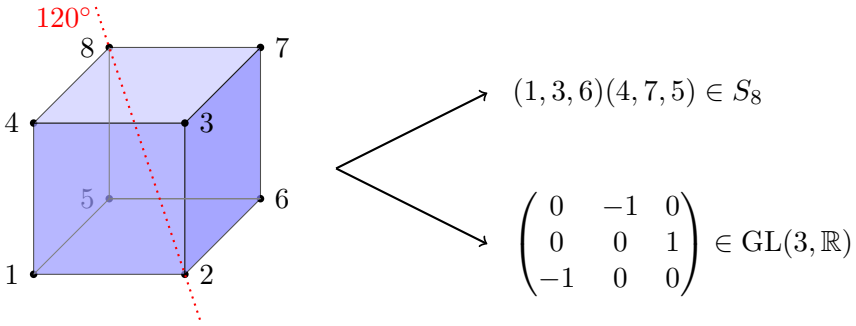
Darstellungstheorie

Vorlesung im Sommersemester 2023

Benjamin Sambale
Leibniz Universität Hannover

Version: 31. Mai 2026



Inhaltsverzeichnis

Vorwort 2

1 Darstellungen 3

2 Charaktere 6

3 Charaktertafeln 12

4 Ganz-algebraische Zahlen 17

5 Induzierte Charaktere 19

6 Anwendungen 21

7 Darstellungen über Zahlkörpern 24

8 Algebren 30

9 Moduln 35

10 Halbeinfache Moduln 39

11 Unzerlegbare Moduln 42

12 Gruppenalgebren 46

13 Ganzzahlige Darstellungen 53

Aufgaben 58

Stichwortverzeichnis 65

Vorwort

In der *Darstellungstheorie* realisiert man abstrakte mathematische Objekte wie Abbildungen, Vektorräume, Gruppen, Ringe, Graphen etc. durch konkrete Objekte wie Koordinatenvektoren, Matrizen oder Permutationen. In der linearen Algebra ist dies leicht: Jeder n-dimensionale Vektorraum über einem Körper K ist zu K^n isomorph und jede lineare Abbildung entspricht einer Matrix. Aus der Algebra kennt man den Satz von Cayley: jede (endliche) Gruppe ist zu einer Untergruppe einer symmetrischen Gruppe isomorph (jedes Gruppenelement entspricht also einer Permutation). Wir interessieren uns in dieser Vorlesung für Darstellungen von endlichen Gruppen durch Matrizen über einem Körper K. Zu Beginn setzen wir der Einfachheit halber oft $K = \mathbb{C}$ voraus. Man kann dann bereits viele Fragen durch die Spur der entsprechenden Matrizen beantworten. Im Kapitel 7 ersetzen wir $\mathbb{C}$ durch einen Zahlkörper (d. h. eine endliche Körpererweiterung von $\mathbb{Q}$). Anschließend gehen wir zu Körpern positiver Charakteristik über. Hier ist es von Vorteil Moduln anstelle von Darstellungen zu studieren. Im letzten Kapitel betrachten wir Darstellungen über den Ring der ganzen Zahlen (anstelle eines Körpers).

Dieses Skript entstand aus einer einstündigen Vorlesung im Sommersemester 2023 an der Leibniz Universität Hannover. Diese Vorlesung richtet sich hauptsächlich an Bachelor- und Master-Studierende

der Mathematik. Es werden Kenntnisse der Algebra 1 vorausgesetzt. Der erste Teil folgt in etwa meinem Skript zur Charaktertheorie. Nachträglich wurden wie immer einige Dinge verändert und ergänzt. Ich danke Karl Böhlke, Lyon Wolfgang Dorgelo, Leon Eickhoff, Leon Lampe, Claude Sonnet (4.6), Frederik Tscherniak, Tim Wittenberg und Yasin Yilmaz für Fehlerhinweise.

Literatur:

- Sambale, Algebra-Skript, Charaktertheorie-Skript
- 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 Darstellungen

Bemerkung 1.1.

(i) Wir benutzen die üblichen Zahlbereiche $\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

(ii) Stets sei K ein Körper und G eine endliche Gruppe.

Definition 1.2. Sei $V \neq 0$ ein endlich-dimensionaler K-Vektorraum. Eine (K-)*Darstellung* von G auf V ist ein Homomorphismus $\Delta\colon G \to \mathrm{GL}(V)$. Man nennt $\dim V$ den *Grad* von Δ. Ist Δ injektiv, so nennt man Δ *treu*. Durch Wahl einer Basis von V erhält man eine entsprechende *Matrixdarstellung* $\Delta'\colon G \to \mathrm{GL}(n, K)$.

Bemerkung 1.3. Ist eine Darstellung $\Delta\colon G \to \mathrm{GL}(V)$ gegeben, so schreiben wir häufig ${}^g v := \Delta(g)(v)$ für $g \in G$ und $v \in V$. Dies definiert eine Operation von G auf V, d. h. es gilt ${}^1 v = v$ und ${}^{gh} v = {}^g({}^h v)$ für alle $g, h \in G$ und $v \in V$. Zusätzlich gilt die Linearität ${}^g(v + w) = {}^g v + {}^g w$. Umgekehrt entspricht jeder Operation von G auf V ein Homomorphismus $G \to \mathrm{Sym}(V)$. Gilt zudem die Linearität, so handelt es sich um einen Homomorphismus $G \to \mathrm{GL}(V)$, also eine Darstellung. Auf diese Weise entsprechen sich Darstellungen und lineare Operationen.

Beispiel 1.4.

(i) Die *triviale* (Matrix-)Darstellung $\mathbb{1}_G\colon G \to \mathrm{GL}(1, K) = K^\times = K \setminus \{0\}$ ist gegeben durch $\mathbb{1}_G(g) = 1$ für $g \in G$.

(ii) Für $n \in \mathbb{N}$ sei S_n die symmetrische Gruppe vom Grad n. Die Abbildung $\mathrm{sgn}\colon S_n \to \mathbb{Q}^\times$, $g \mapsto \mathrm{sgn}(g)$ ist eine $\mathbb{Q}$-Darstellung vom Grad 1. Der Kern von sgn ist die alternierende Gruppe A_n.

(iii) Sei

$$D_{2n} = \langle \sigma, \tau : \sigma^n = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$$

die *Diedergruppe* der Ordnung $2n$, also die Symmetriegruppe des regelmäßigen n-Ecks. Dann definiert

$$\Delta(\sigma) := \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}, \qquad \Delta(\tau) := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

eine $\mathbb{R}$-Matrixdarstellung vom Grad 2 ($\Delta(\sigma)$ ist die Drehung um $2\pi/n$ und $\Delta(\tau)$ die Spiegelung an der x-Achse).

(iv) Für zwei K-Darstellungen $\Delta\colon G \to \mathrm{GL}(V)$ und $\Gamma\colon G \to \mathrm{GL}(W)$ ist auch $\Delta \oplus \Gamma\colon G \to \mathrm{GL}(V \times W)$ eine K-Darstellung mit ${}^g(v, w) := ({}^g v, {}^g w)$ für $g \in G$, $v \in V$ und $w \in W$. Bzgl. einer geeigneten Basis hat die entsprechende Matrixdarstellung Blockdiagonalgestalt:

$$(\Delta \oplus \Gamma)'(g) = \begin{pmatrix} \Delta'(g) & 0 \\ 0 & \Gamma'(g) \end{pmatrix}.$$

(v) Ist $\Delta\colon H \to \mathrm{GL}(V)$ eine Darstellung und $f\colon G \to H$ ein Gruppenhomomorphismus, so ist auch $\Delta \circ f\colon G \to \mathrm{GL}(V)$ eine Darstellung. Ist $G \leq H$ und f die Inklusionsabbildung, so erhält man die *Einschränkung* (*Restriktion*) $\Delta_G\colon G \to \mathrm{GL}(V)$, $g \mapsto \Delta(g)$. Ist $H = G/N$ mit $N \trianglelefteq G$ und $f\colon G \to H$, $g \mapsto gN$ der kanonische Epimorphismus, so nennt man $\Delta \circ f$ die *Inflation* von Δ.

(vi) Ist $\Delta\colon G \to \mathrm{GL}(V)$ eine Darstellung und $N \trianglelefteq G$ mit $N \subseteq \mathrm{Ker}(\Delta)$, so erhält man durch *Deflation* eine wohldefinierte Darstellung $\widehat{\Delta}\colon G/N \to \mathrm{GL}(V)$, $gN \mapsto \Delta(g)$. Insbesondere ist $\widehat{\Delta}\colon G/\mathrm{Ker}(\Delta) \to \mathrm{GL}(V)$ eine treue Darstellung.

(vii) Inflation und Deflation sind offenbar zueinander invers.

Definition 1.5. Zwei Darstellungen $\Delta\colon G \to \mathrm{GL}(V)$ und $\Gamma\colon G \to \mathrm{GL}(W)$ heißen *ähnlich*, falls ein Isomorphismus $f\colon V \to W$ mit $f \circ \Delta(g) = \Gamma(g) \circ f$ für alle $g \in G$ existiert. Gegebenenfalls ist das folgende Diagramm kommutativ:

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

Entsprechend sind zwei Matrixdarstellungen $\Delta\colon G \to \mathrm{GL}(n, K)$ und $\Gamma\colon G \to \mathrm{GL}(m, K)$ ähnlich, falls $n = m$ ist und ein $A \in \mathrm{GL}(n, K)$ existiert mit $A\Delta(g) = \Gamma(g)A$ für alle $g \in G$.

Bemerkung 1.6.

(i) Ähnlichkeit ist eine Äquivalenzrelation. Ähnliche Darstellungen haben den gleichen Grad. Man interessiert sich in der Regel nur für Darstellungen bis auf Ähnlichkeit (so wie für Gruppen bis auf Isomorphie).

(ii) In der linearen Algebra zeigt man, dass zwei quadratische Matrizen A, B genau dann die gleiche Abbildung beschreiben, wenn es eine invertierbare Matrix T mit $AT = TB$ gibt. Somit sind zwei Matrixdarstellungen, die der gleichen Darstellung von G entsprechen, stets ähnlich.

(iii) Die Ähnlichkeitsklassen von Darstellungen und Matrixdarstellungen entsprechen sich offenbar. Wir werden daher im Folgenden Darstellungen oft mit ihren entsprechenden Matrixdarstellungen identifizieren.

Definition 1.7. Sei $\Delta\colon G \to \mathrm{GL}(V)$ eine Darstellung. Ein Unterraum $U \leq V$ heißt Δ-*invariant*, falls ${}^gU := \{{}^gu : u \in U\} = U$ für alle $g \in G$ gilt. Gegebenenfalls ist $\Delta'\colon G \to \mathrm{GL}(U)$, $g \mapsto \Delta(g)_{|U}$ auch eine Darstellung. Sind 0 und V die einzigen Δ-invarianten Untervektorräume, so ist Δ *irreduzibel*. Anderenfalls ist Δ *reduzibel*.

Beispiel 1.8.

(i) Darstellungen vom Grad 1 sind offensichtlich irreduzibel.

(ii) Inflation und Deflation irreduzibler Darstellungen sind wieder irreduzibel (die Bilder ändern sich nicht).

Satz 1.9 (Maschke)**.** *Sei* $\operatorname{char} K \nmid |G|$ (*z. B.* $\operatorname{char} K = 0$). *Sei* $\Delta\colon G \to \mathrm{GL}(V)$ *eine Darstellung und* $U \leq V$ Δ*-invariant. Dann besitzt* U *ein* Δ*-invariantes Komplement* $W \leq V$*, d. h.* $V = U \oplus W$*.*

Beweis. Wir wählen zunächst einen beliebigen Unterraum X von V mit $V = U \oplus X$ (Basisergänzungssatz) und bezeichnen mit $\pi\colon V \to V$, $u + x \mapsto u$ die Projektion auf U. Wegen $\operatorname{char} K \nmid |G|$ ist

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

wohldefiniert und $W := \mathrm{Ker}(\rho) \leq V$. Für $u \in U$ ist

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

Insbesondere ist $U \cap W = 0$. Für $v \in V$ ist $\rho(v) \in U$, also

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

d. h. $v - \rho(v) \in W$ und $v = \rho(v) + (v - \rho(v)) \in U + W$. Folglich ist $V = U \oplus W$. Für $w \in W$ und $g \in G$ gilt

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

$$= {}^g\rho(w) = {}^g0 = 0,$$

also ${}^gw \in \mathrm{Ker}(\rho) = W$. Somit ist W Δ-invariant. □

Bemerkung 1.10.

(i) Sei Δ eine Darstellung auf V, und sei $V = U \oplus W$ eine Δ-invariante Zerlegung. Dies liefert Teildarstellungen $\Gamma_U\colon G \to \mathrm{GL}(U)$, $g \mapsto \Delta(g)_{|U}$ und $\Gamma_W\colon G \to \mathrm{GL}(W)$, $g \mapsto \Delta(g)_{|W}$. Durch Wahl einer geeigneten Basis von V hat Δ dann die Form

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

für alle $g \in G$. Somit ist $\Delta = \Gamma_U \oplus \Gamma_W$. Im Fall $\operatorname{char} K \nmid |G|$ lässt sich somit jede Darstellung als direkte Summe irreduzibler Darstellungen schreiben.

(ii) Ist $\operatorname{char} K$ ein Teiler von $|G|$, so gibt es Darstellungen, für die der Satz von Maschke falsch ist (Aufgabe 1).

Lemma 1.11 (SCHURs Lemma)**.** *Seien $\Delta\colon G \to \mathrm{GL}(n, K)$, $\Gamma\colon G \to \mathrm{GL}(m, K)$ irreduzible Matrixdarstellungen und $0 \neq A \in K^{n\times m}$ mit $A\Gamma(g) = \Delta(g)A$ für alle $g \in G$. Dann gilt:*

(i) $n = m$ und A ist invertierbar. Insbesondere sind Δ und Γ ähnlich.

(ii) Ist $\Delta = \Gamma$ und K algebraisch abgeschlossen, so gilt $A = \lambda 1_n$ für ein $\lambda \in K^\times$.

Beweis.

(i) Für $g \in G$ und $v \in \operatorname{Ker}(A)$ ist
$$A\Gamma(g)v = \Delta(g)Av = 0,$$
also $\Gamma(g)v \in \operatorname{Ker}(A)$. Daher ist $\operatorname{Ker}(A)$ ein Γ-invarianter Unterraum von K^m. Analog ist $\operatorname{Bild}(A)$ ein Δ-invarianter Unterraum von K^n. Aus der Irreduzibilität von Δ und Γ folgt $\operatorname{Ker}(A) = 0$ und $\operatorname{Bild}(A) = K^n$. Daher ist A invertierbar und $n = m$.

(ii) Da K algebraisch abgeschlossen ist, besitzt A einen Eigenwert λ. Dann gilt $(A - \lambda 1_n)\Gamma(g) = A\Gamma(g) - \lambda\Gamma(g) = \Delta(g)(A - \lambda 1_n)$ für alle $g \in G$. Da $A - \lambda 1_n$ nicht invertierbar ist, folgt $A - \lambda 1_n = 0$ aus (i). □

2 Charaktere

Bemerkung 2.1. In den nächsten Kapiteln sei stets $K = \mathbb{C}$. Wegen $\operatorname{char} K = 0 \nmid |G|$ lässt sich der Satz von Maschke anwenden. Nach dem Fundamentalsatz der Algebra ist $\mathbb{C}$ algebraisch abgeschlossen. Also kann man auch den zweiten Teil von Schurs Lemma benutzen.

Satz 2.2. *Jede irreduzible Darstellung einer abelschen Gruppe hat Grad* 1.

Beweis. Sei G abelsch und $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ eine irreduzible Matrixdarstellung von G. Sei $g \in G$ fest. Für alle $h \in G$ gilt dann $\Delta(g)\Delta(h) = \Delta(gh) = \Delta(hg) = \Delta(h)\Delta(g)$. Nach Schurs Lemma ist also $\Delta(g) = \lambda_g 1_n$ für ein $\lambda_g \in \mathbb{C}$. Insbesondere ist $\mathbb{C}(1, 0, \ldots, 0)$ ein Δ-invarianter Unterraum von $\mathbb{C}^n$. Da Δ irreduzibel ist, folgt $n = 1$. □

Definition 2.3. Sei $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ eine Matrixdarstellung. Die Abbildung
$$\chi\colon G \to \mathbb{C}, \qquad g \mapsto \operatorname{tr} \Delta(g)$$
heißt *Charakter* von Δ (und von G). Dabei ist $\chi(1) = \operatorname{tr} \Delta(1) = \operatorname{tr} 1_n = n$ der *Grad* von χ (und von Δ). Ist Δ irreduzibel (treu, …), so bezeichnet man auch χ als *irreduzibel* (*treu*, …). Die Menge der irreduziblen Charaktere von G bezeichnen wir mit $\operatorname{Irr}(G)$. Achtung: Treue Charaktere sind im Allgemeinen nicht injektiv (siehe Bemerkung 2.15).

Bemerkung 2.4. Für $A = (a_{ij}) \in K^{n\times m}$ und $B = (b_{ij}) \in K^{m\times n}$ gilt

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

Lemma 2.5. *Ähnliche Matrixdarstellungen haben den gleichen Charakter.*

Beweis. Seien $\Delta\colon G \to \mathrm{GL}(n,\mathbb{C})$ und $\Gamma\colon G \to \mathrm{GL}(n,\mathbb{C})$ ähnliche Matrixdarstellungen. Dann existiert ein $A \in \mathrm{GL}(n,\mathbb{C})$ mit $\Delta(g)A = A\Gamma(g)$ für alle $g \in G$. Aus (2.1) folgt

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

für alle $g \in G$. □

Bemerkung 2.6.

(i) Charaktere wurden ursprünglich von Dirichlet für prime Restklassengruppen $(\mathbb{Z}/n\mathbb{Z})^\times$ eingeführt, um damit seinen Primzahlsatz zu beweisen.[1]

(ii) Charaktere sind die „Schatten" von Darstellungen, d. h. man verliert einerseits Information, indem man die n^2 Einträge einer Matrix durch einen einzigen Wert ersetzt, aber andererseits bleibt genug Information, um Eigenschaften der Gruppe abzulesen.

(iii) Ist $\Delta\colon G \to \mathrm{GL}(V)$ eine Darstellung, so kann man Δ einen Charakter zuordnen, indem man eine entsprechende Matrixdarstellung wählt. Wegen Lemma 2.5 kommt es dabei nicht auf die Wahl der Basis von V an.

(iv) Offenbar stimmen Darstellungen vom Grad 1 mit ihrem Charakter überein. Man nennt diese Charaktere *linear*. Insbesondere gibt es den *trivialen* Charakter $\mathbb{1}_G\colon G \to \mathbb{C}$ mit $\mathbb{1}_G(g) = 1$ für $g \in G$.

(v) Für jede Darstellung $\Delta\colon G \to \mathrm{GL}(V)$ ist $\det\Delta\colon G \to \mathbb{C}$, $g \mapsto \det\Delta(g)$ ein linearer Charakter. Da ähnliche Matrizen die gleiche Determinante haben, hängt $\det\Delta$ nur vom Charakter χ von Δ ab. Man kann daher $\det\chi := \det\Delta$ definieren.

(vi) Sind Δ und Γ Darstellungen mit Charakter χ bzw. ψ, so hat $\Delta\oplus\Gamma$ den Charakter $\chi+\psi$. Summen von Charakteren sind also wieder Charaktere.

Definition 2.7.

(i) Man nennt $g, h \in G$ *konjugiert*, falls ein $x \in G$ mit $xgx^{-1} = h$ existiert. Die zu g konjugierten Elemente bilden die *Konjugationsklasse*

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

von g. Die Menge der Konjugationsklassen von G sei $\mathrm{Cl}(G)$. Man nennt $k(G) := |\mathrm{Cl}(G)|$ die *Klassenzahl* von G. Sei

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

der *Zentralisator* von g in G. In der Algebra zeigt man $|\mathrm{Cl}(g)| = |G : \mathrm{C}_G(g)|$.

[1] Siehe Zahlentheorie-Skript

(ii) Bekanntlich wird die Menge aller Abbildungen $G \to \mathbb{C}$ durch

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

für $\alpha, \beta \colon G \to \mathbb{C}$, $g \in G$, $\lambda \in \mathbb{C}$ zu einem $\mathbb{C}$-Vektorraum der Dimension $|G|$. Eine Abbildung $\alpha \colon G \to \mathbb{C}$ heißt *Klassenfunktion*, falls $\alpha(g) = \alpha(hgh^{-1})$ für alle $g, h \in G$ gilt. Klassenfunktionen sind also konstant auf Konjugationsklassen. Der Unterraum $\mathrm{CF}(G)$ aller Klassenfunktionen hat offenbar Dimension $|\mathrm{Cl}(G)|$.

Lemma 2.8. *Die Charaktere von G sind Klassenfunktionen. Insbesondere ist* $\mathrm{Irr}(G) \subseteq \mathrm{CF}(G)$.

Beweis. Sei $\Delta \colon G \to \mathrm{GL}(V)$ eine Darstellung mit Charakter χ. Für $g, h \in G$ ist

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

Definition 2.9. Offenbar definiert

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

ein Skalarprodukt des $\mathbb{C}$-Vektorraums $\mathrm{CF}(G)$.

Bemerkung 2.10.

(i) Sind $g_1, \ldots, g_k \in G$ Repräsentanten für die Konjugationsklassen von G, so gilt

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

Bis auf die Faktoren $|\mathrm{C}_G(g_i)|^{-1}$ entspricht $(\chi, \psi)_G$ also dem Standardskalarprodukt von $\mathbb{C}^k$.

(ii) Für Charaktere χ, ψ von G ist nach Aufgabe 5 auch

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

Lemma 2.11 (Schur-Relationen)**.** *Seien $\Delta \colon G \to \mathrm{GL}(n, \mathbb{C})$, $\Gamma \colon G \to \mathrm{GL}(m, \mathbb{C})$ irreduzible Matrixdarstellungen mit $\Delta(g) = (\lambda_{ij}(g))$ und $\Gamma(g) = (\theta_{ij}(g))$ für $g \in G$.*

(i) Sind Δ und Γ nicht ähnlich, so ist

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

für alle i, j.

(ii) Es ist

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

Beweis.

(i) Sei $E_{ij} \in \mathbb{C}^{n\times m}$ die Matrix mit einer 1 an Position (i,j) und sonst nur Nullen. Wir setzen

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

Für $h \in G$ ist dann $\Delta(h)F_{ij}\Gamma(h^{-1}) = F_{ij}$, d. h. $\Delta(h)F_{ij} = F_{ij}\Gamma(h)$. Sind Δ und Γ nicht ähnlich, so folgt $F_{ij} = 0$ aus Schurs Lemma. Insbesondere ist F_{ij} an der Position (i,j) gleich 0, d. h. (i) gilt.

