 32
Rado, 55
ramification index, 59
representation
  (ir)reducible, 5
  absolutely irreducible, 25
  degree, 4
  faithful, 4
  integral, 52
  of an algebra, 36

orthogonal, 58
regular, 58
similar, 5
trivial, 4
restriction, 4

S
Schur, 29
Schur relations, 9
Schur's Lemma, 6
splitting field, 25
subalgebra, 30
sublattice, 52
submodule, 35

T
Taunt, 23
tensor product, 53

W
Wedderburn, 30