(ii) Sei nun $\Delta = \Gamma$. Nach Schur ist $F_{ij} = \rho_{ij} \cdot 1_n$ für ein $\rho_{ij} \in \mathbb{C}$. Für den Eintrag von F_{ij} an Position $(1,1)$ gilt dann

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

Mit $\rho := \rho_{11}\,(= \rho_{ii})$ folgt

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

wegen $\Delta(g)\Delta(g^{-1}) = 1_n$ für $g \in G$. Nun ergibt sich (ii) durch den Eintrag von F_{ij} an Position (i,j). □

Satz 2.12 (Erste Orthogonalitätsrelation)**.** *Für $\chi, \psi \in \mathrm{Irr}(G)$ gilt*

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

Beweis. Seien Δ und Γ irreduzible Darstellungen von G mit Charakter χ bzw. ψ. Sei zunächst $\chi \neq \psi$. Nach Lemma 2.5 sind dann Δ und Γ nicht ähnlich. Wir schreiben $\Delta(g) = (\lambda_{ij}(g))$ und $\Gamma(g) = (\theta_{ij}(g))$ für $g \in G$. Dann ist $\chi(g) = \sum \lambda_{ii}(g)$ und $\psi(g) = \sum \theta_{ii}(g)$. Nach Lemma 2.11 ist

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

Analog gilt

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

Bemerkung 2.13. Aus Satz 2.12 folgt leicht, dass $\mathrm{Irr}(G)$ eine linear unabhängige Teilmenge von $\mathrm{CF}(G)$ ist. Insbesondere ist $|\mathrm{Irr}(G)| \leq \dim_{\mathbb{C}} \mathrm{CF}(G) = |\mathrm{Cl}(G)| \leq |G| < \infty$.

Satz 2.14. *Zwei Darstellungen sind genau dann ähnlich, wenn sie den gleichen Charakter haben.*

Beweis. Eine Richtung ist Lemma 2.5. Seien nun Δ und Γ Darstellungen mit dem gleichen Charakter χ. Wir schreiben $\Delta = \bigoplus_{i=1}^{n} \Delta_i$ und $\Gamma = \bigoplus_{i=1}^{m} \Gamma_i$ als Summen von irreduziblen Darstellungen. Dann zerlegt sich auch χ in

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

Nach Bemerkung 2.13 ist $n = m$ und $\chi_{\Delta_i} = \chi_{\Gamma_i}$ für $i = 1, \ldots, n$ bei geeigneter Nummerierung. Wären Δ_i und Γ_i nicht ähnlich, so erhält man den Widerspruch $1 = (\chi_{\Delta_i}, \chi_{\Gamma_i})_G = 0$ wie im Beweis von Satz 2.12. Sei also $A_i \in \mathrm{GL}(\chi_{\Delta_i}(1), \mathbb{C})$ mit $A_i \Delta_i(g) = \Gamma_i(g) A_i$ für alle $g \in G$. Für

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

gilt dann offenbar $A\Delta(g) = \Gamma(g)A$ für alle $g \in G$, d. h. Δ und Γ sind ähnlich. □

Bemerkung 2.15.

(i) Sei ρ der reguläre Charakter von G. Nach Aufgabe 1 gilt

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

Für $\chi \in \mathrm{Irr}(G)$ ist daher

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

Es folgt $\rho = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi$ und $\boxed{|G| = \rho(1) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2.}$

(ii) Seien $C, D, E \in \mathrm{Cl}(G)$, $e \in E$ und $g \in G$. Dann ist die Abbildung $(c, d) \mapsto (gcg^{-1}, gdg^{-1})$ eine Bijektion zwischen $\{(c, d) \in C \times D : cd = e\}$ und $\{(c, d) \in C \times D : cd = geg^{-1}\}$. Daher hängt die *Klassenmultiplikationskonstante*

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

nicht von der Wahl von $e \in E$ ab.

Lemma 2.16. *Für eine irreduzible Darstellung Δ mit Charakter χ und $g \in C \in \mathrm{Cl}(G)$ gilt*

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

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

Beweis. Sei $A := \sum_{x \in C} \Delta(x)$. Für $y \in G$ gilt $\Delta(y) A \Delta(y^{-1}) = \sum_{x \in C} \Delta(yxy^{-1}) = A$. Aus Schurs Lemma folgt $A = \omega_\Delta(C) \,\mathrm{id}$ für ein $\omega_\Delta(C) \in \mathbb{C}$. Weiter ist

$$\omega_\Delta(C)\chi(1) = \mathrm{tr}\, A = \sum_{x \in C} \chi(x) = |C|\chi(g).$$ □

Satz 2.17 (Zweite Orthogonalitätsrelation)**.** *Für $g, h \in G$ gilt*

$$\boxed{\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = \begin{cases} |\mathrm{C}_G(g)| & \text{falls } g \text{ und } h \text{ konjugiert sind,} \\ 0 & \text{sonst.} \end{cases}}$$

Beweis. Seien $C, D \in \mathrm{Cl}(G)$ mit $g \in C$ und $h^{-1} \in D$. Sei $\Delta\colon G \to \mathrm{GL}(n, \mathbb{C})$ eine irreduzible Matrixdarstellung mit Charakter χ. Nach Lemma 2.16 gilt

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

Aus der Definition von ω_χ erhält man

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

wobei jeweils $e \in E$ gewählt ist. Sei ρ der reguläre Charakter von G. Summieren über χ liefert

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

Offenbar ist $\mathrm{Cl}(h) = D^{-1} = \{d^{-1} : d \in D\}$. Sind g und h nicht konjugiert, so ist $C \cap D^{-1} = \varnothing$ und $\gamma_{CD\{1\}} = 0$. Anderenfalls ist $\gamma_{CD\{1\}} = |C| = |D|$ und die Behauptung folgt aus $\frac{|G|}{|C|} = |\mathrm{C}_G(g)|$. □

Satz 2.18. $\mathrm{Irr}(G)$ *ist eine Orthonormalbasis von* $\mathrm{CF}(G)$*. Insbesondere ist* $\boxed{k(G) = |\mathrm{Irr}(G)|.}$

Beweis. Wir wissen bereits, dass $\mathrm{Irr}(G)$ linear unabhängig ist (Bemerkung 2.13). Nach der zweiten Orthogonalitätsrelation ist für $g \in C \in \mathrm{Cl}(G)$ andererseits

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

die charakteristische Funktion auf C (d. h. $\varphi_C(x)$ ist 1, falls $x \in C$, und sonst 0). Da die charakteristischen Funktionen eine Basis von $\mathrm{CF}(G)$ bilden, ist $\mathrm{Irr}(G)$ auch ein Erzeugendensystem. Die Orthonormalität folgt aus der ersten Orthogonalitätsrelation. □

Bemerkung 2.19.

(i) Jede Klassenfunktion $f \in \mathrm{CF}(G)$ lässt sich also eindeutig in der Form

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

mit $a_\chi \in \mathbb{C}$ schreiben. Genau dann ist f ein Charakter, wenn $a_\chi \in \mathbb{N}_0$ für alle $\chi \in \mathrm{Irr}(G)$ und $a_\psi > 0$ für mindestens ein $\psi \in \mathrm{Irr}(G)$ gilt (Bemerkung 2.6(vi)). Ist $a_\chi = (f, \chi)_G > 0$, so nennt man χ einen *irreduziblen Bestandteil* von f mit *Vielfachheit* a_χ. Außerdem gilt $(f, f)_G = \sum_\chi a_\chi^2$. Insbesondere ist ein Charakter χ genau dann irreduzibel, falls $(\chi, \chi)_G = 1$ gilt.

(ii) Im Allgemeinen kennt man keine kanonische Bijektion zwischen $\mathrm{Cl}(G)$ und $\mathrm{Irr}(G)$.

3 Charaktertafeln

Bemerkung 3.1. Seien $g_1, \dots, g_k \in G$ Repräsentanten für die Konjugationsklassen von G, und sei $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_k\}$. Die $k \times k$-Matrix $C(G) := (\chi_i(g_j))_{i,j}$ heißt *Charaktertafel* von G. Natürlich hängt C von der Reihenfolge der Elemente und Charaktere ab. In der Regel wählt man $g_1 = 1$, $\chi_1 = \mathbb{1}_G$ und $\chi_1(1) \leq \chi_2(1) \leq \ldots \leq \chi_k(1)$. In diesem Kapitel wollen wir C für einige Gruppen berechnen. Die erste Orthogonalitätsrelation lässt sich in der Form

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

schreiben (siehe (2.2)). Dies betrifft also die Zeilen von C. Die zweite Orthogonalitätsrelation besagt, dass die Spalten von C paarweise orthogonal bzgl. des Standardskalarprodukts von $\mathbb{C}^k$ sind. Insbesondere ist C invertierbar.

Definition 3.2. Für Matrizen $A = (a_{ij}) \in K^{n\times n}$ und $B \in K^{m\times m}$ nennt man

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

das *Kroneckerprodukt* von A und B.

Lemma 3.3. *Für $A, C \in K^{n\times n}$ und $B, D \in K^{m\times m}$ gilt* $\boxed{(A \otimes B)(C \otimes D) = AC \otimes BD.}$

Beweis.

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

Satz 3.4. *Seien $\Delta\colon G \to \mathrm{GL}(n,\mathbb{C})$ und $\Gamma\colon H \to \mathrm{GL}(m,\mathbb{C})$ Darstellungen von Gruppen G und H mit Charakteren χ bzw. ψ. Dann ist $\Delta \otimes \Gamma\colon G \times H \to \mathrm{GL}(nm,\mathbb{C})$, $(g,h) \mapsto \Delta(g) \otimes \Gamma(h)$ eine Darstellung von $G \times H$ mit Charakter $(\chi \times \psi)(g,h) := \chi(g)\psi(h)$ für $g \in G$, $h \in H$.*

Beweis. Für $g_1, g_2 \in G$ und $h_1, h_2 \in H$ gilt

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

Daher ist $\Delta \otimes \Gamma$ eine Darstellung von $G \times H$. Sei $\Delta(g) = (a_{ij})$. Dann gilt

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

Satz 3.5. *Für endliche Gruppen G, H ist* $\mathrm{Irr}(G \times H) = \{\chi \times \psi : \chi \in \mathrm{Irr}(G), \psi \in \mathrm{Irr}(H)\}$.

Beweis. Sei $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_n\}$ und $\mathrm{Irr}(H) = \{\psi_1, \dots, \psi_m\}$. Dann ist

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

Also sind die Charaktere $\chi_i \times \psi_j$ irreduzibel und paarweise verschieden. Wegen

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

hat man alle irreduziblen Charaktere von $G \times H$ gefunden. □

Folgerung 3.6. *Sind χ und ψ Charaktere von G, so auch $\chi\psi$ mit $(\chi\psi)(g) := \chi(g)\psi(g)$ für $g \in G$.*

Beweis. Seien Δ und Γ Darstellungen von G mit Charakter χ bzw. ψ. Dann ist $G \to G \times G \to \mathrm{GL}(\chi(1)\psi(1), \mathbb{C})$, $g \mapsto (g, g) \mapsto (\Delta \otimes \Gamma)(g, g)$ eine Darstellung von G mit Charakter $\chi\psi$. □

Bemerkung 3.7. Für $\chi, \psi \in \mathrm{Irr}(G)$ ist $\chi\psi$ nicht unbedingt irreduzibel (wähle $\chi(1) = \psi(1) > 1$ maximal).

Bemerkung 3.8.

(i) Seien $C(G) \in \mathbb{C}^{n\times n}$ und $C(H) \in \mathbb{C}^{m\times m}$ die Charaktertafeln von G bzw. H. Dann ist $C(G) \otimes C(H)$ die Charaktertafel von $G \times H$ bei geeigneter Anordnung.

(ii) Sei G zyklisch der Ordnung n (wir schreiben $G \cong C_n$). Nach Aufgabe 2 ist die Charaktertafel von G durch $(e^{\frac{2\pi ikl}{n}})_{k,l=0}^{n-1}$ gegeben ($\mathrm{i} = \sqrt{-1}$). Aus der Algebra weiß man, dass jede abelsche Gruppe G das direkte Produkt zyklischer Gruppen ist. Mit Satz 3.5 lässt sich also leicht die Charaktertafel von G berechnen.

Beispiel 3.9. Sei $G := \{1, x, y, z\,(= xy)\} \cong C_2 \times C_2 = C_2^2$ die Kleinsche Vierergruppe mit $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_4\}$. Dann ist

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

die Charaktertafel von G.

Definition 3.10. Für $x, y \in G$ ist $[x, y] := xyx^{-1}y^{-1}$ der *Kommutator* von x und y. Sei

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

die *Kommutatorgruppe* von G.

Bemerkung 3.11. Für $\alpha \in \mathrm{Aut}(G)$ und $x, y \in G$ ist offenbar $\alpha([x,y]) = [\alpha(x), \alpha(y)] \in G'$. Insbesondere ist $G' \trianglelefteq G$ (wähle $\alpha \in \mathrm{Inn}(G)$). Für $xG', yG' \in G/G'$ ist

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

d. h. G/G' ist abelsch. Ist umgekehrt $N \trianglelefteq G$ mit G/N abelsch, so gilt $[x,y]N = xNyN(xN)^{-1}(yN)^{-1} = N$ für $x, y \in G$, d. h. $G' \subseteq N$. Daher ist G' der kleinste Normalteiler mit abelscher Faktorgruppe. Der nächste Satz verallgemeinert Satz 2.2.

Satz 3.12. *Die linearen Charaktere von G sind die Inflationen von* $\mathrm{Irr}(G/G')$.

Beweis. Jeder lineare Charakter ist ein Homomorphismus $\chi\colon G \to \mathbb{C}^\times$. Insbesondere ist $G/\mathrm{Ker}(\chi)$ als Untergruppe von $\mathbb{C}^\times$ abelsch, d. h. $G' \subseteq \mathrm{Ker}(\chi)$. Deflation liefert also ein $\psi \in \mathrm{Irr}(G/G')$ und χ ist die Inflation von ψ. Umgekehrt hat die Inflation jedes $\chi \in \mathrm{Irr}(G/G')$ Grad 1 wegen Satz 2.2. □

Beispiel 3.13. Die alternierende Gruppe A_4 besitzt mit der Kleinschen Vierergruppe

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

eine normale 2-Sylowgruppe. Die drei Involutionen (Elemente der Ordnung 2) in V_4 sind durch einen 3-Zyklus konjugiert. Nach Sylow ist jedes Element in $A_4 \setminus V_4$ zu $x := (1,2,3)$ oder x^{-1} konjugiert. Andererseits können x und x^{-1} nicht konjugiert sein, denn sonst wären auch die entsprechenden Nebenklassen in der abelschen Gruppe $A_4/V_4 \cong C_3$ konjugiert. Also sind 1, $(1,2)(3,4)$, $(1,2,3)$ und $(1,3,2)$ Repräsentanten für die Konjugationsklassen von A_4. Durch Inflation von A_4/V_4 erhält man drei lineare Charaktere χ_1, χ_2, χ_3. Für den verbleibenden Charakter χ_4 gilt

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

also $\chi_4(1) = 3$. Die fehlenden Werte von χ_4 ergeben sich aus der zweiten Orthogonalitätsrelation:

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. *Sei $g \in G$ der Ordnung k. Für jede Darstellung Δ von G mit Charakter χ gilt*

(i) $\chi(g)$ *ist die Summe von* $\chi(1)$ *vielen k-ten Einheitswurzeln.*

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

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

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

Beweis.

(i) Sei $n := \chi(1)$, und seien $\epsilon_1, \ldots, \epsilon_n \in \mathbb{C}$ die Eigenwerte von $\Delta(g)$ (mit Vielfachheiten). Wegen $(\Delta(g))^k = \Delta(g^k) = \Delta(1) = 1_n$ sind die ϵ_i k-te Einheitswurzeln und $\chi(g) = \epsilon_1 + \ldots + \epsilon_n$.

(ii) Wir wenden die Cauchy-Schwarz-Ungleichung auf die Vektoren $v := (\epsilon_1, \ldots, \epsilon_n)$ und $w := (1, \ldots, 1)$ an:

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

(iii) Gilt Gleichheit in (3.1), so sind v und w linear abhängig und es folgt $\epsilon := \epsilon_1 = \epsilon_2 = \ldots = \epsilon_n$. Da $\Delta(g)$ diagonalisierbar ist (Aufgabe 4), ist die geometrische Vielfachheit des Eigenwerts ϵ gleich n, d. h. $\Delta(g) = \epsilon\,\mathrm{id}$. Ist umgekehrt $\Delta(g) \in \mathbb{C}^\times\,\mathrm{id}$, so folgt sicher $|\chi(g)| = \chi(1)$.

(iv) Ist sogar $\chi(g) = \chi(1)$, so ist offensichtlich $\epsilon = 1$ und $g \in \mathrm{Ker}(\Delta)$. Die Umkehrung ist hier auch klar. □

Definition 3.15. Für eine Darstellung Δ mit Charakter χ setzen wir $\mathrm{Ker}(\chi) := \mathrm{Ker}(\Delta)$ und

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

Man nennt $\mathrm{Z}(\chi)$ das *Zentrum* von χ (bzw. Δ).

Beispiel 3.16.

(i) Ist $g \in G$ eine Involution und χ ein Charakter von G, so gilt $\chi(g) \in \mathbb{Z}$ und $\chi(g) \equiv \chi(1) \pmod 2$ nach Lemma 3.14(i).

(ii) Sei Δ eine Darstellung von G mit Charakter χ und Grad n. Für $g \in G$ und $z \in \mathrm{Z}(\chi)$ gilt dann

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

Dies ist nützlich, um Zeilen der Charaktertafel zu vervollständigen. Aufgabe 6 liefert eine duale Aussage für die Spalten von $C(G)$.

Satz 3.17. *Für jeden Charakter χ von G sind* $\mathrm{Ker}(\chi)$ *und* $\mathrm{Z}(\chi)$ *Normalteiler von G. Dabei ist* $\mathrm{Ker}(\chi) \leq \mathrm{Z}(\chi)$ *und* $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi)$ *ist zyklisch.*

Beweis. Sicher ist $\mathrm{Ker}(\chi) \trianglelefteq G$ und $\mathrm{Ker}(\chi) \subseteq \mathrm{Z}(\chi)$. Sei $\Delta\colon G \to \mathrm{GL}(V)$ eine Darstellung mit Charakter χ. Wegen $\mathbb{C}^\times\,\mathrm{id}_V \trianglelefteq \mathrm{GL}(V)$ ist $\mathrm{Z}(\chi) = \Delta^{-1}(\mathbb{C}^\times\,\mathrm{id}_V) \trianglelefteq G$. Nach dem Homomorphiesatz ist außerdem $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi)$ zu einer endlichen Untergruppe H von $\mathbb{C}^\times\,\mathrm{id}_V \cong \mathbb{C}^\times$ isomorph. Offenbar besteht H genau aus den $|H|$-ten Einheitswurzeln und ist daher zyklisch. □

Bemerkung 3.18.

(i) Auf diese Weise kann man häufig Normalteiler konstruieren, denn jeder Normalteiler ist Kern eines Charakters (Aufgabe 10).

(ii) Sei $\mathrm{Cl}(G) = \{K_1, \ldots, K_k\}$, $g_i \in K_i$ und $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$. Dann unterscheidet sich die Matrix $\Omega := (\omega_{\chi_i}(K_j))_{i,j}$ von der Charaktertafel $C(G)$ nur durch Skalarmultiplikation von Zeilen und Spalten. Mit $C(G)$ ist daher auch Ω invertierbar.

Satz 3.19. *Die Charaktertafel von G lässt sich aus den Klassenmultiplikationskonstanten berechnen.*

Beweis (BURNSIDE-*Algorithmus*). Sei $\mathrm{Cl}(G) = \{K_1, \ldots, K_n\}$ und $\gamma_{ijk} := \gamma_{K_i K_j K_k}$ die Klassenmultiplikationskonstante. Sei $T_i := (\gamma_{ijk})_{j,k} \in \mathbb{Z}^{n\times n}$. Seien $\Delta_1, \ldots, \Delta_n$ die irreduziblen Darstellungen von G und $\omega_i := \omega_{\Delta_i}$ für $i = 1, \ldots, n$. Wie im Beweis von Satz 2.17 gilt

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

für $1 \le i, j, l \le n$. Folglich ist $e_l := (\omega_l(K_k))_k \in \mathbb{C}^n$ ein Eigenvektor von T_i zum Eigenwert $\omega_l(K_i)$.[2] Nach Bemerkung 3.18 ist $\{e_1, \ldots, e_n\}$ eine Basis von $\mathbb{C}^n$. Jeder Eigenraum von T_i wird daher von einigen der e_l aufgespannt. Wir schneiden diese Eigenräume mit den Eigenräumen der T_j für $j \neq i$. Die nicht-trivialen Durchschnitte haben die Form

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

für ein $1 \le l \le n$ (beachte $e_l \in V_l$). Seien $v_l \in V_l$ mit $\sum_{l=1}^n v_l = 0$. Dann folgt

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

für $i = 1, \ldots, n$. Da die Matrix $(\omega_l(K_i))_{l,i}$ nach Bemerkung 3.18 invertierbar ist, ergibt sich $v_1 = \ldots = v_n = 0$ und $\sum_{l=1}^n V_l = \bigoplus_{l=1}^n V_l$. Aus Dimensionsgründen ist $V_l = \langle e_l \rangle$ für $l = 1, \ldots, n$. Wegen $\omega_l(K_1) = 1$ lässt sich e_l aus V_l berechnen. Nach der ersten Orthogonalitätsrelation existiert nur ein Vektor e_l, sagen wir e_1, der nur aus positiven Zahlen besteht. Er gehört zur trivialen Darstellung Δ_1. Daraus ergeben sich die Klassenlängen $|K_i| = \omega_1(K_i)$ für $i = 1, \ldots, n$. Wegen

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

erhält man $\chi_l(1)$ und anschließend auch $\chi_l(g_i) = \frac{\chi_l(1)\omega_l(K_i)}{|K_i|}$ für $g_i \in K_i$. □

Bemerkung 3.20. In der Regel braucht man nicht alle Matrizen T_i, um die Charaktertafel zu berechnen. Hat zum Beispiel $\omega_l(K_i)$ als Eigenwert von T_i Vielfachheit 1, so kann man e_l direkt als Erzeuger des Eigenraums bestimmen. Optimierungen dieser Art führen zum *Dixon-Schneider-Algorithmus*, der in der Praxis häufig benutzt wird.

Satz 3.21. *Sei* $\mathrm{Cl}(G) = \{K_1, \ldots, K_n\}$ *und* $g_i \in K_i$. *Dann gilt*

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

für $1 \le i, j, k \le n$. *Die Klassenmultiplikationskonstanten lassen sich also aus der Charaktertafel bestimmen.*

Beweis. Wie im Beweis von Satz 3.19 ist $\omega_\chi(K_i)\omega_\chi(K_j) = \sum_{k=1}^n \gamma_{ijk}\omega_\chi(K_k)$. Daraus folgt

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

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

[2] Die Eigenwerte von T_i lassen sich zwar berechnen, aber deren Zuordnung zu ω_l ist nicht eindeutig.

4 Ganz-algebraische Zahlen

Definition 4.1. Eine Zahl $\zeta \in \mathbb{C}$ heißt *ganz-algebraisch*, falls sie Nullstelle eines normierten, ganzzahligen Polynoms ist, d. h. es existieren Zahlen $n \in \mathbb{N}$ und $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ mit $\zeta^n + a_{n-1}\zeta^{n-1} + \ldots + a_1\zeta + a_0 = 0$.

Beispiel 4.2.

(i) Ganze Zahlen sind offenbar ganz-algebraisch und ganz-algebraische Zahlen sind algebraisch.

(ii) Einheitswurzeln sind ganz-algebraisch als Nullstellen von Polynomen der Form $X^n - 1$.

Lemma 4.3. *Sind $\alpha, \beta \in \mathbb{C}$ ganz-algebraisch, so auch $\alpha + \beta$ und $\alpha\beta$. (Die ganz-algebraischen Zahlen bilden also einen Ring.)*

Beweis. Wir schreiben

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

mit $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1} \in \mathbb{Z}$. Sei $S := \{\alpha^i\beta^j : i = 0, \ldots, n-1,\ j = 0, \ldots, m-1\}$ und $\gamma := \alpha + \beta$ (bzw. $\alpha\beta$). Für $s \in S$ existieren dann Zahlen $c_{st} \in \mathbb{Z}$ mit $\gamma s = \sum_{t \in S} c_{st} t$ (benutze (4.1)). Für $A := (c_{st})_{s,t \in S} \in \mathbb{Z}^{nm \times nm}$ und $v := (s : s \in S) \in \mathbb{C}^{nm}$ gilt $Av = \gamma v$. Also ist γ Nullstelle des normierten, ganzzahligen, charakteristischen Polynoms $\det(X1_{nm} - A)$. □

Bemerkung 4.4. Ist χ ein Charakter von G, so ist $\chi(g)$ als Summe von Einheitswurzeln (Lemma 3.14) ganz-algebraisch für $g \in G$.

Lemma 4.5. *Ist $\zeta \in \mathbb{Q}$ ganz-algebraisch, so ist $\zeta \in \mathbb{Z}$.*

Beweis. Sei $\zeta = \frac{r}{s}$ mit $r, s \in \mathbb{Z}$ und $\mathrm{ggT}(r, s) = 1$. Nach Voraussetzung existieren $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ mit

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

Umstellen ergibt

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

Also ist $s \mid r^n$. Wegen $\mathrm{ggT}(r, s) = 1$ folgt $s = \pm 1$ und $\zeta \in \mathbb{Z}$. □

Lemma 4.6. *Für $C \in \mathrm{Cl}(G)$ und $\chi \in \mathrm{Irr}(G)$ ist $\omega_\chi(C)$ ganz-algebraisch.*

Beweis. Wie im Beweis von Satz 3.19 gezeigt, ist $\omega_\chi(C)$ ein Eigenwert einer ganzzahligen Matrix T. Also ist $\omega_\chi(C)$ als Nullstelle des normierten, ganzzahligen, charakteristischen Polynoms von T ganz-algebraisch. □

Satz 4.7. *Für $\chi \in \mathrm{Irr}(G)$ ist* $\boxed{\chi(1) \mid |G|.}$

Beweis. Seien $g_1, \dots, g_k \in G$ Repräsentanten für die Konjugationsklassen $K_1, \dots, K_k$ von G. Nach der ersten Orthogonalitätsrelation ist dann

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

Nach Lemma 4.6 ist $\frac{|G|}{\chi(1)}$ ganz-algebraisch. Die Behauptung folgt nun aus Lemma 4.5. □

Beispiel 4.8.

(i) Sei G eine p-Gruppe mit $|G| \geq p^2$. Nach Bemerkung 2.15 und Satz 4.7 gilt

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

und $|G/G'| \geq p^2$. Insbesondere ist G abelsch, falls $|G| = p^2$. Durch Induktion nach $|G|$ erhält man, dass jede p-Gruppe auflösbar ist.

(ii) Nach Algebra ist die alternierende Gruppe $G = A_5$ nicht-abelsch und einfach. Die Permutationen

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

haben paarweise verschiedene Ordnungen und sind daher nicht konjugiert. Nehmen wir an, dass $g := (1,2,3,4,5)$ zu g^2 konjugiert ist. Sei $x \in G$ mit $xgx^{-1} = g^2$. Dann ist $x^2gx^{-2} = g^4 = g^{-1}$ und $x^4gx^{-4} = g$. Daher muss die Ordnung von x durch 4 teilbar sein. Allerdings besitzt G kein Element der Ordnung 4. Somit sind g und g^2 nicht konjugiert und $k(G) \geq 5$. Sei $\mathbb{1}_G \neq \chi \in \mathrm{Irr}(G)$. Wegen $G' = G$ ist $\chi(1) > 1$. Nehmen wir $\chi(1) = 2$ an. Sei $g := (1,2)(3,4) \in G$. Nach Beispiel 3.13 ist χ_{A_4} die Summe von zwei linearen Charakteren. Dann wäre aber $\chi(g) = 2 = \chi(1)$ im Widerspruch zu $\mathrm{Ker}(\chi) = 1$. Also gilt $\chi(1) \geq 3$. Für die Gleichung

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

gibt es nun zwei Lösungen: $60 = 1+3^2+3^2+4^2+5^2 = 1+3^2+3^2+3^2+4^2+4^2$. Angenommen die zweite Zerlegung ist korrekt (d. h. $k(G) = 6$). Für $\chi(1) = 3$ bzw. $\chi(1) = 4$ erhält man $\chi(g) = -1$ bzw. $\chi(g) = 0$ aus Beispiel 3.13. Dies zeigt

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

im Widerspruch zur zweiten Orthogonalitätsrelation. Daher sind $1, 3, 3, 4, 5$ die Charaktergrade von G und $k(G) = 5$. Da es nur einen Charakter vom Grad 4 gibt, muss dieser reell sein. Die Einschränkung nach A_4 liefert somit folgende Einträge der Charaktertafel:

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		

Wir vervollständigen die Tafel in Beispiel 5.8 und Beispiel 7.14.

5 Induzierte Charaktere

Bemerkung 5.1. Für $H \leq G$ und $\varphi \in \mathrm{CF}(G)$ ist offenbar die Einschränkung $\varphi_H \colon H \to \mathbb{C}$ eine Klassenfunktion von H. Wir konstruieren umgekehrt aus $\varphi \in \mathrm{CF}(H)$ eine Klassenfunktion auf G.

Definition 5.2. Für $H \leq G$ und $\varphi \in \mathrm{CF}(H)$ sei

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

Man nennt φ^G die von φ *induzierte* Klassenfunktion.

Satz 5.3. *Für $\varphi \in \mathrm{CF}(H)$ ist $\varphi^G \in \mathrm{CF}(G)$.*

Beweis. Für $x, y \in G$ ist

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

Bemerkung 5.4.

(i) Man sieht leicht, dass die Induktion eine lineare Abbildung von $\mathrm{CF}(H)$ nach $\mathrm{CF}(G)$ ist.

(ii) Ist $|\langle x \rangle|$ kein Teiler von $|H|$, so liegt kein Konjugiertes von x in H und es folgt $\varphi^G(x) = 0$. Für $N \trianglelefteq G$, $\varphi \in \mathrm{CF}(N)$ und $x \in G \setminus N$ gilt ebenso $\varphi^G(x) = 0$.

(iii) Für $H \leq G$, $\varphi \in \mathrm{CF}(H)$ und $x \in G$ gilt

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

Dies ist nützlich für die praktische Berechnung.

Satz 5.5. *Seien $K \leq H \leq G$, $\varphi \in \mathrm{CF}(G)$, $\mu \in \mathrm{CF}(H)$ und $\nu \in \mathrm{CF}(K)$. Dann gilt*

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

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

(iii) $\boxed{(\varphi, \mu^G)_G = (\varphi_H, \mu)_H}$ (FROBENIUS-Reziprozität).

Beweis.

(i) Nach Bemerkung 5.4(iii) gilt

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

für $x \in G$.

(ii) Wie in (i) gilt

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

für $x \in G$.

(iii) Es gilt

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

Bemerkung 5.6. Die Frobenius-Reziprozität besagt, dass Restriktion und Induktion zueinander adjungierte Abbildungen zwischen $\mathrm{CF}(G)$ und $\mathrm{CF}(H)$ sind.

Satz 5.7. *Für jeden Charakter ψ von $H \leq G$ ist ψ^G ein Charakter von G vom Grad $|G:H|\psi(1)$.*

Beweis. Wir schreiben $\psi^G = \sum_{\chi\in\mathrm{Irr}(G)} a_\chi\chi$ mit $a_\chi \in \mathbb{C}$. Dann ist

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

denn χ_H ist ein Charakter von H. Also ist ψ^G ein Charakter von G. Nach Definition ist

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

Beispiel 5.8.

(i) Nach Bemerkung 2.15 ist $\mathbb{1}_1^G$ der reguläre Charakter von G. Insbesondere ist φ^G nicht unbedingt irreduzibel, falls φ irreduzibel ist. Ist φ reduzibel, so muss auch φ^G reduzibel sein wegen der Linearität der Induktion.

(ii) Sei $G := A_5$ und $H := A_4$. Nach Aufgabe 17 ist $\pi := (\mathbb{1}_H)^G$ der Permutationscharakter von G auf $\{1, \ldots, 5\}$, denn H ist der Stabilisator von 5. Für $g \in G$ ist $\pi(g)$ die Anzahl der Fixpunkte von g. Da G transitiv operiert, ist $\mathbb{1}_G$ ein irreduzibler Bestandteil von π mit Vielfachheit 1. Da G nach Beispiel 4.8 keinen irreduziblen Charakter vom Grad 2 besitzt, ist $\chi := \pi - \mathbb{1}_G$ ein irreduzibler Charakter vom Grad 4. Man erhält die fehlenden Werte $\chi((1,2,3,4,5)) = -1 = \chi((1,3,5,2,4))$. Sei nun $\lambda \in \mathrm{Irr}(H)$ ein nicht-trivialer linearer Charakter und $\psi := \lambda^G$. Wegen $(\psi, \mathbb{1}_G)_G = (\lambda, \mathbb{1}_H)_H = 0$ und $\psi(1) = |G : H|\lambda(1) = 5$ ist auch ψ irreduzibel. Wegen $5 \nmid 12 = |H|$ liegt kein 5-Zyklus in H. Dies zeigt $\psi((1,2,3,4,5)) = 0 = \psi((1,3,5,2,4))$.

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

Die fehlenden Werte werden in Beispiel 7.14 berechnet.

6 Anwendungen

Bemerkung 6.1. William Burnside verfasste 1897 das erste Buch über Gruppentheorie. Mangels Anwendungen wurde die von ihm und Frobenius entwickelte Charaktertheorie darin noch nicht erwähnt. Dies änderte sich mit seinem Beweis des $p^a q^b$-Satzes. Im Vorwort der 1911 erschienenen zweiten Auflage schreibt er:

> *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. *Sei $\chi \in \mathrm{Irr}(G)$ und $g \in C \in \mathrm{Cl}(G)$ mit $\mathrm{ggT}(\chi(1), |C|) = 1$. Dann ist $g \in \mathrm{Z}(\chi)$ oder $\chi(g) = 0$.*

Beweis. Sei $\alpha := \frac{\chi(g)}{\chi(1)}$. Wegen $\mathrm{ggT}(\chi(1), |C|) = 1$ existieren $a, b \in \mathbb{Z}$ mit $a\chi(1) + b|C| = 1$. Mit $\omega_\chi(C)$ und $\chi(g)$ ist auch

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

ganz-algebraisch. Sei $n := |\langle g \rangle|$. Als Summe n-ter Einheitswurzeln liegt $\chi(g)$ im Kreisteilungskörper $\mathbb{Q}_n$. Sei $\mathcal{G} := \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$. Für $\sigma \in \mathcal{G}$ ist auch $\sigma(\alpha)$ ganz-algebraisch, denn α und $\sigma(\alpha)$ sind Nullstellen des gleichen ganzzahligen Polynoms. Daher ist auch $\beta := \prod_{\sigma \in \mathcal{G}} \sigma(\alpha)$ ganz-algebraisch (Lemma 4.3). Wegen $\sigma(\beta) = \beta$ für alle $\sigma \in \mathcal{G}$ liegt β im Fixkörper von $\mathcal{G}$, d. h. $\beta \in \mathbb{Q}$, da $\mathbb{Q} \subseteq \mathbb{Q}_n$ eine Galois-Erweiterung ist. Nach Lemma 4.5 ist $\beta \in \mathbb{Z}$. Im Fall $g \notin \mathrm{Z}(\chi)$ ist $|\alpha| < 1$ (Lemma 3.14). Mit $\chi(g)$ ist auch $\sigma(\chi(g))$ eine Summe von $m := \chi(1)$ vielen n-ten Einheitswurzeln $\epsilon_1, \ldots, \epsilon_m$. Es folgt

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

und $|\sigma(\alpha)| \leq 1$ für $\sigma \in \mathcal{G}$. Folglich ist $|\beta| < 1$, d. h. $\beta = 0$. Also ist $\alpha = 0$ und $\chi(g) = 0$. □

Satz 6.3. *Sei G einfach und nicht-abelsch, $C \in \mathrm{Cl}(G)$ und $|C|$ eine Potenz einer Primzahl p. Dann ist $C = \{1\}$.*

Beweis. Wir nehmen $C \neq \{1\}$ an und wählen $g \in C$ und $\chi \in \mathrm{Irr}(G) \setminus \{\mathbb{1}_G\}$. Da G einfach ist, ist $\mathrm{Ker}(\chi) = 1$. Da G nicht-abelsch ist, ist auch $\mathrm{Z}(\chi) = 1$ (Satz 3.17). Im Fall $p \nmid \chi(1)$ ist also $\chi(g) = 0$ nach Lemma 6.2. Daher ist

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

ganz-algebraisch. Widerspruch. □

Satz 6.4 (Burnside)**.** *Sei $|G| = p^a q^b$ mit Primzahlen p, q und $a, b \in \mathbb{N}_0$. Dann ist G auflösbar.*

Beweis. Sei G ein minimales Gegenbeispiel und $N \lhd G$. Ist $N \neq 1$, so wären N und G/N auflösbar und daher auch G. Also ist $N = 1$ und G ist einfach und nicht-abelsch. O. B. d. A. sei $1 \neq P \in \mathrm{Syl}_p(G)$. Nach Algebra existiert $g \in \mathrm{Z}(P) \setminus \{1\}$. Sei C die Konjugationsklasse von g. Dann ist

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

eine Primzahlpotenz. Nach Satz 6.3 ist $C = \{1\}$. Widerspruch. □

Bemerkung 6.5. Satz 6.4 war eine der ersten Anwendungen der Darstellungstheorie zur Untersuchung endlicher Gruppen. Mittlerweile kennt man auch einen (deutlich schwierigeren) Beweis, der ohne Darstellungstheorie auskommt.[3] Für Satz 6.3 und den folgenden Satz kennt man jedoch keinen solchen Beweis.[4]

Satz 6.6 (Frobenius)**.** *Sei $H \leq G$ mit $gHg^{-1} \cap H = 1$ für alle $g \in G \setminus H$. Dann existiert $N \trianglelefteq G$ mit $G = HN$ und $H \cap N = 1$.*

Beweis (Knapp-Schmid). Sei

$$H^* := \Big(\bigcup_{g \in G} gHg^{-1} \Big) \setminus \{1\}$$

und $N := G \setminus H^*$. Nach Voraussetzung gilt $\mathrm{N}_G(H) = H$, d. h. H besitzt genau $|G : H|$ Konjugierte in G. Für je zwei verschiedene Konjugierte xHx^{-1} und yHy^{-1} gilt

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

Dies zeigt $|H^*| = |G : H|(|H| - 1) = |G| - |G : H|$ und $|N| = |G : H|$. Wenn wir zeigen können, dass die Klassenfunktion

$$\rho\colon G \to \mathbb{C}, \qquad g \mapsto \begin{cases} |H| & \text{falls } g \in N, \\ 0 & \text{falls } g \in H^* \end{cases}$$

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

ein Charakter von G ist, so folgt $N = \mathrm{Ker}(\rho) \trianglelefteq G$. Wegen $N \cap H = 1$ ist dann $|HN| = |H||N| = |G|$ und $G = HN$. Für $\chi \in \mathrm{Irr}(G)$ müssen wir $(\chi, \rho) \in \mathbb{N}_0$ zeigen. Zunächst gilt $(\rho, \mathbb{1}_G) = \frac{|H||N|}{|G|} = 1$. Für $\chi \neq \mathbb{1}_G$ gilt nach der ersten Orthogonalitätsrelation

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

Wir können $c_\chi \neq 0$ annehmen. Die Cauchy-Schwarz-Ungleichung angewendet auf die Vektoren $(\chi(g) : g \in N)$ und $(1, \ldots, 1)$ ergibt

$$(|N|c_\chi)^2 = \Big(\sum_{g \in N} \chi(g) \Big)^2 \leq |N| \sum_{g \in N} |\chi(g)|^2.$$

Es folgt

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

Wegen $c_\chi^2 - \chi(1)^2 = (c_\chi + \chi(1))(c_\chi - \chi(1))$ ist andererseits

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

Daher gilt Gleichheit in der Cauchy-Schwarz-Ungleichung. Dies impliziert $\chi(g) = \chi(1)$ für alle $g \in N$. Also ist $c_\chi = \chi(1) > 0$ wie gewünscht. □

Bemerkung 6.7. In der Situation von Satz 6.6 mit $1 < H < G$ nennt man G eine *Frobeniusgruppe* mit *Komplement* H und *Kern* N.

Beispiel 6.8. Sei $n \geq 3$ ungerade. Dann ist

$$D_{2n} = \langle \sigma, \tau : \sigma^n = \tau^2 = 1,\ \tau\sigma\tau = \sigma^{-1} \rangle$$

eine Frobeniusgruppe mit Komplement $\langle \tau \rangle$ und Kern $\langle \sigma \rangle$, denn $\sigma^i \tau \sigma^{-i} = \sigma^{2i}\tau \neq \tau$ für $i = 1, \ldots, n-1$. Weitere Beispiele werden in Aufgabe 16 konstruiert.

Satz 6.9 (Taunt)**.** *Für jede p-Sylowgruppe P von G gilt $G' \cap \mathrm{Z}(G) \cap P \leq P'$.*

Beweis. Als Untergruppe von $\mathrm{Z}(G)$ ist $N := G' \cap \mathrm{Z}(G) \cap P$ ein Normalteiler von G. Sei $\lambda \in \mathrm{Irr}(P)$ ein linearer Charakter. Da $\lambda^G(1) = |G : P|$ nicht durch p teilbar ist, existiert ein irreduzibler Bestandteil χ von λ^G mit $d := \chi(1) \not\equiv 0 \pmod p$. Nach Frobenius-Reziprozität ist λ ein Bestandteil von χ_P. Daher ist λ_N ein irreduzibler Bestandteil von χ_N. Wegen $N \subseteq \mathrm{Z}(G)$ kann χ_N nach Aufgabe 15 keine weiteren Bestandteile haben. Dies zeigt $\chi_N = d\lambda_N$. Für $\mu := \det \chi$ ist daher $\mu_N = \det(\chi_N) = \lambda_N^d$ (Bemerkung 2.6). Wegen $\mu(1) = 1$ gilt $N \leq G' \leq \mathrm{Ker}(\mu)$ und $\lambda_N^d = \mathbb{1}_N$. Andererseits gilt $\lambda(x)^{|N|} = \lambda(x^{|N|}) = \lambda(1) = 1$ für alle $x \in N$, d. h. $\lambda_N^{|N|} = \mathbb{1}_N$. Wir wählen $a, b \in \mathbb{Z}$ mit $ad + b|N| = \mathrm{ggT}(d, |N|) = 1$. Dann ist $\lambda_N = (\lambda_N^d)^a (\lambda_N^{|N|})^b = \mathbb{1}_N$. Dies zeigt $N \leq \mathrm{Ker}(\lambda)$. Satz 3.12 und Aufgabe 10 angewendet auf P/P' liefern

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

Beispiel 6.10. Sei G eine Gruppe kubikfreier Ordnung (d. h. $|G|$ ist nicht durch die dritte Potenz einer Primzahl teilbar). Nach Beispiel 4.8 sind alle Sylowgruppen P von G abelsch. Mit Taunt folgt $G' \cap \mathrm{Z}(G) \cap P = 1$. Da $G' \cap \mathrm{Z}(G) \cap P$ eine Sylowgruppe von $G' \cap \mathrm{Z}(G)$ ist, gilt sogar $G' \cap \mathrm{Z}(G) = 1$.

Lemma 6.11. *Sei $P \in \mathrm{Syl}_p(G)$ und $x, y \in \mathrm{Z}(P)$. Sind x, y in G konjugiert, so auch in $\mathrm{N}_G(P)$.*

Beweis. Sei $g \in G$ mit $gxg^{-1} = y$. Nach Voraussetzung ist $P \leq \mathrm{C}_G(x) \cap \mathrm{C}_G(y) = \mathrm{C}_G(x) \cap g\mathrm{C}_G(x)g^{-1}$. Also ist $P, g^{-1}Pg \in \mathrm{Syl}_p(\mathrm{C}_G(x))$ und nach Sylow existiert ein $c \in \mathrm{C}_G(x)$ mit $cPc^{-1} = g^{-1}Pg$. Dies impliziert $gc \in \mathrm{N}_G(P)$ und $gcx(gc)^{-1} = gxg^{-1} = y$. □

Satz 6.12 (Burnsides Verlagerungssatz)**.** *Sei $P \in \mathrm{Syl}_p(G)$ mit $\mathrm{N}_G(P) = \mathrm{C}_G(P)$. Dann existiert ein $N \trianglelefteq G$ mit $G = PN$ und $P \cap N = 1$.*

Beweis. Wegen $P \leq \mathrm{N}_G(P) = \mathrm{C}_G(P)$ ist P abelsch. Sei $g_1, \ldots, g_n$ ein Repräsentantensystem für G/P. Sei $\sigma\colon G \to S_n$, $x \mapsto \sigma_x$ die Operation auf G/P durch Linksmultiplikation, d. h. $xg_iP = g_{\sigma_x(i)}P$ für $i = 1, \ldots, n$. Für $\lambda \in \mathrm{Irr}(P)$ ist

$$\Delta_\lambda\colon G \to \mathrm{GL}(n, \mathbb{C}), \qquad x \mapsto \big(\delta_{i,\sigma_x(j)}\lambda(g_i^{-1}xg_j)\big)$$

nach Aufgabe 29 eine Darstellung. Mit $\operatorname{sgn} \circ \sigma$ ist auch $\chi_\lambda := (\operatorname{sgn} \circ \sigma) \det(\Delta_\lambda)$ ein Charakter. Aus der Leibniz-Formel für Determinanten folgt[5]

$$\chi_\lambda(x) = \prod_{i=1}^{n} \lambda(g_i^{-1}xg_{\sigma_x^{-1}(i)}).$$

Sei $(i_1, \ldots, i_k)$ ein Zyklus von σ_x^{-1}. Die entsprechenden Faktoren in $\chi_\lambda(x)$ liefern den Beitrag

$$\lambda(g_{i_1}^{-1}xg_{i_2})\lambda(g_{i_2}^{-1}xg_{i_3}) \ldots \lambda(g_{i_k}^{-1}xg_{i_1}) = \lambda(g_{i_1}^{-1}x^kg_{i_1}),$$

da λ ein Homomorphismus ist.

Sei

$$N := \bigcap_{\lambda \in \mathrm{Irr}(P)} \mathrm{Ker}(\chi_\lambda) \trianglelefteq G.$$

Für ein p'-Element $x \in G$ gilt $g_{i_1}^{-1}x^kg_{i_1} \in P$ nur im Fall $x^k = 1$. Es folgt $x \in N$. Sei nun $x \in P \setminus \{1\}$. Nach Aufgabe 10 existiert ein $\lambda \in \mathrm{Irr}(P)$ mit $\lambda(x) \neq 1$. Aus $g_{i_1}^{-1}x^kg_{i_1} \in P$ folgt $g_{i_1}^{-1}x^kg_{i_1} = x^k$ nach Lemma 6.11. Daher vereinfacht sich χ_λ zu $\chi_\lambda(x) = \lambda(x^n)$. Da $n = |G : P|$ zu p teilerfremd ist, gilt $\chi_\lambda(x) \neq 1$. Dies zeigt $x \notin N$ und $P \cap N = 1$. Da N andererseits alle p'-Elemente besitzt, ist G/N eine p-Gruppe. Es folgt $G = PN$. □

7 Darstellungen über Zahlkörpern

Bemerkung 7.1. Für die symbolische (d. h. exakte) Berechnung von Darstellungen mit dem Computer ist es notwendig, den Körper $\mathbb{C}$ durch „kleinere“ Körper zu approximieren.

(i) Für die bisherige Entwicklung der Charaktertheorie haben wir nur benutzt, dass $\mathbb{C}$ Charakteristik 0 hat (Maschke), algebraisch abgeschlossen ist (Schurs Lemma) und die komplexe Konjugation

[5] Die Konstruktion entspricht der Verlagerungsabbildung aus der Gruppentheorie.

existiert (Skalarprodukt).[6] Alle Aussagen gelten daher auch für den algebraischen Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}$ ($\overline{\mathbb{Q}}$ ist die Menge der algebraischen Zahlen). Im Gegensatz zu $\mathbb{C}$ ist $\overline{\mathbb{Q}}$ zwar abzählbar, aber unendlich-dimensional über $\mathbb{Q}$.

(ii) Nach Lemma 3.14 liegen die Charakterwerte von G im Kreisteilungskörper $\mathbb{Q}_{|G|}$.[7] Brauers tiefliegender Induktionssatz[8] impliziert, dass sich sogar jede $\mathbb{C}$-Darstellung von G über $\mathbb{Q}_{|G|}$ realisieren lässt. Wir beweisen mit weniger Aufwand eine schwächere Aussage.

(iii) Ein *Zahlkörper* ist ein Teilkörper $K \subseteq \mathbb{C}$ mit $|K : \mathbb{Q}| = \dim_{\mathbb{Q}} K < \infty$. Ggf. ist $\mathbb{Q} \subseteq K$ eine algebraische Körpererweiterung und K liegt in $\overline{\mathbb{Q}}$. Sei $x_1, \ldots, x_n \in K$ eine $\mathbb{Q}$-Basis von K. Sei $\mu_i \in \mathbb{Q}[X]$ das Minimalpolynom von x_i für $i = 1, \ldots, n$. Dann ist der Zerfällungskörper $L \subseteq \mathbb{C}$ von $\mu_1 \ldots \mu_n$ eine Galois-Erweiterung über $\mathbb{Q}$ mit $K \subseteq L$. Wir können daher bei Bedarf annehmen, dass K selbst eine Galois-Erweiterung ist. Bekanntlich ist $\mathbb{Q} \subseteq \mathbb{Q}_n$ für alle $n \in \mathbb{N}$ eine Galois-Erweiterung (das haben wir bereits im Beweis von Lemma 6.2 benutzt).

Satz 7.2. *Für jede endliche Gruppe G existiert ein Zahlkörper K, sodass jede $\mathbb{C}$-Darstellung von G zu einer K-Darstellung ähnlich ist.*

Beweis. Seien $\psi_1, \ldots, \psi_k$ die Charaktere der irreduziblen $\overline{\mathbb{Q}}$-Darstellungen bis auf Ähnlichkeit. Wie in Satz 2.18 ist $\{\psi_1, \ldots, \psi_k\}$ eine Orthonormalbasis von $\mathrm{CF}(G)$ und $k = k(G)$. Da jede $\overline{\mathbb{Q}}$-Darstellung auch eine $\mathbb{C}$-Darstellung ist, gilt

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

für $1 \leq i \leq k$ und gewisse $a_{i,\chi} \in \mathbb{N}_0$. Aus $1 = (\psi_i, \psi_i)_G = \sum_{\chi \in \mathrm{Irr}(G)} a_{i,\chi}^2$ folgt $\psi_i \in \mathrm{Irr}(G)$ und $\mathrm{Irr}(G) = \{\psi_1, \ldots, \psi_k\}$. Jede (irreduzible) $\mathbb{C}$-Darstellung ist also zu einer $\overline{\mathbb{Q}}$-Darstellung Δ ähnlich (Satz 2.14). Die Einträge von $\Delta(g)$ für $g \in G$ sind algebraische Zahlen, sie liegen somit in einem Zahlkörper K. Wir können K so groß wählen, dass jede (irreduzible) $\overline{\mathbb{Q}}$-Darstellung Einträge in K hat. □

Definition 7.3. Eine Darstellung über einem Zahlkörper K heißt *absolut irreduzibel*, wenn sie als $\mathbb{C}$-Darstellung irreduzibel ist. Sind alle irreduziblen K-Darstellungen absolut irreduzibel, so nennt man K einen *Zerfällungskörper* von G.

Beispiel 7.4.

(i) Nach Satz 7.2 besitzt jede Gruppe einen Zerfällungskörper mit endlichem Grad über $\mathbb{Q}$. Nach Satz 2.2 ist $\mathbb{Q}_n$ ein Zerfällungskörper jeder abelschen Gruppe der Ordnung n. Man kann zeigen, dass $\mathbb{Q}$ ein Zerfällungskörper der symmetrischen Gruppen ist (ohne Beweis, vgl. Aufgabe 19).

(ii) Die Begleitmatrix $B := \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ des Kreisteilungspolynoms $\Phi_3 = X^2 + X + 1$ hat Ordnung 3. Da die Eigenwerte von B irrational sind, ist die Einbettung $\Delta \colon \langle B \rangle \hookrightarrow \mathrm{GL}(2, \mathbb{Q})$ eine irreduzible $\mathbb{Q}$-Darstellung. Da der Grad von Δ die Gruppenordnung nicht teilt, kann Δ nicht absolut irreduzibel sein (das folgt auch aus Satz 2.2).

Lemma 7.5. *Sei $n, k \in \mathbb{N}$ und $k\mathbb{Z}^n \leq A \leq \mathbb{Z}^n$. Dann ist $A \cong \mathbb{Z}^n$.*

[6] Wir haben nicht benutzt, dass $\mathbb{C}$ als normierter Raum abgeschlossen ist.
[7] Sogar $\mathbb{Q}_{\exp(G)}$ mit $\exp(G) := \mathrm{kgV}(|\langle g \rangle| : g \in G)$.
[8] siehe Satz 6.7 in Charaktertheorie

Beweis. Induktion nach n: Im Fall $n = 1$ ist $A = d\mathbb{Z} \cong \mathbb{Z}$ mit $d \mid k$. Sei nun $n \geq 2$. Sei $\pi\colon A \to \mathbb{Z}$, $(a_1, \ldots, a_n) \mapsto a_n$ die Projektion auf die n-te Koordinate. Sei

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

Dann gilt $k\mathbb{Z}^{n-1} \leq B \leq \mathbb{Z}^{n-1}$. Nach Induktion folgt $\mathrm{Ker}(\pi) \cong B \cong \mathbb{Z}^{n-1}$. Da $A/\mathrm{Ker}(\pi) \cong \pi(A) \leq \mathbb{Z}$ zyklisch ist, existiert $a = (a_1, \ldots, a_n) \in A$ mit $A = \langle a \rangle + \mathrm{Ker}(\pi)$. Wegen $k\mathbb{Z}^n \leq A$ ist $a_n \neq 0$. Für alle $m \in \mathbb{Z} \setminus \{0\}$ ist daher $ma \notin \mathrm{Ker}(\pi)$. Also gilt $\langle a \rangle \cap \mathrm{Ker}(\pi) = 0$ und $A = \langle a \rangle \oplus \mathrm{Ker}(\pi) \cong \mathbb{Z}^n$. □

Satz 7.6 (Minkowski)**.** *Jede endliche Untergruppe G von $\mathrm{GL}(n, \mathbb{Q})$ ist zu einer Untergruppe von $\mathrm{GL}(n, \mathbb{Z})$ konjugiert. Außerdem ist G für jede Primzahl $p > 2$ zu einer Untergruppe von $\mathrm{GL}(n, p)$ isomorph.*

Beweis. Offenbar ist $M := \sum_{g \in G} g\mathbb{Z}^n \subseteq \mathbb{Q}^n$ eine abelsche Gruppe, die $\mathbb{Z}^n = 1\mathbb{Z}^n$ enthält. Ist k das kgV aller Nenner von Matrixeinträgen aus allen $g \in G$, so gilt $k\mathbb{Z}^n \subseteq kM \subseteq \mathbb{Z}^n$. Nach Lemma 7.5 ist $M \cong kM \cong \mathbb{Z}^n$. Sei $\gamma\colon \mathbb{Z}^n \to M$ ein entsprechender Isomorphismus von abelschen Gruppen. Da $\mathbb{Z}^n$ die Standardbasis von $\mathbb{Q}^n$ enthält, lässt sich γ (eindeutig) zu einem Isomorphismus $\gamma\colon \mathbb{Q}^n \to \mathbb{Q}^n$ von $\mathbb{Q}$-Vektorräumen fortsetzen. Für $g \in G$ gilt

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

Eine Auswertung an der Standardbasis zeigt $\gamma^{-1} G \gamma \leq \mathrm{GL}(n, \mathbb{Z})$.

Für die zweite Behauptung können wir $G \leq \mathrm{GL}(n, \mathbb{Z})$ annehmen. Es genügt zu zeigen, dass

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

injektiv ist. Im Fall $\mathrm{Ker}(\Gamma) \neq 1$ existiert ein $g \in \mathrm{Ker}(\Gamma)$ mit Primzahlordnung q. Sei $g = 1_n + dA$ mit $d \in \mathbb{Z}$ und $A \in \mathbb{Z}^{n \times n}$ mit teilerfremden Einträgen. Wegen $g \equiv 1_n \pmod p$ ist $p \mid d$. Nach der binomischen Formel gilt

$$\begin{aligned} 1_n = g^q = (1_n + dA)^q &= 1_n + qdA + \frac{q(q-1)}{2} d^2 A^2 + \ldots + d^q A^q, \\ -qA = \frac{q(q-1)}{2} dA + \ldots + d^{q-1} A^q &\equiv 0 \pmod p. \end{aligned}$$

Dies zeigt $q = p$. Wegen $p > 2$ erhält man den Widerspruch

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

Folgerung 7.7. *Für jedes $n \in \mathbb{N}$ besitzt $\mathrm{GL}(n, \mathbb{Q})$ bis auf Isomorphie nur endlich viele endliche Untergruppen.*

Beweis. Für jede endliche Untergruppe $G \leq \mathrm{GL}(n, \mathbb{Q})$ gilt $|G| \leq |\mathrm{GL}(n, 3)| \leq 3^{n^2}$ nach Satz 7.6. □

Bemerkung 7.8. In Folgerung 13.15 zeigen wir, dass es sogar nur endlich viele Konjugationsklassen von endlichen Untergruppen in $\mathrm{GL}(n, \mathbb{Q})$ gibt.

Beispiel 7.9.

(i) Die Begleitmatrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z})$ von $\Phi_6 = X^2 - X + 1$ hat Ordnung 6. Wegen $\mathrm{GL}(2, 2) \cong S_3$ kann Satz 7.6 nicht für $p = 2$ gelten (vgl. Aufgabe 31).

(ii) Sei $G \leq \mathrm{GL}(n, \mathbb{Q})$. Für $n = 1$ ist offensichtlich $G \leq \langle -1 \rangle$. Bekanntlich gilt

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

für jede Primzahl p. Für $n = 2$ und $p = 3$ erhält man $|G| \mid 48$. Nach Aufgabe 9 ist

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

allerdings zu keiner Untergruppe von $\mathrm{GL}(2, \mathbb{Q})$ konjugiert. Da $\mathrm{SL}(2,3)$ die einzige Untergruppe der Ordnung 24 in $\mathrm{GL}(2,3)$ ist (ohne Beweis), gilt $|G| \in \{1, 2, 3, 4, 6, 8, 12\}$. Mit der Matrix aus (i) gilt

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

Nach Beispiel 1.4 ist auch D_8 zu einer Untergruppe von $\mathrm{GL}(2, \mathbb{Z})$ isomorph.

(iii) Eine $n \times n$-Matrix der Form $(\epsilon_i \delta_{i\pi(j)})_{i,j}$ mit $\pi \in S_n$ und $\epsilon_1, \dots, \epsilon_n \in \{\pm 1\}$ heißt *verallgemeinerte Permutationsmatrix*. Die verallgemeinerten Permutationsmatrizen bilden eine Untergruppe $M \leq \mathrm{GL}(n, \mathbb{Z})$ der Ordnung $2^n n!$. Feit hat gezeigt, dass es für $n \geq 11$ keine größere Untergruppe gibt und jede Untergruppe der Ordnung $2^n n!$ zu M konjugiert ist.

(iv) Mit C_n und D_{2n} für $n \in \mathbb{N}$ besitzt $\mathrm{GL}(2, \mathbb{R})$ unendlich viele endliche Untergruppen (Beispiel 1.4). Nach Aufgabe 32 sind dies aber bis auf Konjugation die einzigen solchen Untergruppen.

(v) Für $G \leq \mathrm{GL}(n, \mathbb{C})$ existiert ein abelscher Normalteiler $A \trianglelefteq G$, sodass $|G : A|$ durch eine Funktion in n beschränkt ist (Satz von Jordan[9]). Für $n \geq 71$ gilt konkret $|G : A| \leq (n+1)!$ mit Gleichheit für $G = S_{n+1}$ (Aufgabe 18).

(vi) Minkowskis Satz lässt sich nicht auf Zahlkörper verallgemeinern: Feit hat gezeigt, dass Q_8 zu einer Untergruppe von $\mathrm{GL}(2, \mathbb{Q}(\sqrt{-35}))$ isomorph ist, aber nicht zu einer Untergruppe von $\mathrm{GL}(2, R)$, wobei $R = \mathbb{Z}[(1 + \sqrt{-35})/2]$ der Ganzheitsring von $\mathbb{Q}(\sqrt{-35})$ ist.[10] Um zu zeigen, dass Folgerung 7.7 für Zahlkörper gilt, verallgemeinern wir zunächst die komplexe Konjugation von Charakteren.

Satz 7.10. *Sei G eine Gruppe der Ordnung n. Sei $\zeta := e^{2\pi \mathrm{i}/n} \in \mathbb{Q}_n$ und $\sigma \in \mathcal{G} := \mathrm{Gal}(\mathbb{Q}_n | \mathbb{Q})$ mit $\sigma(\zeta) = \zeta^k$. Dann gilt:*

(i) Durch ${}^{\sigma}\mathrm{Cl}(g) := \mathrm{Cl}(g^k)$ für $g \in G$ operiert $\mathcal{G}$ auf $\mathrm{Cl}(G)$.

(ii) Durch $\boxed{({}^{\sigma}\chi)(g) := \sigma(\chi(g)) = \chi(g^k)}$ für $g \in G$ und $\chi \in \mathrm{Irr}(G)$ operiert $\mathcal{G}$ auf $\mathrm{Irr}(G)$.

Beweis.

(i) Wegen $\mathrm{ggT}(k, n) = 1$ existiert $k' \in \mathbb{Z}$ mit $kk' \equiv 1 \pmod{n}$. Daher ist $G \to G$, $g \mapsto g^k$ eine Bijektion mit Umkehrabbildung $g \mapsto g^{k'}$. Für $g, h, x \in G$ gilt $g = xhx^{-1} \iff g^k = xh^k x^{-1}$. Also ist ${}^{\sigma}C \in \mathrm{Cl}(G)$ für alle $C \in \mathrm{Cl}(G)$. Für $\tau \in \mathcal{G}$ mit $\tau(\zeta) = \zeta^l$ gilt

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

Somit operiert $\mathcal{G}$ auf $\mathrm{Cl}(G)$.

[9] Siehe Charaktertheorie-Skript

[10] R ist die Menge der ganz-algebraischen Zahlen in $\mathbb{Q}(\sqrt{-35})$.

(ii) Sei K ein Zahlkörper wie in Satz 7.2 und $\Delta\colon G \to \mathrm{GL}(d,K)$ eine Darstellung mit Charakter χ. Nach Bemerkung 7.1 können wir annehmen, dass $\mathbb{Q} \subseteq K$ eine Galois-Erweiterung ist, die $\mathbb{Q}_n$ enthält. Wegen

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

ist die Einschränkung $\mathrm{Gal}(K|\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ surjektiv. Sei $\hat{\sigma} \in \mathrm{Gal}(K|\mathbb{Q})$ mit $\hat{\sigma}_{|\mathbb{Q}_n} = \sigma$. Die Anwendung von $\hat{\sigma}$ auf Matrixeinträge liefert einen Automorphismus von $\mathrm{GL}(d,K)$. Also ist $\hat{\sigma} \circ \Delta\colon G \to \mathrm{GL}(d,K)$ eine irreduzible K-Darstellung mit Charakter

$$g \mapsto \mathrm{tr}\big(\hat{\sigma}(\Delta(g))\big) = \sigma(\mathrm{tr}\,\Delta(g)) = \sigma(\chi(g))$$

für $g \in G$. Seien $\zeta^{a_1}, \ldots, \zeta^{a_d} \in \mathbb{Q}_n$ die Eigenwerte von $\Delta(g)$. Dann gilt

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

(vgl. Aufgabe 5). Man sieht leicht, dass $(\sigma,\chi) \mapsto {}^{\sigma}\chi$ eine Operation definiert. □

Folgerung 7.11. *Ist $\chi \in \mathrm{Irr}(G)$ der einzige irreduzible Charakter vom Grad d, so ist χ ganzzahlig.*

Beweis. Für $\sigma \in \mathcal{G}$ gilt ${}^{\sigma}\chi = \chi$. Daher liegen die Werte von χ im Fixkörper $\mathbb{Q}$ von $\mathcal{G}$, da $\mathbb{Q} \subseteq \mathbb{Q}_n$ eine Galois-Erweiterung ist. Als ganz-algebraische Zahlen sind die Werte von χ ganzzahlig. □

Bemerkung 7.12.

(i) Konjugationsklassen bzw. Charaktere, die in der gleichen Bahn unter $\mathcal{G}$ liegen, nennt man *Galois-konjugiert*.

(ii) Da $\mathcal{G}$ abelsch ist, erhält man auch durch ${}^{\sigma}\mathrm{Cl}(g) := \mathrm{Cl}(g^{k'})$ mit $kk' \equiv 1 \pmod{n}$ eine Operation. Es gilt dann $({}^{\sigma}\chi)({}^{\sigma}g) = \chi(g)$.

(iii) Die natürliche Operation von $\mathrm{Aut}(G)$ auf G (d. h. die Einbettung $\mathrm{Aut}(G) \hookrightarrow \mathrm{Sym}(G)$) induziert Operationen von $\mathrm{Aut}(G)$ auf $\mathrm{Cl}(G)$ und $\mathrm{Irr}(G)$. Für $\alpha \in \mathrm{Aut}(G)$, $\chi \in \mathrm{Irr}(G)$ und $g \in G$ gilt dabei ${}^{\alpha}\mathrm{Cl}(g) := \mathrm{Cl}(\alpha(g))$ und $({}^{\alpha}\chi)(g) = \chi(\alpha^{-1}(g))$. Wieder erhält man $({}^{\alpha}\chi)({}^{\alpha}g) = \chi(g)$. Da $\mathrm{Inn}(G)$ im Kern beider Operationen liegt, genügt es die Operationen der äußeren Automorphismengruppe $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ zu betrachten.

(iv) Die Operationen von $\mathcal{G}$ und $\mathrm{Out}(G)$ bewirken Permutationen der Zeilen und Spalten der Charaktertafel von G. Das nächste Resultat impliziert, dass Zeilen und Spalten nicht unabhängig permutiert werden können.

Satz 7.13 (Brauers Permutationslemma)**.** *Seien G, H endliche Gruppen, sodass G auf $\mathrm{Cl}(H)$ und $\mathrm{Irr}(H)$ operiert. Für alle $g \in G$, $h \in H$ und $\chi \in \mathrm{Irr}(H)$ gelte $({}^{g}\chi)({}^{g}\mathrm{Cl}(h)) = \chi(h)$. Dann stimmen die Zyklentypen von g in $\mathrm{Sym}(\mathrm{Cl}(H))$ und $\mathrm{Sym}(\mathrm{Irr}(H))$ überein. Insbesondere gilt*

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

für alle $g \in G$.

Beweis. Sei $\mathrm{Cl}(H) = \{K_1, \dots, K_k\}$ und $\mathrm{Irr}(H) = \{\chi_1, \dots, \chi_k\}$. Sei $X := (\chi_i(K_j))_{i,j}$ die Charaktertafel von H. Sei $g \in G$ fest. Die Operation von g auf $\mathrm{Irr}(H)$ (bzw. $\mathrm{Cl}(H)$) wird durch Multiplikation mit einer Permutationsmatrix $P = (\delta_{i\sigma(j)})$ (bzw. $Q = (\delta_{i\tau(j)})$ von links (bzw. rechts) beschrieben:

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

Nach der zweiten Orthogonalitätsrelation ist X invertierbar. Es folgt $P = XQX^{-1}$, d. h. P und Q sind ähnlich. Sei $(l_1, \dots, l_n)$ der Zyklentyp von P. Aus Aufgabe 14 erhält man die Eigenwerte von P:

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

(mit Vielfachheiten). Da P und Q die gleichen Eigenwerte haben, ist $(l_1, \dots, l_n)$ auch der Zyklentyp von Q. Die letzte Behauptung erhält man durch Zählen von Einerzyklen. □

Beispiel 7.14.

(i) Sei $|G|$ ungerade. Angenommen es existieren $g, x \in G$ mit $xgx^{-1} = g^{-1}$. Dann ist $x^2gx^{-2} = g$. Da $n := |\langle x\rangle|$ nach Lagrange ungerade ist, existieren $a, b \in \mathbb{Z}$ mit $an + 2b = 1$. Es folgt

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

Daher ist $g = 1$ der einzige Fixpunkt der Abbildung $\mathrm{Cl}(G) \to \mathrm{Cl}(G)$, $\mathrm{Cl}(g) \mapsto \mathrm{Cl}(g^{-1})$. Nach Brauers Permutationslemma ist $\mathbb{1}_G$ der einzige Fixpunkt der Abbildung $\mathrm{Irr}(G) \to \mathrm{Irr}(G)$, $\chi \mapsto \overline{\chi}$. Wir wählen $\chi_1, \dots, \chi_s \in \mathrm{Irr}(G)$ mit $\mathrm{Irr}(G) = \{\mathbb{1}_G, \chi_1, \dots, \chi_s, \overline{\chi_1}, \dots, \overline{\chi_s}\}$. Wegen $\chi_i(1) \mid |G|$ gilt $\chi_i(1)^2 \equiv 1, 9 \pmod{16}$ und $2\chi_i(1)^2 \equiv 2 \pmod{16}$. Dies zeigt

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

(ii) In Beispiel 5.8 hatten wir einen (ganzzahligen) Teil der Charaktertafel von $G = A_5$ konstruiert. Sei $g = (1,2,3,4,5) \in G$. Wegen $(2,5)(3,4)g(2,5)(3,4) = (1,5,4,3,2) = g^{-1}$ ist die gesamte Charaktertafel von G reell. Nach Brauers Permutationslemma existieren zwei Galois-konjugierte Charaktere $\chi, \psi \in \mathrm{Irr}(G)$ (vom gleichen Grad) mit Werten in $\mathbb{Q}_5$. Es muss $\chi(1) = \psi(1) = 3$ gelten. Da $\chi(g)$ eine Summe von drei 5-ten Einheitswurzeln ist, gilt o. B. d. A. $\chi(g) = 1 + \zeta + \zeta^{-1} = \frac{1+\sqrt{5}}{2}$ und $\psi(g) = 1 + \zeta^2 + \zeta^{-2} = \frac{1-\sqrt{5}}{2}$ mit $\zeta = e^{2\pi \mathrm{i}/5}$. [11]

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

[11] Diese Werte lassen sich auch mit der zweiten Orthogonalitätsrelation berechnen.

Satz 7.15 (SCHUR). *Sei χ ein treuer Charakter von G mit Werten in einem Zahlkörper K. Dann ist $|G|$ durch eine Funktion in $\chi(1)$ und $|K:\mathbb{Q}|$ beschränkt.*

Beweis. Nach Lemma 3.14 können wir $K \subseteq \mathbb{Q}_n$ mit $n = |G|$ annehmen. Da $\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ abelsch ist, gilt $\mathrm{Gal}(\mathbb{Q}_n|K) \trianglelefteq \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$. Nach dem Hauptsatz der Galois-Theorie ist $\mathbb{Q} \subseteq K$ eine Galois-Erweiterung. Sei $\mathrm{Gal}(K|\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_k\}$ mit $k := |K:\mathbb{Q}|$ und $d := \chi(1)$. Dann ist

$$\psi := \sum_{i=1}^{k} {}^{\sigma_i}\chi$$

ein Charakter vom Grad dk mit Werten in $\mathbb{Q}$. Als ganz-algebraische Zahlen liegen die Werte von ψ sogar in $\mathbb{Z}$. Nach Lemma 3.14 gilt $|\psi(g)| \leq dk$ für alle $g \in G$. Daher nimmt ψ höchstens $2dk+1$ viele Werte an, sagen wir $dk = x_0, \ldots, x_s$ mit $s \leq 2dk$. Sei $m_i := |\{g \in G : \psi(g) = x_i\}|$ für $0 \leq i \leq s$. Mit χ ist auch ψ treu (Aufgabe 10). Dies zeigt $m_0 = 1$ nach Lemma 3.14. Da ψ^l ein Charakter ist, gilt

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

für $l = 0, 1, \ldots$. Also ist $v = (m_0, \ldots, m_s)$ eine Lösung des Gleichungssystems $Av \equiv 0 \pmod{|G|}$ mit ganzzahliger Vandermonde-Matrix $A := (x_j^i)_{i,j=0}^{s}$. Multiplikation mit der zu A komplementären Matrix zeigt $\det(A)v \equiv 0 \pmod{|G|}$. Die Auswertung an der ersten Koordinate liefert

$$0 \neq \prod_{0 \leq i < j \leq s} (x_j - x_i) = m_0 \det(A) \equiv 0 \pmod{|G|}.$$

Insbesondere ist

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

Folgerung 7.16. *Für $n \in \mathbb{N}$ und jeden Zahlkörper K besitzt $\mathrm{GL}(n, K)$ nur endlich viele endliche Untergruppen bis auf Isomorphie.*

Beweis. Man wendet Satz 7.15 auf den Charakter einer Einbettung $G \to \mathrm{GL}(n, K)$ an. □

8 Algebren

Bemerkung 8.1. Wir führen in den nächsten vier Kapiteln ringtheoretische Begriffe ein, die beim Studium von Darstellungen über Körpern mit positiver Charakteristik nützlich sind. Dafür sei K ein beliebiger Körper.

Definition 8.2. Eine *Algebra* über K (kurz eine *K-Algebra*) ist ein Ring A (mit Einselement) und zugleich ein endlich-dimensionaler K-Vektorraum, sodass die Skalarmultiplikation und die Ringmultiplikation kompatibel sind, d. h. es gilt

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

für alle $\lambda \in K$ und $a, b \in A$. Man bezeichnet A als *Divisionsalgebra*, falls $A^\times = A \setminus \{0\}$ gilt, d. h. jedes von 0 verschiedene Element ist invertierbar.

- Eine *Unteralgebra* einer K-Algebra A ist ein Teilring von A, der zugleich ein K-Vektorraum ist. Man kann K mit der Unteralgebra $K1_A$ von A identifizieren.

- Ein *Homomorphismus* von K-Algebren A und B ist ein Ringhomomorphismus $A \to B$, der zugleich K-linear ist. Wie üblich definiert man Epi-, Mono-, Iso- und Automorphismen von Algebren.

Beispiel 8.3.

(i) Ist $K \subseteq L$ eine endliche Körpererweiterung, so ist L eine K-Algebra, wobei Ring- und Skalarmultiplikation identisch sind.

(ii) Für $\varphi \in K[X] \setminus K$ ist $A := K[X]/(\varphi)$ eine kommutative K-Algebra mit $\dim A = \deg \varphi$.

(iii) Für jede K-Algebra A ist das *Zentrum* $\mathrm{Z}(A) := \{a \in A : \forall b \in A : ab = ba\}$ eine kommutative Unteralgebra.

(iv) Sind $A_1, \ldots, A_n$ Algebren über K, so auch das direkte Produkt $A_1 \times \ldots \times A_n$.

(v) Ist A eine K-Algebra und $n \in \mathbb{N}$, so ist auch $A^{n\times n}$ eine K-Algebra. Insbesondere ist $K^{n\times n}$ eine K-Algebra.

(vi) Ersetzt man die Multiplikation einer Algebra A durch $a * b := ba$, so erhält man die *entgegengesetzte* Algebra A^o. Die Transposition liefert einen Isomorphismus $\varphi\colon (A^{n\times n})^o \cong (A^o)^{n\times n}$, $a \mapsto a^{\mathrm{t}}$, denn

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

für $a, b \in A$. Für Algebren A, B ist die Identität ein Isomorphismus $(A \times B)^o \to A^o \times B^o$.

(vii) Eine kommutative Divisionsalgebra ist ein Körper. Wedderburn hat gezeigt, dass jede endliche Divisionsalgebra ein Körper ist.

(viii) Jeder Schiefkörper R ist eine $\mathrm{Z}(R)$-Divisionsalgebra, denn $\mathrm{Z}(R)$ ist in diesem Fall ein Körper.

Lemma 8.4. *Jede Divisionsalgebra über einem algebraisch abgeschlossenen Körper K ist zu K isomorph.*

Beweis. Sei D eine K-Divisionsalgebra und $x \in D$. Dann sind die Potenzen $1_D, x, x^2, \ldots$ linear abhängig über K. Daher existiert ein normiertes Polynom $\alpha \in K[X] \setminus K$ mit $\alpha(x) = 0$. Da K algebraisch abgeschlossen ist, zerfällt α in Linearfaktoren, etwa $\alpha = (X - \lambda_1) \ldots (X - \lambda_n)$ mit $\lambda_1, \ldots, \lambda_n \in K$. Als Divisionsalgebra besitzt D keine Nullteiler. Aus $\alpha(x) = 0$ folgt also $x = \lambda_i 1_D$ für ein $i \in \{1, \ldots, n\}$. Daher ist $D = K1_D \cong K$. □

Definition 8.5. Sei A eine K-Algebra.

(i) Ein *Ideal* von A ist eine nichtleere Teilmenge $I \subseteq A$ mit $x - y, ax, xa \in I$ für alle $x, y \in I$ und $a \in A$. Man schreibt dann $I \trianglelefteq A$ oder $I \triangleleft A$, falls I ein *echtes* Ideal ist, d. h. $I \neq A$.

(ii) Man nennt A *einfach*, falls $\{0\}$ und A die einzigen Ideale von A sind. Wie üblich verwenden wir die Schreibweise $0 := \{0\}$ für das Nullideal.

(iii) Für $I, J \trianglelefteq A$ sind auch $I + J := \{x + y : x \in I, y \in J\}$, $I \cap J$ und

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

Ideale von A. Dabei gilt $IJ \subseteq I \cap J \subseteq I \cup J \subseteq I + J$.

(iv) Für $I \trianglelefteq A$ sei $I^0 := A$ und $I^{n+1} := I^n I$ für $n \in \mathbb{N}_0$. Man nennt I *nilpotent*, falls ein n mit $I^n = 0$ existiert.

Beispiel 8.6.

(i) Sei $f\colon A \to B$ ein Homomorphismus von Algebren. Für $J \trianglelefteq B$ ist das Urbild $f^{-1}(J) \trianglelefteq A$. Für $I \trianglelefteq A$ ist andererseits $f(I)$ in der Regel *kein* Ideal von B.

(ii) Jede Divisionsalgebra ist einfach.

(iii) Sei $0 \neq I \trianglelefteq A := K^{n\times n}$ und $x = (x_{ij}) \in I$ mit $x_{st} \neq 0$. Sei $E_{st} \in A$ die Matrix mit einer 1 an Position (s, t) und sonst nur Nullen. Dann ist $E_{ij} = x_{st}^{-1} E_{is} x E_{tj} \in I$ für alle $1 \leq i, j \leq n$. Dies zeigt $I = A$. Also ist A einfach, aber keine Divisionsalgebra für $n \geq 2$.

(iv) Sei $A \subseteq K^{n\times n}$ die Unteralgebra aller oberen Dreiecksmatrizen. Die Dreiecksmatrizen mit Nullen auf der Hauptdiagonalen bilden ein nilpotentes Ideal $I \trianglelefteq A$ mit $I^n = 0 \neq I^{n-1}$.

Bemerkung 8.7. Sei $I \trianglelefteq A$, $x \in I$ und $\lambda \in K$. Dann gilt $\lambda x = (\lambda 1_A)x \in I$. Daher ist I ein K-Vektorraum. Bekanntlich ist A/I ein Ring und somit auch eine K-Algebra.

Satz 8.8.

(i) (Homomorphiesatz) Für jeden Homomorphismus $f\colon A \to B$ von Algebren ist $\mathrm{Ker}(f) \trianglelefteq A$ *und $f(A)$ ist eine Unteralgebra von B. Außerdem ist*

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

ein Isomorphismus von Algebren.

(ii) (1. Isomorphiesatz) Sei B eine Unteralgebra von A und $I \trianglelefteq A$. Dann ist $B + I$ eine Unteralgebra von A, $I \trianglelefteq B + I$, $B \cap I \trianglelefteq B$ und

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

(iii) (Korrespondenzsatz) Sei $I \trianglelefteq A$. Dann ist die Abbildung $\{J \trianglelefteq A : I \subseteq J\} \to \{L \trianglelefteq A/I\}$, $J \mapsto J/I$ eine Bijektion.

(iv) (2. Isomorphiesatz) Seien $I, J \trianglelefteq A$ mit $I \subseteq J$. Dann ist

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

Beweis. Nach Algebra ist die Abbildung $F\colon A/\mathrm{Ker}(f) \to f(A)$, $a\mathrm{Ker}(f) \mapsto f(a)$ zumindest ein Ringisomorphismus. Offenbar ist F auch K-linear und somit ein Isomorphismus von Algebren. Die Isomorphiesätze sind Anwendungen des Homomorphiesatzes und gelten daher auch für Algebren. Dies beinhaltet auch die Wohldefiniertheit der Abbildung $f(J) = J/I$ aus dem Korrespondenzsatz. Da J die Vereinigung der Nebenklassen J/I ist, ist f injektiv. Sei nun $L \trianglelefteq A/I$ und $\pi\colon A \to A/I$, $a \mapsto a + I$ der kanonische Epimorphismus. Dann ist $J := \pi^{-1}(L) \trianglelefteq A$ mit $I \subseteq J$ und $f(J) = J/I = \pi(J) = L$. □

Lemma 8.9. *Sind $I, J \trianglelefteq A$ nilpotent, so auch $I + J$.*

Beweis. Sei $n \in \mathbb{N}$ mit $I^n = J^n = 0$. Jedes Element von $(I+J)^{2n}$ hat die Form $z := (x_1+y_1)\dots(x_{2n}+y_{2n})$ mit $x_1, \dots, x_{2n} \in I$ und $y_1, \dots, y_{2n} \in J$. Durch Ausmultiplizieren erhält man eine Summe von Termen der Form $z_1 \dots z_{2n}$ mit $z_1, \dots, z_{2n} \in I \cup J$. O. B. d. A. liegen mindestens n viele der z_i in I. Dann ist $z_1 \dots z_{2n} \in I^n = 0$. Dies zeigt $z = 0$ und $(I + J)^{2n} = 0$. □

Definition 8.10. Sei A eine Algebra.

(i) Die Summe $\mathrm{J}(A)$ aller nilpotenten Ideale von A nennt man das (JACOBSON-)*Radikal* von A. Aus Dimensionsgründen ist $\mathrm{J}(A)$ bereits die Summe von endlich vielen nilpotenten Idealen. Nach Lemma 8.9 ist $\mathrm{J}(A)$ also das größte nilpotente Ideal von A.

(ii) Man nennt A *halbeinfach*, falls $\mathrm{J}(A) = 0$ gilt.

(iii) Man nennt A *lokal*, falls $A/\mathrm{J}(A)$ eine Divisionsalgebra ist.

Beispiel 8.11.

(i) Wegen $1 \in A^n$ für alle $n \in \mathbb{N}$ ist $\mathrm{J}(A) \neq A$. Jede einfache Algebra ist somit halbeinfach. Andererseits ist $K \times K$ halbeinfach, aber nicht einfach, denn $K \times 0 \trianglelefteq K \times K$. Merke:

$$\text{Körper} \implies \text{Divisionsalgebra} \implies \text{einfach} \implies \text{halbeinfach}$$

(ii) Ist A lokal, so ist $\mathrm{J}(A)$ nach dem Korrespondenzsatz ein maximales Ideal von A. In dieser Hinsicht ist lokal das Gegenteil von halbeinfach.

(iii) Sei $A \subseteq K^{n\times n}$ die Algebra der oberen Dreiecksmatrizen mit $n \geq 2$. Dann besteht $\mathrm{J}(A)$ aus den Dreiecksmatrizen mit Nullen auf der Hauptdiagonale. Der Epimorphismus $A \to K^n$, $(a_{ij}) \mapsto (a_{11}, \dots, a_{nn})$ hat Kern $\mathrm{J}(A)$. Insbesondere ist $A/\mathrm{J}(A) \cong K^n$ keine Divisionsalgebra. Also ist A weder halbeinfach noch lokal.

(iv) Die Algebra $A := K[X]/(X^2)$ ist lokal mit $\mathrm{J}(A) = (X)/(X^2)$ und $A/\mathrm{J}(A) \cong K[X]/(X) \cong K$.

Lemma 8.12. *Für Algebren A, B und $n \in \mathbb{N}$ gilt:*

(i) $A/\mathrm{J}(A)$ *ist halbeinfach.*

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

Beweis.

(i) Nach dem Korrespondenzsatz existiert ein Ideal $I \trianglelefteq A$ mit $I/\mathrm{J}(A) = \mathrm{J}(A/\mathrm{J}(A))$. Es existieren $n, m \in \mathbb{N}$ mit $\mathrm{J}(A)^n = 0$ und $I^m \subseteq \mathrm{J}(A)$. Daher ist $I^{nm} = 0$ und $I = \mathrm{J}(A)$.

(ii) Für $(a,b) \in A \times B$ gilt

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

(iii) Wir identifizieren A mit $A \times 0$ und B mit $B \times 0$. Offenbar sind dann $\mathrm{J}(A)$ und $\mathrm{J}(B)$ nilpotente Ideale von $A \times B$. Dies zeigt $\mathrm{J}(A) \times \mathrm{J}(B) = \mathrm{J}(A) + \mathrm{J}(B) \subseteq \mathrm{J}(A \times B) =: J$. Für $(a,b) \in J$ ist $(a,0) = (a,b)(1,0) \in J \cap A$ und $(0,b) \in J \cap B$. Da $J \cap A$ und $J \cap B$ nilpotente Ideale von A bzw. B sind, folgt

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

Also gilt $J \subseteq \mathrm{J}(A) \times \mathrm{J}(B)$.

(iv) Sicher ist $\mathrm{Z}(A)1_n \subseteq \mathrm{Z}(A^{n\times n})$. Sei umgekehrt $M = (a_{ij}) \in \mathrm{Z}(A^{n\times n})$. Dann ist

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

für alle $1 \leq s,t \leq n$ und es folgt $M \in A1_n$. Sicher ist auch $M \in \mathrm{Z}(A1_n) = \mathrm{Z}(A)1_n$.

(v) Sei $J := \mathrm{J}(A)$. Eine Induktion nach k zeigt $(J^{n\times n})^k \subseteq (J^k)^{n\times n}$. Also ist $J^{n\times n}$ nilpotent und $J^{n\times n} \subseteq \mathrm{J}(A^{n\times n})$. Sei umgekehrt $a = (a_{ij})_{i,j} \in \mathrm{J}(A^{n\times n})$. Sei $I = (a_{st}) \trianglelefteq A$ das von a_{st} erzeugte Ideal. Dann ist

$$IE_{11} \subseteq (E_{1s}aE_{t1}) \subseteq \mathrm{J}(A^{n\times n}).$$

Da $\mathrm{J}(A^{n\times n})$ nilpotent ist, muss auch I nilpotent sein. Dies zeigt $a_{st} \in I \subseteq J$ und $\mathrm{J}(A^{n\times n}) \subseteq J^{n\times n}$. □

Definition 8.13. Ein Element e einer Algebra A heißt

- *Idempotent*, falls $e^2 = e$ gilt.
- *nilpotent*, falls $e^n = 0$ für ein $n \in \mathbb{N}$ gilt.

Beispiel 8.14.

(i) In jeder Algebra A sind 0 und 1 Idempotente.

(ii) Ist $e \in A$ ein Idempotent, so auch $1 - e$, denn $(1-e)^2 = 1 - e - e + e^2 = 1 - e$. Für $a \in A^\times$ ist auch aea^{-1} ein Idempotent, denn $(aea^{-1})^2 = aea^{-1}aea^{-1} = ae^2a^{-1} = aea^{-1}$.

(iii) Die Matrizen der Form E_{ii} sind Idempotente in $K^{n\times n}$.

(iv) Offenbar besteht $\mathrm{J}(A)$ aus nilpotenten Elementen. Andererseits ist $E_{12} \in K^{2\times 2}$ nilpotent, aber $\mathrm{J}(K^{2\times 2}) = 0$.

Lemma 8.15 (Heben von Einheiten/Idempotenten)**.** *Sei A eine Algebra und $I \trianglelefteq A$ nilpotent. Dann gilt:*

(i) Ist $e + I \in (A/I)^\times$ eine Einheit, so auch $e \in A^\times$.

(ii) Für jedes Idempotent $\bar{e} \in A/I$ existiert ein Idempotent $e \in A$ mit $e + I = \bar{e}$.

Beweis (Koh).

(i) Sei $a \in A$ mit $ea \equiv 1 \pmod{I}$ und $b := 1 - ea \in I$. Da I nilpotent ist, existiert ein $n \in \mathbb{N}$ mit $b^n = 0$. Dies zeigt

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

Eine analoge Rechnung mit $1 - ae$ ergibt $e \in A^\times$.

(ii) Sei $a \in A$ beliebig mit $a + I = \bar{e}$. Dann ist $(1-a)a = a - a^2 \in I$. Da I nilpotent ist, existiert ein $n \in \mathbb{N}$ mit $(1-a)^n a^n = ((1-a)a)^n = 0$. Sei

$$e := \sum_{i=0}^{n} \binom{2n}{i} (1-a)^i a^{2n-i}, \qquad f := \sum_{i=n+1}^{2n} \binom{2n}{i} (1-a)^i a^{2n-i}.$$

Dann gilt

$$e + f = \sum_{i=0}^{2n} \binom{2n}{i} (1-a)^i a^{2n-i} = ((1-a)+a)^{2n} = 1.$$

Wegen $a^{2n-i}(1-a)^j = 0$ für $0 \leq i \leq n$ und $n+1 \leq j \leq 2n$ gilt $ef = 0$. Dies zeigt $e = e(e+f) = e^2 + ef = e^2$ und $e \equiv a^{2n} \equiv a \pmod{I}$. □

9 Moduln

Bemerkung 9.1. Wir untersuchen in diesem Kapitel „Vektorräume“ über Algebren anstelle von Körpern. Anders als in der linearen Algebra existieren in dieser Situation im Allgemeinen keine Basen (siehe Beispiel 9.3). Selbst wenn Basen existieren, müssen sie nicht gleich groß sein. Die Theorie wird dadurch komplizierter, aber auch reichhaltiger. Stets sei A eine K-Algebra.

Definition 9.2. Ein *A-Modul* ist ein endlich-dimensionaler K-Vektorraum M mit einer Verknüpfung $A \times M \to M$, $(a, m) \mapsto am$, sodass für $a, b \in A$, $m, n \in M$ und $\lambda \in K$ gilt:

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

Beispiel 9.3.

(i) Der *triviale* A-Modul $0 := \{0\}$.

(ii) Ist A ein Körper, so sind die A-Moduln genau die A-Vektorräume.

(iii) Durch die gewöhnliche Multiplikation $A \times A \to A$, $(a, b) \mapsto ab$ wird A zu einem A-Modul, den man den *regulären* A-Modul nennt.

(iv) Für A-Moduln M, N ist auch $M \times N$ ein A-Modul.

(v) Für $n, m \in \mathbb{N}$ ist $K^{n\times m}$ ein $K^{n\times n}$-Modul bzgl. Matrixmultiplikation. Insbesondere ist $K^n := K^{n\times 1}$ ein $K^{n\times n}$-Modul. Für jedes $x \in K^n$ und $A := K^{n\times n}$ gilt $Ax = K^n$ (lineare Algebra), d. h. $\{x\}$ ist ein Erzeugendensystem von K^n. Andererseits existiert ein $a \in A \setminus \{0\}$ mit $ax = 0$, d. h. $\{x\}$ ist linear abhängig. Dies zeigt, dass K^n keine Basis als A-Modul besitzt.

Bemerkung 9.4. Sei M ein A-Modul, $a \in A$ und $m \in M$. Dann gilt wie in der linearen Algebra

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

Definition 9.5.

- Eine Teilmenge N eines A-Moduls M heißt *Untermodul* von M, falls N mit den eingeschränkten Verknüpfungen selbst ein A-Modul ist. Wie bei Gruppen schreiben wir dann $N \leq M$ oder $N < M$, falls $N \neq M$.
- Sind 0 und $M \neq 0$ die einzigen Untermoduln, so nennt man M *einfach*.

Beispiel 9.6.

(i) Wie üblich sind Durchschnitte und Summen von Untermoduln wieder Untermoduln.

(ii) Sei $A = K^{n\times n}$ und $M = K^n$. Für $x, y \in M \setminus \{0\}$ existiert ein $a \in A$ mit $ax = y$ (lineare Algebra). Daher ist M ein einfacher A-Modul. Im Gegensatz zu Vektorräumen sind einfache Moduln also nicht unbedingt 1-dimensional.

(iii) Für A-Moduln $N \leq M$ ist auch der Faktorraum M/N ein A-Modul mit $a(m + N) := am + N$ für $a \in A$, $m + N \in M/N$.

(iv) Für Untermoduln $U, V, W \leq M$ mit $U \leq W$ gilt die Dedekind-*Identität*

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

Definition 9.7. Eine Abbildung $f\colon M \to N$ für A-Moduln M, N heißt *Homomorphismus* (oder A-*linear*), falls $f(ax+y) = af(x) + f(y)$ für $a \in A$ und $x, y \in M$ gilt. Die Menge aller Homomorphismen bezeichnet man mit $\mathrm{Hom}_A(M, N)$. Wie üblich definiert man Mono-, Epi-, Endo-, Iso- und Automorphismen. Abweichend von Gruppen und Algebren schreiben wir $M \simeq N$ oder genauer $M \simeq_A N$ für die Isomorphie von Moduln.

Bemerkung 9.8.

(i) Sei $f\colon M \to N$ ein Homomorphismus von A-Moduln. Für $m \in M$ und $\lambda \in K$ gilt

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

d. h. f ist K-linear.

(ii) Für jeden Homomorphismus $f\colon M \to N$ von A-Moduln ist $\mathrm{Ker}(f) \leq M$ und $f(M) \leq N$. Der Homomorphiesatz, der Korrespondenzsatz und die Isomorphiesätze gelten für Moduln genauso wie für Vektorräume.

(iii) Ist $f\colon M \to N$ ein bijektiver Homomorphismus, so ist auch $f^{-1}\colon N \to M$ ein Homomorphismus, denn
$$f^{-1}(am) = f^{-1}\big(af(f^{-1}(m))\big) = f^{-1}\big(f(af^{-1}(m))\big) = af^{-1}(m)$$
für $m \in M$ und $a \in A$.

(iv) Sind $f, g\colon M \to N$ A-linear, so auch $f+g\colon M \to N$, $m \mapsto f(m)+g(m)$ und $\lambda f\colon M \to N$, $m \mapsto \lambda f(m)$ für $\lambda \in K$. Dadurch wird $\mathrm{Hom}_A(M,N)$ zu einem K-Vektorraum (aber in der Regel kein A-Modul). Im Fall $M = N$ ist auch $f \circ g \in \mathrm{Hom}_A(M,M) =: \mathrm{End}_A(M)$. Wie üblich gilt dann $f \circ (g+h) = f \circ g + f \circ h$ und $(f+g) \circ h = f \circ h + g \circ h$ für $f, g, h \in \mathrm{End}_A(M)$. Auf diese Weise wird $\mathrm{End}_A(M)$ zu einer K-Algebra mit Einselement id_M. Man nennt $\mathrm{End}_A(M)$ die *Endomorphismenalgebra* von M.

(v) Sei M ein A-Modul. Für $a \in A$ ist $f_a\colon M \to M$, $m \mapsto am$ ein Homomorphismus von Vektorräumen (aber nicht von A-Moduln). Wegen $f_{a+b} = f_a + f_b$ und $f_{ab} = f_a \circ f_b$ für $a, b \in A$ ist $f\colon A \to \mathrm{End}_K(M)$, $a \mapsto f_a$ ein Homomorphismus von Algebren. Man nennt f eine *Darstellung* von A. Durch Basiswahl erhält man eine entsprechende *Matrixdarstellung* $A \to K^{n\times n}$.

Lemma 9.9. *Für einfache A-Moduln $M \not\simeq N$ gilt* $\mathrm{Hom}_A(M,N) = 0$ *und* $\mathrm{End}_A(M)$ *ist eine Divisionsalgebra.*

Beweis. Für $f \in \mathrm{Hom}_A(M,N)$ sind $\mathrm{Ker}(f)$ und $f(M)$ Untermoduln von M bzw. N. Im Fall $\mathrm{Ker}(f) = 0$ wäre $M \simeq f(M) = N$. Also ist $\mathrm{Ker}(f) = M$ und $f = 0$. Im Fall $M = N$ ist $f = 0$ oder f ist bijektiv. Daher ist $\mathrm{End}_A(M)$ eine Divisionsalgebra. □

Definition 9.10. Sei M ein A-Modul. Eine Folge von Untermoduln $0 = M_0 < M_1 < \ldots < M_n = M$ heißt *Kompositionsreihe* von M, falls die Faktoren M_i/M_{i-1} für $i = 1, \ldots, n$ einfach sind.

Satz 9.11 (Jordan-Hölder)**.** *Jeder A-Modul besitzt eine Kompositionsreihe. Sind $0 = M_k < \ldots < M_0 = M$ und $0 = N_l < \ldots < N_0 = M$ Kompositionsreihen von M, so ist $k = l$ und es existiert ein $\pi \in S_k$ mit $M_{i-1}/M_i \cong N_{\pi(i)-1}/N_{\pi(i)}$ für $i = 1, \ldots, k$. Man nennt $M_0/M_1, \ldots, M_{k-1}/M_k$ die* Kompositionsfaktoren *von M.*

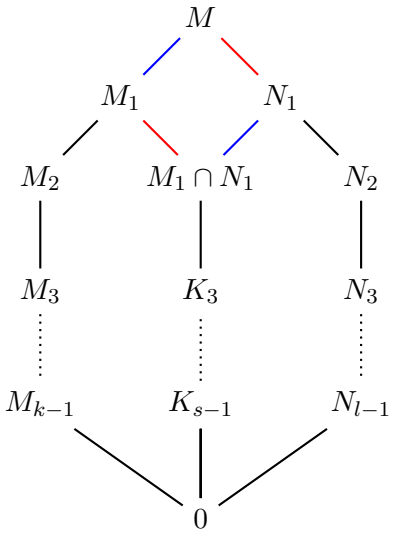
Beweis. Induktion nach $\dim M$: Im Fall $M = 0$ besteht die Kompositionsreihe nur aus M. Sei nun $M \neq 0$ und $L < M$ ein maximaler Untermodul. Nach Induktion besitzt L eine Kompositionsreihe $0 = L_0 < \ldots < L_n = L$. Offensichtlich ist dann $L_0 < \ldots < L_n < M$ eine Kompositionsreihe von M.

Nun zur Eindeutigkeit: Im Fall $M_1 = N_1$ folgt die Behauptung mit Induktion. Sei also $M_1 \neq N_1$. Da M/M_1 einfach ist, ist $M = M_1 + N_1$. Der erste Isomorphiesatz zeigt

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

Sei $0 = K_s < \ldots < K_2 = M_1 \cap N_1$ eine beliebige Kompositionsreihe. Nach Induktion sind dann die Kompositionsreihen $M_k < \ldots < M_1$ und $K_s < \ldots < K_2 < M_1$ gleich lang (d. h. $k = s$) und ihre Faktoren sind (bis auf die Reihenfolge) isomorph. Nun sind auch die Kompositionsreihen $0 = K_k < \ldots < K_2 < N_1$ und $0 = N_l < \ldots < N_1$ gleich lang mit isomorphen Faktoren. Also ist $k = s = l$ und nach (9.1) haben die Kompositionsreihen

$$
\begin{aligned}
&M_k < \ldots < M_0,\\
&K_k < \ldots < K_2 < M_1 < M_0,\\
&K_k < \ldots < K_2 < N_1 < N_0,\\
&N_k < \ldots < N_0
\end{aligned}
$$



isomorphe Faktoren. □

Folgerung 9.12. *Jeder einfache A-Modul ist zu einem Kompositionsfaktor des regulären A-Moduls isomorph. Insbesondere gibt es höchstens* $\dim A$ *viele einfache A-Moduln bis auf Isomorphie.*

Beweis. Sei M ein einfacher A-Modul und $m \in M \setminus \{0\}$. Dann ist die Abbildung $\varphi\colon A \to M$, $a \mapsto am$ ein Epimorphismus. Nach dem Homomorphiesatz ist $M \simeq A/\mathrm{Ker}(\varphi)$. Man kann nun eine Kompositionsreihe von $\mathrm{Ker}(\varphi)$ mit M zu einer Kompositionsreihe von A verlängern. Die zweite Aussage folgt, da jeder einfache Modul mindestens 1-dimensional ist. □

Definition 9.13. Für einen A-Modul M nennt man

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

den *Annullator* von M.

Bemerkung 9.14. Ist $\varphi\colon M \to N$ ein Isomorphismus von A-Moduln, so gilt

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

Satz 9.15. *Sind $M_1, \ldots, M_k$ die einfachen A-Moduln bis auf Isomorphie, so gilt*

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

Beweis. Für jeden A-Modul M und jedes Ideal $I \trianglelefteq A$ ist

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

Insbesondere ist $\mathrm{J}(A)M_i \leq M_i$. Sei $\mathrm{J}(A)^s = 0$. Im Fall $\mathrm{J}(A)M_i = M_i$ wäre $0 = \mathrm{J}(A)^s M_i = \mathrm{J}(A)^{s-1} M_i = \ldots = M_i$. Also ist $\mathrm{J}(A)M_i = 0$ für $i = 1, \ldots, k$, da M_i einfach ist. Dies zeigt $\mathrm{J}(A) \subseteq \mathrm{Ann}(M_1) \cap \ldots \cap \mathrm{Ann}(M_k) =: I$.

Sei $0 = A_0 < \ldots < A_l = A$ eine Kompositionsreihe des regulären A-Moduls. Da A/A_{l-1} zu einem M_i isomorph ist, gilt $I(A/A_{l-1}) = 0$, d. h. $IA \subseteq A_{l-1}$ nach Bemerkung 9.14. Analog gilt $I^2 A \subseteq IA_{l-1} \subseteq A_{l-2}$ und schließlich $I^l = I^l A = 0$. Daher ist I nilpotent und $I \subseteq \mathrm{J}(A)$. □

10 Halbeinfache Moduln

Bemerkung 10.1. Bekanntlich ist jeder endlich-dimensionale Vektorraum eine direkte Summe von einfachen (also 1-dimensionalen) Unterräumen. Wir untersuchen Moduln mit der entsprechenden Eigenschaft. Wieder sei A stets eine K-Algebra.

Satz 10.2. *Für einen A-Modul M sind die folgenden Aussagen äquivalent:*

(1) M ist eine Summe von einfachen Untermoduln.

(2) M ist eine direkte Summe von einfachen Untermoduln.

(3) Für jeden Untermodul $U \leq M$ existiert ein Untermodul $V \leq M$ mit $M = U \oplus V$.

Gegebenenfalls nennt man M halbeinfach.

Beweis.

(1) $\Rightarrow$ (3): Sei $M = M_1 + \ldots + M_k$ mit einfachen Untermoduln $M_1, \ldots, M_k \leq M$. Sei $V \leq M$ mit $U \cap V = 0$, sodass $\dim V$ möglichst groß ist (notfalls $V = 0$). Nehmen wir $U \oplus V < M$ an. Dann existiert $1 \leq i \leq k$ mit $M_i \not\subseteq U + V$. Aus der Einfachheit von M_i folgt $M_i \cap (U + V) = 0$. Sei $u = v + m \in U \cap (V + M_i)$ mit $v \in V$ und $m \in M_i$. Dann ist $u - v = m \in M_i \cap (U + V) = 0$ und $u = v \in U \cap V = 0$. Dies zeigt $U \cap (V + M_i) = 0$ im Widerspruch zur Wahl von V. Also ist $M = U \oplus V$.

(3) $\Rightarrow$ (2): Sei $U := U_1 \oplus \ldots \oplus U_k$ eine direkte Summe von einfachen Untermoduln $U_1, \ldots, U_k \leq M$, sodass $\dim U$ möglichst groß ist. Nehmen wir $U < M$ an. Dann existiert $V \leq M$ mit $M = U \oplus V$. Aus Dimensionsgründen existiert ein einfacher Untermodul $N \leq M$ mit $N \leq V$. Dann wäre aber $U + N = U \oplus N$ im Widerspruch zur Wahl von U.

(2) $\Rightarrow$ (1): Trivial. □

Beispiel 10.3.

(i) Jeder einfache A-Modul ist halbeinfach.

(ii) Ist $M = M_1 \oplus \ldots \oplus M_k$ eine Zerlegung in einfache Moduln, so ist $0 < M_1 < M_1 \oplus M_2 < \ldots < M$ eine Kompositionsreihe von M. Daher sind $M_1, \ldots, M_k$ die Kompositionsfaktoren von M.

(iii) Sind $M_1, \ldots, M_k$ halbeinfache A-Moduln, so auch $M_1 \times \ldots \times M_k$.

(iv) Sei $A = K^{2\times 2}$. Dann ist der reguläre A-Modul halbeinfach als Summe der einfachen Moduln $\left\{\left(\begin{smallmatrix} * & 0 \\ * & 0 \end{smallmatrix}\right)\right\} \simeq K^2 \simeq \left\{\left(\begin{smallmatrix} 0 & * \\ 0 & * \end{smallmatrix}\right)\right\}$ (Beispiel 9.6). Beachte: Als Algebra ist A einfach, als Modul aber nicht.

(v) Sei A die Algebra der oberen 2×2-Dreiecksmatrizen. Dann ist K^2 nicht halbeinfach, denn der Untermodul $K\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ besitzt kein Komplement.

Lemma 10.4. *Untermoduln und Faktormoduln von halbeinfachen A-Moduln sind halbeinfach.*

Beweis. Sei M ein halbeinfacher A-Modul und $N \leq M$. Für $L \leq N$ existiert ein $L_1 \leq M$ mit $M = L \oplus L_1$. Dann gilt $N = L + (L_1 \cap N)$ mit $L \cap (L_1 \cap N) = (L \cap L_1) \cap N = 0$ nach Dedekind. Daher ist $L_1 \cap N$ ein Komplement von L in N und N ist halbeinfach. Für einen einfachen Untermodul $S \leq M$ ist $(S+N)/N \simeq S/(S \cap N)$ einfach oder trivial. Mit M ist daher auch M/N eine Summe von einfachen Untermoduln. Also ist M/N halbeinfach. □

Satz 10.5. *Für jede Algebra A sind folgende Aussagen äquivalent:*

(1) A ist halbeinfach.

(2) Der reguläre A-Modul ist halbeinfach.

(3) Jeder A-Modul ist halbeinfach.

Beweis.

(1) ⇒ (2): Seien $M_1, \ldots, M_n$ die einfachen A-Moduln bis auf Isomorphie. Sei $x_1, \ldots, x_k \in M_i$ eine K-Basis von M_i. Dann ist $A \to M_i^k$, $a \mapsto a(x_1, \ldots, x_k)$ ein Homomorphismus mit Kern $\mathrm{Ann}(M_i)$. Als Untermodul von M_i^k ist $A/\mathrm{Ann}(M_i)$ halbeinfach nach Lemma 10.4. Nach Satz 9.15 ist die Abbildung

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

ein Monomorphismus. Daher ist auch der reguläre A-Modul halbeinfach.

(2) ⇒ (3): Sei M ein A-Modul mit K-Basis $m_1, \ldots, m_k \in M$. Dann ist $A^k \to M$, $(a_1, \ldots, a_k) \mapsto a_1 m_1 + \ldots + a_k m_k$ ein Epimorphismus. Da A^k halbeinfach ist, muss nach Lemma 10.4 auch M halbeinfach sein.

(3) ⇒ (1): Da der reguläre A-Modul halbeinfach ist, existieren einfache A-Moduln $M_1, \ldots, M_k$ mit $A = M_1 \oplus \ldots \oplus M_k$. Sei $1 = m_1 + \ldots + m_k$ mit $m_i \in M_i$. Für $x \in \mathrm{J}(A) \subseteq \mathrm{Ann}(M_1) \cap \ldots \cap \mathrm{Ann}(M_k)$ gilt $x = x1 = xm_1 + \ldots + xm_k = 0$. Daher ist $\mathrm{J}(A) = 0$ und A ist halbeinfach. □

Lemma 10.6. *Für A-Moduln M, M', N, N' gilt*

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

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

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

Beweis.

(i) Offenbar ist die Abbildung

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

K-linear. Wegen $(f \circ g)(1) = f(g(1)) = f(g(1) \cdot 1) = g(1)f(1)$ ist Φ ein Homomorphismus von Algebren. Wegen $f(a) = f(a1) = af(1)$ für $a \in A$ ist f durch $f(1)$ bereits eindeutig bestimmt. Daher ist Φ injektiv. Sei umgekehrt $a \in A$ beliebig. Dann ist die Abbildung $f_a \colon A \to A$, $b \mapsto ba$ ein Homomorphismus mit $f_a(1) = a$. Dies zeigt die Surjektivität von Φ.

(ii) Für $i = 1, \dots, n$ sind die Abbildungen

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

A-linear. Es gilt

$$\pi_i \rho_j = \begin{cases} \mathrm{id}_M & \text{falls } i = j, \\ 0 & \text{falls } i \neq j, \end{cases} \qquad \mathrm{id}_{M^n} = \sum_{i=1}^{n} \rho_i \pi_i.$$

Wir definieren $\Phi \colon \mathrm{End}_A(M^n) \to \mathrm{End}_A(M)^{n \times n}$, $f \mapsto (\pi_i f \rho_j)_{i,j=1}^n$. Dann ist $\Phi(\mathrm{id}) = (\pi_i \rho_j)_{i,j} = 1_n$ und $\Phi(f + g) = \Phi(f) + \Phi(g)$ für $f, g \in \mathrm{End}_A(M^n)$. Außerdem ist

$$\Phi(fg) = (\pi_i f \,\mathrm{id}\, g \rho_j)_{i,j} = \Big(\pi_i f \sum_{k=1}^{n} \rho_k \pi_k g \rho_j\Big)_{i,j} = (\pi_i f \rho_j)_{i,j} (\pi_i g \rho_j)_{i,j} = \Phi(f)\Phi(g).$$

Daher ist Φ ein Homomorphismus von Algebren. Für $\Phi(f) = 0$ ist auch

$$f = \Big(\sum_{i=1}^{n} \rho_i \pi_i\Big) f \Big(\sum_{j=1}^{n} \rho_j \pi_j\Big) = \sum_{i,j=1}^{n} \rho_i (\pi_i f \rho_j) \pi_j = 0$$

und Φ ist injektiv. Sei schließlich $(f_{ij})_{i,j} \in \mathrm{End}_A(M)^{n \times n}$ gegeben. Dann ist $f := \sum_{i,j=1}^n \rho_i f_{ij} \pi_j \in \mathrm{End}_A(M^n)$ mit

$$\Phi(f) = \Big(\pi_i \sum_{k,l=1}^{n} \rho_k f_{kl} \pi_l \rho_j\Big)_{i,j} = (\mathrm{id}\, f_{ij}\, \mathrm{id})_{i,j} = (f_{ij})_{i,j}.$$

Also ist Φ surjektiv.

(iii) Ähnlich wie in (ii) sei $\Phi \colon \mathrm{End}_A(M \times N) \to \mathrm{End}_A(M) \times \mathrm{End}_A(N)$, $f \mapsto (\pi_1 f \rho_1, \pi_2 f \rho_2)$. Man zeigt leicht, dass Φ ein Homomorphismus von Algebren ist. Sei $\Phi(f) = 0$. Wegen

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

ist auch

$$f = (\rho_1 \pi_1 + \rho_2 \pi_2) f (\rho_1 \pi_1 + \rho_2 \pi_2) = 0$$

und Φ ist injektiv. Für $(f_1, f_2) \in \mathrm{End}_A(M) \times \mathrm{End}_A(N)$ sei $f \colon = \rho_1 f_1 \pi_1 + \rho_2 f_2 \pi_2 \in \mathrm{End}_A(M \times N)$. Dann ist

$$\Phi(f) = \big(\pi_1(\rho_1 f_1 \pi_1 + \rho_2 f_2 \pi_2)\rho_1, \pi_2(\rho_1 f_1 \pi_1 + \rho_2 f_2 \pi_2)\rho_2\big) = (f_1, f_2).$$

Daher ist Φ surjektiv.

(iv) Man zeigt leicht, dass die Abbildungen

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

zueinander inverse Isomorphismen von K-Vektorräumen sind.

(v) Analog. □

Satz 10.7 (Artin-Wedderburn)**.** *Eine Algebra A ist genau dann halbeinfach, wenn Divisionsalgebren $D_1, \ldots, D_k$ und $n_1, \ldots, n_k \in \mathbb{N}$ mit*

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

existieren. Ggf. sind $n_1, \ldots, n_k$ die Vielfachheiten und $\dim(D_1)n_1, \ldots, \dim(D_k)n_k$ die Dimensionen der einfachen Moduln als Kompositionsfaktoren des regulären A-Moduls.

Beweis. Sei A halbeinfach. Nach Satz 10.5 gilt $A \simeq M_1^{n_1} \oplus \ldots \oplus M_k^{n_k}$ mit paarweise nicht-isomorphen einfachen A-Moduln $M_1, \ldots, M_k$. Nach Lemma 9.9 ist $\mathrm{Hom}_A(M_i, M_j) = 0$ für $i \neq j$ und $D_i := \mathrm{End}_A(M_i)^o$ ist eine Divisionsalgebra für $i = 1, \ldots, k$. Aus Lemma 10.6 folgt $\mathrm{Hom}_A(M_i^{n_i}, M_j^{n_j}) \simeq_K \mathrm{Hom}_A(M_i, M_j)^{n_i n_j} = 0$ und

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

Sei umgekehrt $A \cong D_1^{n_1 \times n_1} \times \ldots \times D_k^{n_k \times n_k}$. Nach Lemma 8.12 gilt

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

d. h. A ist halbeinfach. Wie in Beispiel 9.6 zeigt man, dass $D_i^{n_i}$ ein einfacher $D_i^{n_i \times n_i}$-Modul ist. Sicher ist dann

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

ein einfacher Untermodul des regulären A-Moduls mit Dimension $\dim(D_i)n_i$. Außerdem ist A die direkte Summe dieser Moduln, wobei $M_{i,1} \simeq \ldots \simeq M_{i,n_i}$. Für $i \neq j$ gilt $M_{i,1} \not\simeq M_{j,1}$, denn die Annullatoren sind verschieden (Bemerkung 9.14). Also tritt $M_{i,1}$ mit Vielfachheit n_i im regulären A-Modul auf. □

Bemerkung 10.8. Wegen $D_1^{n_1 \times n_1} \trianglelefteq D_1^{n_1 \times n_1} \times \ldots \times D_k^{n_k \times n_k}$ gilt: Genau dann ist A einfach, wenn eine Divisionsalgebra D und $n \in \mathbb{N}$ mit $A \cong D^{n \times n}$ existiert. Dieser Spezialfall wurde von Wedderburn bewiesen.

11 Unzerlegbare Moduln

Bemerkung 11.1. Weiterhin sei A eine K-Algebra. Ist ein A-Modul M nicht halbeinfach, so kann man M dennoch in möglichst kleine Untermoduln $M = M_1 \oplus \ldots \oplus M_k$ zerlegen. Wir untersuchen die Eigenschaften einer solchen Zerlegung.

Definition 11.2. Sei $M \neq 0$ ein A-Modul. Man nennt M *zerlegbar*, falls Untermoduln $M_1, M_2 < M$ mit $M = M_1 \oplus M_2$ existieren. Anderenfalls nennt man M *unzerlegbar*.

Beispiel 11.3.

(i) Jeder einfache Modul ist unzerlegbar.

(ii) Der 2-dimensionale Modul K^2 von $A = \left\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\right\}$ aus Beispiel 10.3 ist unzerlegbar, da er sonst halbeinfach wäre.

Satz 11.4. *Für jede Algebra A sind die folgenden Aussagen äquivalent:*

(1) A ist lokal.

(2) Jedes Element in A ist invertierbar oder nilpotent.

(3) 0 und 1 sind die einzigen Idempotente von A.

Beweis.

(1) $\Rightarrow$ (2): Jedes Element in $\mathrm{J}(A)$ ist nilpotent. Sei $a \in A \setminus \mathrm{J}(A)$. Da $A/\mathrm{J}(A)$ eine Divisionsalgebra ist, ist $a + \mathrm{J}(A) \in (A/\mathrm{J}(A))^\times$. Nach Lemma 8.15 gilt $a \in A^\times$.

(2) $\Rightarrow$ (3): Sei $e = e^2 \in A$. Im Fall $e \in A^\times$ ist $e = eee^{-1} = ee^{-1} = 1$. Anderenfalls ist $e^n = 0$ für ein $n \in \mathbb{N}$. Dann folgt $e = e^2 = \ldots = e^n = 0$.

(3) $\Rightarrow$ (1): Nach Lemma 8.15 besitzt die halbeinfache Algebra $A/\mathrm{J}(A)$ nur die Idempotente 0 und 1. Jede Komponente $D^{n\times n}$ in der Artin-Wedderburn-Zerlegung von $A/\mathrm{J}(A)$ liefert aber (mindestens) n Idempotente $E_{11}, \ldots, E_{nn}$ nach Beispiel 8.14. Daher muss $A/\mathrm{J}(A)$ selbst eine Divisionsalgebra sein. □

Lemma 11.5 (Fitting)**.** *Sei M ein A-Modul und $f \in \mathrm{End}_A(M)$. Dann existiert ein $k \in \mathbb{N}$ mit $M = \mathrm{Ker}(f^k) \oplus f^k(M)$.*

Beweis. Aus Dimensionsgründen werden die Folgen $\mathrm{Ker}(f) \subseteq \mathrm{Ker}(f^2) \subseteq \ldots$ und $f(M) \supseteq f^2(M) \supseteq \ldots$ konstant. Sei $k \in \mathbb{N}$ mit $\mathrm{Ker}(f^k) = \mathrm{Ker}(f^{k+1}) = \ldots$ und $f^k(M) = f^{k+1}(M) = \ldots$. Für $x \in \mathrm{Ker}(f^k) \cap f^k(M)$ existiert $y \in M$ mit $f^k(y) = x$. Aus $f^{2k}(y) = f^k(x) = 0$ folgt $y \in \mathrm{Ker}(f^{2k}) = \mathrm{Ker}(f^k)$ und $x = f^k(y) = 0$. Also gilt $\mathrm{Ker}(f^k) \cap f^k(M) = 0$. Die Behauptung folgt aus

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

Satz 11.6. *Ein A-Modul $M \neq 0$ ist genau dann unzerlegbar, wenn $\mathrm{End}_A(M)$ lokal ist.*

Beweis. Sei M unzerlegbar. Angenommen $E := \mathrm{End}_A(M)$ besitzt ein Idempotent $e \notin \{0, 1\}$. Nach Fitting gilt $M = e(M) \oplus \mathrm{Ker}(e)$. Wegen $e \neq 0$ ist $\mathrm{Ker}(e) < M$. Da M unzerlegbar ist, folgt $e(M) = M$, d. h. e ist invertierbar. Dann wäre aber $e = 1$. Also ist E lokal nach Satz 11.4.

Sei umgekehrt E lokal und $M = M_1 \oplus M_2$. Sei $\pi_1 \colon M \to M$, $m_1 + m_2 \mapsto m_1$ die Projektion auf M_1. Offenbar ist $\pi_1 \in E$ ein Idempotent und es folgt $\pi_1 \in \{0, \mathrm{id}_M\}$ aus Satz 11.4. Dies zeigt $M_2 = M$ oder $M_1 = M$, d. h. M ist unzerlegbar. □

Folgerung 11.7. *Eine Algebra A ist genau dann lokal, wenn der reguläre A-Modul unzerlegbar ist.*

Beweis. Folgt aus $\mathrm{End}_A(A) \cong A^o$ (Lemma 10.6). □

Satz 11.8 (Krull-Schmidt)**.** *Jeder A-Modul M besitzt eine Zerlegung in unzerlegbare Moduln $M = M_1 \oplus \ldots \oplus M_k$, die bis auf Reihenfolge und Isomorphie eindeutig bestimmt sind.*

Beweis. Die Existenz folgt leicht mit Induktion nach $\dim M$. Seien $M = M_1 \oplus \ldots \oplus M_k = N_1 \oplus \ldots \oplus N_l$ Zerlegungen in unzerlegbare Moduln. Induktion nach k: Für $k = 1$ ist M unzerlegbar und $l = 1$. Sei also $k \geq 2$. Sei $\pi_i \colon M \to M_i$ die i-te Projektion der ersten Zerlegung und $\rho \colon M \to N_1$ die erste Projektion der zweiten Zerlegung. Dann ist

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

Nicht alle Summanden auf der rechten Seite können in $\mathrm{J}(\mathrm{End}_A(N_1))$ liegen. Nach Satz 11.6 und Satz 11.4 ist mindestens ein Summand, sagen wir $\tau := (\rho \circ \pi_1)_{|N_1}$, invertierbar. Insbesondere ist $(\pi_1)_{|N_1}$ injektiv und $\rho_{|M_1}$ surjektiv. Für $\sigma := \pi_1 \circ \tau^{-1} \circ \rho_{|M_1} \in \mathrm{End}_A(M_1)$ gilt offenbar

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

Aus Satz 11.6 und Satz 11.4 folgt $\sigma = \mathrm{id}_{M_1}$. Daher ist $(\pi_1)_{|N_1}$ auch surjektiv. Dies zeigt $N_1 \simeq M_1$. Für $x \in M_1$ existiert $y \in N_1$ mit $\pi_1(x) = x = \pi_1(y)$ und $x - y \in \mathrm{Ker}(\pi_1) = M_2 + \ldots + M_k$. Es folgt $M = N_1 + M_2 + \ldots + M_k$. Für $x \in N_1 \cap (M_2 + \ldots + M_k)$ ist $\pi_1(x) = 0$ und $x = 0$, da $(\pi_1)_{|N_1}$ injektiv ist. Damit ist

$$M = N_1 \oplus M_2 \oplus \ldots \oplus M_k$$

gezeigt. Wegen $M_2 \oplus \ldots \oplus M_k \simeq M/N_1 \simeq N_2 \oplus \ldots \oplus N_l$ folgt die Behauptung nun durch Induktion. □

Definition 11.9. Für eine K-Algebra A sei

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

der *Kommutatorraum* von A.

Bemerkung 11.10. Achtung: $\gamma(A)$ ist weder ein Ideal noch ein Teilring von A.

Lemma 11.11. *Für K-Algebren A, B gilt:*

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

(ii) Für $I \trianglelefteq A$ gilt $\gamma(A/I) = (\gamma(A) + I)/I$.

(iii) Für $n \in \mathbb{N}$ gilt $\gamma(K^{n\times n}) = \{M \in K^{n\times n} : \mathrm{tr}\, M = 0\}$. *Insbesondere ist* $\dim_K(K^{n\times n}/\gamma(K^{n\times n})) = 1$.

Beweis.

(i) Sicher gilt $\gamma(A) \times \gamma(B) = (\gamma(A) \times 0) + (0 \times \gamma(B)) \subseteq \gamma(A \times B)$. Für $a_1, a_2 \in A$ und $b_1, b_2 \in B$ gilt

$$(a_1, b_1)(a_2, b_2) - (a_2, b_2)(a_1, b_1) = (a_1a_2 - a_2a_1, b_1b_2 - b_2b_1) \in \gamma(A) \times \gamma(B).$$

(ii) Für $a, b \in A$ ist $(a + I)(b + I) - (b + I)(a + I) = ab - ba + I \in \gamma(A) + I$.

(iii) Für $a, b \in K^{n\times n}$ gilt $\mathrm{tr}(ab - ba) = \mathrm{tr}(ab) - \mathrm{tr}(ba) \overset{(2.1)}{=} 0$, d. h. $\gamma(K^{n\times n}) \subseteq \mathrm{Ker}(\mathrm{tr})$. Sei wie üblich $E_{st} = (\delta_{is}\delta_{jt})_{i,j} \in K^{n\times n}$. Für $s \neq t$ gilt

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

Offenbar bilden die Matrizen E_{st} $(s \neq t)$ und $E_{11} - E_{ss}$ $(2 \leq s \leq n)$ eine Basis von $\mathrm{Ker}(\mathrm{tr})$. Daher gilt $\mathrm{Ker}(\mathrm{tr}) \subseteq \gamma(K^{n\times n})$. Die zweite Behauptung folgt aus dem Homomorphiesatz für tr. □

Lemma 11.12. *Sei A eine K-Algebra und $p := \operatorname{char} K > 0$. Für $a, b \in A$ gilt:*

(i) $(a+b)^p \equiv a^p + b^p \pmod{\gamma(A)}$.

(ii) $a \in \gamma(A) \Longrightarrow a^p \in \gamma(A)$.

(iii) $\mathrm{J}(A) + \gamma(A) = \left\{a \in A : \exists n \in \mathbb{N}_0 : a^{p^n} \in \gamma(A)\right\}$, *falls K algebraisch abgeschlossen ist.*

Beweis.

(i) Wenn man $(a+b)^p$ ausmultipliziert erhält man die Summe aller 2^p Terme der Form $c_1 \dots c_p$ mit $c_1, \dots, c_p \in \{a, b\}$.[12] Wegen

$$c_1 \dots c_p \equiv c_2 \dots c_p c_1 \equiv \dots \equiv c_p c_1 \dots c_{p-1} \pmod{\gamma(A)}$$

gilt

$$c_1 \dots c_p + c_2 \dots c_p c_1 + \dots + c_p c_1 \dots c_{p-1} \equiv p c_1 \dots c_p \equiv 0 \pmod{\gamma(A)}.$$

Modulo $\gamma(A)$ verbleiben in $(a+b)^p$ also nur die beiden Terme a^p und b^p.

(ii) Nach (i) können wir $a = bc - cb$ mit $c \in A$ annehmen. Dann gilt

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

(iii) Sei $a \equiv b \pmod{\gamma(A)}$. Nach (i) und (ii) gilt $a^p - b^p \equiv (a-b)^p \equiv 0 \pmod{\gamma(A)}$. Für beliebige $a, b \in A$ ist daher $(a+b)^{p^2} \equiv (a^p + b^p)^p \equiv a^{p^2} + b^{p^2} \pmod{\gamma(A)}$ und induktiv $(a+b)^{p^n} \equiv a^{p^n} + b^{p^n} \pmod{\gamma(A)}$ für $n \in \mathbb{N}$. Dies zeigt, dass

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

ein Vektorraum mit $\gamma(A) \subseteq T$ ist. Da $\mathrm{J}(A)$ nilpotent ist, gilt $\mathrm{J}(A) \subseteq T$, also $\mathrm{J}(A) + \gamma(A) \subseteq T$. Nach Artin-Wedderburn und Lemma 8.4 ist $A/\mathrm{J}(A) \cong K^{n_1 \times n_1} \times \dots \times K^{n_k \times n_k}$. Zusammen mit Lemma 11.11 ergibt sich

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

und $\dim A/(\gamma(A) + \mathrm{J}(A)) = k$. Andererseits sind die Idempotente

$$(E_{11}, 0, \dots, 0), \dots, (0, \dots, 0, E_{11}) \in K^{n_1 \times n_1} \times \dots \times K^{n_k \times n_k}$$

offenbar linear unabhängig modulo T. Dies zeigt $\dim A/T \geq k$ und $T = \gamma(A) + \mathrm{J}(A)$. □

Folgerung 11.13. *Sei K algebraisch abgeschlossen mit Charakteristik $p > 0$. Dann ist*

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

die Anzahl der einfachen A-Moduln bis auf Isomorphie.

Beweis. Nach Aufgabe 22 ist jeder einfache A-Modul auch ein einfacher $A/\mathrm{J}(A)$-Modul. Nach Artin-Wedderburn und (11.1) ist $\dim A/(\gamma(A) + \mathrm{J}(A))$ die Anzahl der einfachen A-Moduln. Die zweite Gleichung folgt aus Lemma 8.12. □

[12] Da a und b nicht unbedingt vertauschbar sind, darf man die binomische Formel nicht benutzen.

12 Gruppenalgebren

Bemerkung 12.1. In Kapitel 2 haben wir gesehen, dass $\mathbb{C}$-Darstellungen einer Gruppe G im Wesentlichen durch ihren Charakter bestimmt sind. Über Körpern mit Charakteristik $p > 0$ ist dies im Allgemeinen falsch, denn der Charakter einer Darstellung der Form $\Delta \oplus \ldots \oplus \Delta$ mit p Summanden ist die Nullabbildung. Wir führen in diesem Kapitel eine Algebra ein, die alle darstellungstheoretischen Informationen von G enthält.

Definition 12.2. Sei KG die Menge aller Abbildungen $G \to K$. Durch

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

wird KG zu einer K-Algebra. Die Assoziativität der Multiplikation folgt aus

$$\begin{aligned}((\alpha\beta)\gamma)(g) &= \sum_{h\in G}(\alpha\beta)(h)\gamma(h^{-1}g) = \sum_{h\in G}\sum_{k\in G}\alpha(k)\beta(k^{-1}h)\gamma(h^{-1}g)\\ &= \sum_{\substack{x,y,z\in G\\ xyz=g}} \alpha(x)\beta(y)\gamma(z) = \ldots = (\alpha(\beta\gamma))(g)\end{aligned}$$

für $\alpha,\beta,\gamma \in KG$ und $g \in G$ (die anderen Axiome sind leicht). Man nennt KG die *Gruppenalgebra* von G über K. Seine Elemente schreibt man meist als formale Linearkombinationen $\alpha = \sum_{g\in G} \alpha_g g$, wobei $\alpha_g = \alpha(g) \in K$. Die Multiplikation funktioniert dann wie bei Polynomen:

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

Indem wir $g \in G$ mit $1_K g$ identifizieren, können wir G als Teilmenge von KG auffassen. Dann ist 1_G das Einselement von KG und G ist eine K-Basis von KG. Insbesondere ist $\dim_K KG = |G|$. Außerdem ist KG genau dann kommutativ, wenn G abelsch ist.

Beispiel 12.3. Für $x := (1,2)+(1,3) \in \mathbb{F}_2 S_3$ gilt

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

Bemerkung 12.4.

(i) Jede Darstellung $\Delta\colon G \to \mathrm{GL}(V)$ von G lässt sich linear zu einer Darstellung

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

von KG fortsetzen. Auf diese Weise wird V zu einem KG-Modul (Bemerkung 9.8). Umgekehrt erhält man aus einem KG-Modul $V \neq 0$ durch Einschränken eine Darstellung von G.

(ii) Darstellungen $\Delta\colon G \to \mathrm{GL}(V)$ und $\Gamma\colon G \to \mathrm{GL}(W)$ sind genau dann ähnlich, wenn ein Vektorraum-Isomorphismus $f\colon V \to W$ mit $f \circ \Delta(g) = \Gamma(g) \circ f$ für alle $g \in G$ existiert. Für $v \in V$ bedeutet dies $f(gv) = gf(v)$, d. h. f ist ein Isomorphismus von KG-Moduln. Daher entsprechen sich die Ähnlichkeitsklassen von Darstellungen von G und die Isomorphieklassen von KG-Moduln. Achtung: Die triviale Darstellung $\mathbb{1}_G$ entspricht dem 1-dimensionalen Modul K. Im Gegensatz zu beliebigen Algebren werden wir K in diesem Zusammenhang als den *trivialen Modul* bezeichnen. Die Existenz dieses Moduls unterscheidet Gruppenalgebren von beliebigen Algebren. Zum Beispiel ist $K^{2\times 2}$ zu keiner Gruppenalgebra isomorph.

(iii) Sei Δ eine Darstellung zum KG-Modul V. Die Δ-invarianten Unterräume sind dann genau die Untermoduln von V. Daher ist Δ genau dann irreduzibel, wenn V einfach ist.

Satz 12.5 (Maschke)**.** *Genau dann ist KG halbeinfach, falls* $\operatorname{char} K$ *kein Teiler von $|G|$ ist.*

Beweis. Sei $\operatorname{char} K \nmid |G|$. Nach Satz 1.9 ist jeder KG-Modul halbeinfach. Nach Satz 10.5 ist auch die Algebra KG halbeinfach. Ist $|G|$ durch $\operatorname{char} K$ teilbar, so ist KG nach Aufgabe 1 nicht halbeinfach. □

Beispiel 12.6.

(i) Sei $\operatorname{char} K \nmid |G|$. Artin-Wedderburn liefert Divisionsalgebren $D_1, \ldots, D_k$ und $n_1, \ldots, n_k \in \mathbb{N}$ mit $KG \cong D_1^{n_1\times n_1} \times \ldots \times D_k^{n_k \times n_k}$. Wegen des trivialen Moduls kann man $D_1^{n_1\times n_1} = K$ annehmen. Außerdem gilt

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

Ist K algebraisch abgeschlossen, so ist $D_i \cong K$ für $i = 1, \ldots, k$ nach Lemma 8.4. Man erhält dann $|G| = n_1^2 + \ldots + n_k^2$ wie in Bemerkung 2.15. Ist G abelsch, so sind $D_1, \ldots, D_k$ Körper und $n_1 = \ldots = n_k = 1$.

(ii) Ist G abelsch der Ordnung n, so gilt $\mathbb{C}G \cong \mathbb{C}^n$ nach Bemerkung 12.4. Der Isomorphietyp von G lässt sich also nicht aus $\mathbb{C}G$ bestimmen.

(iii) Nach Beispiel 7.4 besitzt C_3 eine irreduzible $\mathbb{R}$-Darstellung vom Grad 2. Da C_3 abelsch ist, folgt leicht $\mathbb{R}C_3 \cong \mathbb{R} \times \mathbb{C}$. Da die $\mathbb{Q}$-Darstellungen von D_6 und D_8 absolut irreduzibel sind, gilt $\mathbb{Q}S_3 \cong \mathbb{Q}D_6 \cong \mathbb{Q}^{2\times 2} \times \mathbb{Q}^2$ und $\mathbb{Q}D_8 \cong \mathbb{Q}^{2\times 2} \times \mathbb{Q}^4$. Ohne Beweis sei erwähnt: $\mathbb{R}Q_8 \cong \mathbb{R}^4 \times \mathbb{H}$.

(iv) Für $G = \langle g \rangle \cong C_n$ ist $\mathbb{Q}[X] \to \mathbb{Q}G$, $X \mapsto g$ ein Epimorphismus von Algebren mit Kern $(X^n - 1)$. Bekanntlich gilt $X^n - 1 = \prod_{d|n} \Phi_d$, wobei Φ_d die (irreduziblen) Kreisteilungspolynome sind. Da die Φ_d paarweise teilerfremd sind, ist

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

ein Isomorphismus (chinesischer Restsatz für Ringe). Schließlich ist $\mathbb{Q}[X]/(\Phi_d) \cong \mathbb{Q}_d$ der d-te Kreisteilungskörper. Insgesamt erhält man die Artin-Wedderburn-Zerlegung

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

Die Anzahl der einfachen $\mathbb{Q}G$-Moduln ist also die Anzahl der Teiler von n.

Satz 12.7 (Burnside)**.** *Für jede Darstellung $\Delta\colon G \to \mathrm{GL}(n,K)$ über einem Zahlkörper K sind die folgenden Aussagen äquivalent:*

(1) Δ *ist absolut irreduzibel.*

(2) $\mathrm{C}_{K^{n\times n}}(\Delta(G)) = K1_n$.

(3) $\Delta(KG) = K^{n\times n}$.

Beweis.

(1) $\Rightarrow$ (2): Nach Schurs Lemma gilt

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

(2) $\Rightarrow$ (1): Ist Δ als $\mathbb{C}$-Darstellung reduzibel, so existiert eine $\mathbb{C}$-Basis mit $\Delta(g) = \left(\begin{smallmatrix}\Delta_1(g) & 0\\ 0 & \Delta_2(g)\end{smallmatrix}\right)$ für $g \in G$ und $\mathbb{C}$-Darstellungen Δ_1, Δ_2. Dann wäre aber $\left(\begin{smallmatrix}\Delta_1(1) & 0\\ 0 & 0\end{smallmatrix}\right) \in \mathrm{C}_{K^{n\times n}}(\Delta(G)) \setminus K1_n$ (beachte, dass (2) nicht von der Basiswahl abhängt).

(1) $\Rightarrow$ (3): Sind Matrizen linear unabhängig über $\mathbb{C}$, so erst recht über K. Daher gilt

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

Wir können also $K = \mathbb{C}$ annehmen. Sei $V := \mathbb{C}^n$ der zu Δ gehörende $\mathbb{C}G$-Modul. Dann ist $\mathrm{Ann}(V)$ der Kern von $\Delta\colon \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(V) \cong \mathbb{C}^{n\times n}$. Insbesondere ist $\dim \mathbb{C}G/\mathrm{Ann}(V) \leq n^2$. Seien $V = V_1, \ldots, V_k$ die einfachen $\mathbb{C}G$-Moduln bis auf Isomorphie. Nach Satz 9.15 ist $\mathbb{C}G \to \times_{i=1}^k \mathbb{C}G/\mathrm{Ann}(V_i)$ ein Monomorphismus. Wegen

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

muss Δ surjektiv sein.

(3) $\Rightarrow$ (1): Angenommen Δ ist als $\mathbb{C}$-Darstellung reduzibel. Nach geeigneter Basiswahl besteht $\Delta(\mathbb{C}G)$ dann aus Matrizen der Form $\left(\begin{smallmatrix}A & 0\\ 0 & B\end{smallmatrix}\right)$. Dies widerspricht (3). □

Definition 12.8. Für eine Konjugationsklasse C von G sei $C^+ := \sum_{g\in C} g \in KG$ die *Klassensumme* von C.

Satz 12.9. *Die Klassensummen bilden eine K-Basis von* $\mathrm{Z}(KG)$*. Insbes. ist* $\boxed{\dim_K \mathrm{Z}(KG) = k(G).}$

Beweis. Für $g \in G$ und $C \in \mathrm{Cl}(G)$ gilt

$$gC^+ = \sum_{c\in C} gc = \sum_{c\in C} gcg^{-1}g = \sum_{d\in C} dg = C^+g.$$

Dies zeigt $C^+ \in \mathrm{Z}(KG)$. Sei umgekehrt $\alpha = \sum_{g\in G} \alpha_g g \in \mathrm{Z}(KG)$. Für $h \in G$ gilt dann

$$\alpha = h\alpha h^{-1} = \sum_{g\in G} \alpha_g hgh^{-1}$$

und $\alpha_g = \alpha_{hgh^{-1}}$. Daher ist α konstant auf den Konjugationsklassen von G. Folglich ist α eine K-Linearkombination der Klassensummen. Da Konjugationsklassen disjunkt sind, sind die Klassensummen linear unabhängig. □

Bemerkung 12.10.

(i) Nach Satz 12.9 besteht $\mathrm{Z}(KG)$ genau aus den Klassenfunktionen $G \to K$.

(ii) Für $C, D \in \mathrm{Cl}(G)$ gilt

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

mit den in Bemerkung 2.15 definierten Klassenmultiplikationskonstanten.

(iii) Sei $\mathrm{char}\, K \nmid |G|$ und $KG \cong D_1^{n_1\times n_1} \times \ldots \times D_k^{n_k\times n_k}$ die Artin-Wedderburn-Zerlegung. Aus Lemma 8.12 folgt

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

Ist K algebraisch abgeschlossen, so erhält man $k(G) = k$ wie im Fall $K = \mathbb{C}$ (Satz 2.18). Im Folgenden bestimmen wir k, falls $\mathrm{char}\, K \mid |G|$.

Definition 12.11. Sei p eine Primzahl. Man nennt $x \in G$ ein *p-Element* bzw. *p'-Element*, falls $|\langle x\rangle|$ eine p-Potenz ist bzw. nicht durch p teilbar ist. Sei G_p bzw. $G_{p'}$ die Menge der p-Elemente bzw. p'-Elemente von G. Dann gilt $G_p \cap G_{p'} = \{1\}$, aber $G \neq G_p \cup G_{p'}$ im Allgemeinen. Man nennt $C \in \mathrm{Cl}(G)$ eine *p-Konjugationsklasse* bzw. *p'-Konjugationsklasse*, falls $C \subseteq G_p$ bzw. $C \subseteq G_{p'}$ (beachte: konjugierte Elemente haben die gleiche Ordnung).

Lemma 12.12. *Jedes Element $x \in G$ lässt sich eindeutig in der Form $x = x_px_{p'} = x_{p'}x_p$ mit $x_p \in G_p$ und $x_{p'} \in G_{p'}$ schreiben. Man nennt x_p den* p-Faktor *und $x_{p'}$ den* p'-Faktor *von x.*

Beweis. Sei $|\langle x\rangle| = p^am$ mit $p \nmid m$. Dann existieren $\alpha, \beta \in \mathbb{Z}$ mit $\alpha p^a + \beta m = \mathrm{ggT}(p^a, m) = 1$. Für $x_p := x^{\beta m} \in G_p$ und $x_{p'} := x^{\alpha p^a} \in G_{p'}$ gilt $x = x^{\alpha p^a+\beta m} = x_px_{p'} = x_{p'}x_p$.

Seien $y \in G_p$ und $z \in G_{p'}$ mit $x = yz = zy$. Dann sind y und z mit x, x_p und $x_{p'}$ vertauschbar. Es folgt $y^{-1}x_p = zx_{p'}^{-1} \in G_p \cap G_{p'} = \{1\}$, d. h. $y = x_p$ und $z = x_{p'}$. □

Bemerkung 12.13. Für $x, g \in G$ gilt $(gxg^{-1})_p = gx_pg^{-1}$ und $(gxg^{-1})_{p'} = gx_{p'}g^{-1}$.

Definition 12.14. Für $x \in G$ sei

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

die *p'-Sektion* von x. Nach Bemerkung 12.13 ist $\mathrm{Sec}_{p'}(x)$ eine Vereinigung von Konjugationsklassen von G.

Beispiel 12.15. Für $x \in G_p$ gilt $\mathrm{Sec}_{p'}(x) = G_p$. Für $g := (1,2) \in S_3$ gilt $\mathrm{Sec}_{3'}(g) = \mathrm{Cl}(g) = \{g, (1,3), (2,3)\}$.

Lemma 12.16. *Für jeden algebraisch abgeschlossenen Körper K der Charakteristik $p > 0$ gilt*

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

Beweis.

(i) Sei Γ die rechte Seite der Gleichung. Für $g, h \in G$ gilt $gh - hg = gh - g^{-1}(gh)g \in \Gamma$. Für $\alpha = \sum_{g\in G} \alpha_g g$ und $\beta = \sum_{h\in G} \beta_h h$ folgt

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

Sei umgekehrt $\sum_{g\in G} \alpha_g g \in \Gamma$ und $x_C \in C \in \mathrm{Cl}(G)$. Für jedes $c \in C$ existiert $g \in G$ mit $c = gx_Cg^{-1}$. Dann gilt $c - x_C = (gx_C)g^{-1} - g^{-1}(gx_C) \in \gamma(KG)$ und

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

(ii) Sei $|G| = p^a m$ mit $p \nmid m$ und $k \geq a$ mit $p^k \equiv 1 \pmod m$ (z. B. $k = a\varphi(m)$). Dann gilt $g^{p^k} = g_p^{p^k} g_{p'}^{p^k} = g_{p'}$ für $g \in G$ nach Lagrange. Sei $\alpha := \sum_{g\in G} \alpha_g g \in KG$ und $x_1, \ldots, x_l$ ein Repräsentantensystem für die p'-Konjugationsklassen von G. Für $g \in \mathrm{Sec}_{p'}(x_i)$ gilt $g_{p'} \equiv x_i \pmod{\gamma(KG)}$ nach (i). Aus Lemma 11.12 folgt

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

Gilt $\sum_{s\in \mathrm{Sec}_{p'}(x_i)} \alpha_s = 0$ für alle i, so ergibt sich $\alpha^{p^k} \in \gamma(KG)$ und $\alpha \in \gamma(KG) + \mathrm{J}(KG)$ nach Lemma 11.12. Ist umgekehrt $\alpha^{p^n} \in \gamma(KG)$ für ein $n \in \mathbb{N}$, so existiert ein $k \geq \max\{a, n\}$ mit $p^k \equiv 1 \pmod m$. Dann folgt $\sum_{s\in \mathrm{Sec}_{p'}(x_i)} \alpha_s = 0$ aus (12.1) für $i = 1, \ldots, l$. □

Satz 12.17 (Brauer)**.** *Sei K ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$. Dann stimmt die Anzahl der einfachen KG-Moduln mit der Anzahl der p'-Konjugationsklassen von G überein.*

Beweis. Offenbar stimmt die Anzahl l der p'-Konjugationsklassen mit der Anzahl der p'-Sektionen überein. Lemma 12.16 beschreibt $\gamma(KG) + \mathrm{J}(KG)$ als Lösung eines linearen Gleichungssystems mit l linear unabhängigen Zeilen. Daher gilt $\dim KG/(\gamma(KG) + \mathrm{J}(KG)) = l$ und die Behauptung folgt aus Folgerung 11.13. □

Beispiel 12.18. Der algebraische Abschluss $K := \overline{\mathbb{F}_p}$ von $\mathbb{F}_p$ hat Charakteristik $p > 0$.

(i) Sei G abelsch und $|G| = p^a m$ mit $p \nmid m$. Dann ist $G = G_p \times G_{p'}$ und $m = |G_{p'}|$ ist die Anzahl der einfachen KG-Moduln. Man erhält diese Moduln als Inflationen von $G_{p'} \cong G/G_p$. Das gilt allgemeiner, falls G_p die einzige p-Sylowgruppe von G ist (Beispiel 12.22).

(ii) Genau dann ist der triviale Modul der einzige einfache KG-Modul, wenn $\{1\}$ die einzige p'-Konjugationsklasse von G ist. Das gilt genau dann, wenn G eine p-Gruppe ist. Diese Aussage bleibt richtig, wenn K nicht algebraisch abgeschlossen ist (siehe Beweis von Satz 12.21).

(iii) Für $p \in \{2, 3\}$ besitzt KS_3 jeweils genau zwei einfache Moduln. Der nicht-triviale Modul für $p = 3$ ist der *alternierende* Modul K mit $\sigma \cdot 1_K = \mathrm{sgn}(\sigma)1_K$ für $\sigma \in S_3$ (Inflation von $C_2 \cong S_3/A_3$). Insbesondere sind hier beide einfache Moduln 1-dimensional, obwohl S_3 nicht abelsch ist (vgl. Satz 2.2). Für $p = 2$ ist

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

der nicht-triviale einfache Modul (mit $\dim V = 2$), wobei S_3 die Koordinaten permutiert.

Bemerkung 12.19.

(i) Die Bestimmung der einfachen Moduln ist in positiver Charakteristik deutlich schwieriger als in Charakteristik 0. Zum Beispiel kennt man nicht einmal die Dimensionen der einfachen $\overline{\mathbb{F}_2}S_{20}$-Moduln. Diese Dimensionen teilen im Allgemeinen auch nicht die Gruppenordnung. Zum Beispiel gibt es einfache $\overline{\mathbb{F}_3}S_7$-Moduln der Dimension 13.

(ii) In der Situation von Satz 12.17 kann man jedem KG-Modul einen sogenannten *Brauer-Charakter* $\varphi\colon G_{p'} \to \mathbb{C}$ zuordnen. Die Menge der irreduziblen Brauer-Charaktere bildet dann eine Basis für den Raum aller Klassenfunktionen auf $G_{p'}$.

(iii) Die Anzahl der einfachen $\mathbb{Q}G$-Moduln ist die Anzahl der Konjugationsklassen von zyklischen Untergruppen von G (ohne Beweis).

(iv) Sei r die Anzahl der Konjugationsklassen der Form $C = C^{-1}$ und $2s$ die Anzahl der Konjugationsklassen $C \neq C^{-1}$ von G. Dann ist $r + s$ die Anzahl der einfachen $\mathbb{R}G$-Moduln (ohne Beweis). Ist $|G|$ ungerade, so ist $r = 1$ und es gibt genau $(k(G) + 1)/2$ einfache $\mathbb{R}G$-Moduln.

(v) Nach Folgerung 9.12 besitzt KG für jeden Körper K nur endlich viele einfache Moduln bis auf Isomorphie. Wir werden sehen, dass die Situation für unzerlegbare Moduln anders ist.

Lemma 12.20. *Sei G eine nicht-zyklische p-Gruppe. Dann existiert $N \trianglelefteq G$ mit $G/N \cong C_p \times C_p$.*

Beweis. Induktion nach $|G|$. Da G nicht zyklisch ist, gilt $|G| \geq p^2$. Im Fall $|G| = p^2$ ist G abelsch nach Beispiel 4.8 und die Behauptung gilt mit $N := 1$. Sei $|G| > p^2$ und $Z := \mathrm{Z}(G) \neq 1$ (Algebra 1). Ist G/Z nicht zyklisch, so existiert nach Induktion ein Normalteiler $N/Z \trianglelefteq G/Z$ mit

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

Sei nun G/Z zyklisch, sagen wir $G/Z = \langle gZ \rangle$. Dann hat jedes Element von G die Form $g^i z$ mit $i \in \mathbb{Z}$ und $z \in Z$. Dies impliziert, dass G abelsch ist. Sei $x \in G$ mit Ordnung p. Nach Induktion können wir annehmen, dass $G/\langle x \rangle$ zyklisch ist, sagen wir $G = \langle x, y \rangle$. Für $N := \langle y^p \rangle \trianglelefteq G$ gilt nun $G/N \cong C_p \times C_p$. □

Satz 12.21. *Für jeden Körper K der Charakteristik $p > 0$ gilt:*

(i) Genau dann ist KG lokal, wenn G eine p-Gruppe ist.

(ii) Ist $G \cong C_{p^n}$, so besitzt KG genau p^n unzerlegbare Moduln bis auf Isomorphie. Diese haben die Dimensionen $1, 2, \ldots, p^n$.

(iii) Ist G eine nicht-zyklische p-Gruppe, so besitzt KG unzerlegbare Moduln in jeder Dimension $d \in \mathbb{N}$.

Beweis.

(i) Nehmen wir zuerst an, dass G keine p-Gruppe ist. Nach Cauchy (oder Sylow) existiert eine Untergruppe $1 \neq H \leq G$ mit $|H| \not\equiv 0 \pmod{p}$, d. h. $|H|^{-1} \in K$. Man sieht leicht, dass $\frac{1}{|H|} \sum_{x \in H} x \in KG \setminus \{0, 1\}$ ein Idempotent ist. Nach Satz 11.4 ist KG nicht lokal.

Sei nun G eine p-Gruppe. Bekanntlich enthält K den Primkörper $\mathbb{F}_p$. Sei M ein einfacher KG-Modul und

$$L := \sum_{g \in G} \mathbb{F}_p gm \subseteq M$$

für ein festes $m \in M \setminus \{0\}$. Offenbar ist L ein endlicher $\mathbb{F}_p$-Vektorraum. Insbesondere ist $|L|$ eine p-Potenz. Für $x \in G$ gilt $xL = \sum_{g\in G} \mathbb{F}_p xgm = L$. Daher operiert G auf L durch Linksmultiplikation. Sicher ist $0 \in L$ ein Fixpunkt von G. Da sowohl $|G|$ als auch $|L|$ Potenzen von p sind, muss G nach der Bahnengleichung einen weiteren Fixpunkt $a \in L \setminus \{0\}$ haben. Nun ist Ka ein Untermodul des einfachen Moduls M und es folgt $M = Ka \simeq K$. Nach Satz 9.15 ist $KG/\mathrm{J}(KG) = KG/\mathrm{Ann}(M) \cong \mathrm{End}_K(M) \cong K$. Daher ist KG lokal.

(ii) Sei $G = \langle g \rangle$ und V ein unzerlegbarer KG-Modul. Das Minimalpolynom μ der linearen Abbildung $f\colon V \to V$, $v \mapsto gv$ teilt $X^{p^n} - 1 = (X-1)^{p^n}$. Also gilt $\mu = (X-1)^k$ für ein $1 \le k \le p^n$. Nach linearer Algebra existiert eine f-invariante Zerlegung $V = U \oplus W$, sodass $f_{|U}$ dem Jordanblock $J_k(1)$ entspricht.[13] Da V unzerlegbar ist, gilt $W = 0$ und $\dim V = \dim U = k$. Außerdem ist V bis auf Isomorphie eindeutig bestimmt. Umgekehrt kann man zu jedem $1 \le k \le p^n$ den Vektorraum $V := K^k$ durch $gv := J_k(1)v$ für $v \in V$ in einen KG-Modul umwandeln. Wegen der Eindeutigkeit der Jordanschen Normalform ist V unzerlegbar.

(iii) Nach Lemma 12.20 existiert $N \trianglelefteq G$ mit $G/N \cong C_p \times C_p$. Ist U ein unzerlegbarer $K[G/N]$-Modul, so wird U durch $gu := (gN)u$ für $g \in G$ und $u \in U$ zu einem unzerlegbaren KG-Modul (Inflation). Wir können daher $G = \langle g, h \rangle \cong C_p \times C_p$ annehmen.

Wir konstruieren zunächst unzerlegbare Moduln in Dimension $2d$. Sei V_{2d} der K-Vektorraum mit Basis $b_1, \ldots, b_d, c_1, \ldots, c_d$. Seien $\alpha, \beta \in \mathrm{End}_K(V_{2d})$ mit

$$\alpha(b_i) = c_i, \quad \beta(b_j) = c_{j+1}, \quad \alpha(c_i) = \beta(c_i) = \beta(b_d) = 0 \quad (i = 1, \ldots, d,\ j = 1, \ldots, d-1).$$

Offenbar gilt $\alpha^2 = \beta^2 = \alpha\beta = \beta\alpha = 0$. Es folgt $(\mathrm{id} + \alpha)^p = \mathrm{id} + \alpha^p = \mathrm{id} = (\mathrm{id} + \beta)^p$. Daher definiert $\Delta\colon G \to \mathrm{GL}(V_{2d})$ mit $\Delta(g) = \mathrm{id} + \alpha$ und $\Delta(h) = \mathrm{id} + \beta$ eine Darstellung. Sei $f \in \mathrm{End}_{KG}(V_{2d})$ mit Matrix $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in K^{2d\times 2d}$ bzgl. der angegebenen Basis. Sei $J = J_d(0) \in K^{d\times d}$ der Jordanblock zum Eigenwert 0 mit Einsen unterhalb der Hauptdiagonalen. Wegen $f(gv) = gf(v)$ für $v \in V_{2d}$ ist f mit α und β vertauschbar, d. h.

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

Es folgt $A = D$, $B = 0$ und $AJ = JA$. Insbesondere ist M eine untere Dreiecksmatrix. Mit $A = (a_{ij})$ gilt konkret

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

Es folgt $a_{11} = \ldots = a_{dd}$. Im Fall $a_{11} \neq 0$ ist f invertierbar und anderenfalls ist f nilpotent. Also ist $\mathrm{End}_{KG}(V_{2d})$ lokal (Satz 11.4) und V_{2d} unzerlegbar (Satz 11.6).

Für ungerade Dimension $2d+1$ erweitern wir V_{2d} zu $V_{2d+1} := V_{2d} \oplus Kc_{d+1}$ und setzen

$$\alpha(b_i) = c_i, \qquad \beta(b_i) = c_{i+1}, \qquad \alpha(c_j) = \beta(c_j) = 0 \qquad (i = 1, \ldots, d,\ j = 1, \ldots, d+1)$$

[13] siehe Vorlesungsskript Lineare Algebra.

(da der triviale Modul unzerlegbar ist, können wir $d \geq 1$ annehmen). Eine ähnliche Rechnung zeigt $M = \left(\begin{smallmatrix} A & 0 \\ C & D \end{smallmatrix}\right)$ mit $A \in K^{d\times d}$, $C \in K^{(d+1)\times d}$ und

$$D = \begin{pmatrix} A & * \\ 0 & * \end{pmatrix} = \begin{pmatrix} * & 0 \\ * & A \end{pmatrix} = \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ * & & a_{11} \end{pmatrix} \in K^{(d+1)\times(d+1)}.$$

Also ist auch V_{2d+1} unzerlegbar. □

Beispiel 12.22. Sei K algebraisch abgeschlossen mit $\operatorname{char} K = p$. Sei $P := G_p \trianglelefteq G$ die einzige p-Sylowgruppe von G. Durch Inflation von G/P erhält man $k(G/P)$ nicht-isomorphe einfache KG-Moduln (Bemerkung 12.10). Sei umgekehrt V ein beliebiger einfacher KG-Modul. Durch Einschränkung ist V auch ein KP-Modul. Nach Satz 12.21 besitzt V einen trivialen KP-Untermodul (zum Beispiel das vorletzte Glied einer Kompositionsreihe). Insbesondere ist $W := \{v \in V : \forall x \in P : xv = v\} \neq 0$. Für $g \in G$, $x \in P$ und $w \in W$ gilt

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

Dies zeigt $gw \in W$ und $W \leq V$. Da V einfach ist, folgt $W = V$, d. h. P operiert trivial auf V. Die Deflation von V ist daher ein einfacher $K[G/P]$-Modul. Folglich entsprechen sich die einfachen KG-Moduln und die einfachen $K[G/P]$-Moduln durch Inflation und Deflation. Insbesondere ist $k(G/P)$ die Anzahl der p'-Konjugationsklassen von G.

Bemerkung 12.23. Higman hat gezeigt, dass die Anzahl der unzerlegbaren KG-Moduln für eine beliebige endliche Gruppe G genau dann endlich ist, wenn G zyklische p-Sylowgruppen besitzt ($p = \operatorname{char} K$). Ggf. sagt man: KG hat *endlichen Darstellungstyp*.

13 Ganzzahlige Darstellungen

Bemerkung 13.1. Nachdem wir Darstellungen über $\mathbb{C}$, über Zahlkörpern und über Körpern positiver Charakteristik studiert haben, verzichten wir in diesem Kapitel gänzlich auf die Körperaxiome. Im einfachsten Fall spielt $\mathbb{Z}$ die Rolle des Körpers. Wie im letzten Kapitel definiert man den Gruppen*ring* $\mathbb{Z}G$. Ein $\mathbb{Z}G$-Modul besitzt in der Regel aber keine Basis. Zum Beispiel ist jede endliche abelsche Gruppe A ein trivialer $\mathbb{Z}G$-Modul und jedes Element $a \in A$ ist linear abhängig wegen $|A|a = 0$. Wir untersuchen daher eine Familie von $\mathbb{Z}G$-Moduln, die per definitionem eine Basis besitzen.

Definition 13.2.

- Ein Homomorphismus der Form $G \to \mathrm{GL}(n, \mathbb{Z})$ heißt *ganzzahlige* Darstellung.
- Eine freie abelsche Gruppe $\mathfrak{A}$ heißt *G-Gitter*, falls eine Operation $G \times \mathfrak{A} \to \mathfrak{A}$ mit ${}^g(x+y) = {}^gx + {}^gy$ existiert. Wie bei Moduln schreiben wir gx anstelle von ${}^gx$. Eine G-invariante Untergruppe $\mathfrak{B} \leq \mathfrak{A}$ heißt *Untergitter*, falls $\mathfrak{A}/\mathfrak{B}$ torsionsfrei ist. Besitzt $\mathfrak{A}$ keine echten, nicht-trivialen Untergitter, so nennt man $\mathfrak{A}$ *einfach*.

Bemerkung 13.3.

(i) Wir nehmen stets an, dass G-Gitter endlichen Rang haben.

(ii) Ist $\Delta\colon G \to \mathrm{GL}(n,\mathbb{Z})$ eine ganzzahlige Darstellung, so wird $\mathfrak{A} := \mathbb{Z}^n$ durch $ga = \Delta(g)a$ für $a \in \mathfrak{A}$ und $g \in G$ wie üblich zu einem G-Gitter. Umgekehrt beschreibt die Operation von G auf einem Gitter $\mathfrak{A}$ eine ganzzahlige Darstellung Δ. Ein Basiswechsel von $\mathfrak{A}$ ersetzt Δ durch $g \mapsto S\Delta(g)S^{-1}$ für ein $S \in \mathrm{GL}(n,\mathbb{Z})$. Die bekannten Diagonalisierungsargumente für Matrizen über Körpern stehen hier also nicht zur Verfügung.

(iii) Ist $\mathfrak{B}$ ein Untergitter von $\mathfrak{A}$, so ist offenbar auch $\mathfrak{A}/\mathfrak{B}$ ein G-Gitter.

(iv) Sei $b_1, \ldots, b_n$ eine Basis eines G-Gitters $\mathfrak{A}$. Dann lässt sich jedes Element $a \in \mathfrak{A}$ eindeutig in der Form $a = z_1b_1 + \ldots + z_nb_n$ mit $z_1, \ldots, z_n \in \mathbb{Z}$ schreiben. Man kann $\mathfrak{A}$ zu einem $\mathbb{Q}$-Vektorraum V erweitern, indem man $z_1, \ldots, z_n \in \mathbb{Q}$ zulässt. Die Operation von G setzt sich nach V fort, sodass man einen $\mathbb{Q}G$-Modul erhält. Diese Konstruktion nennt man das *Tensorprodukt* von $\mathbb{Q}$ und $\mathfrak{A}$, geschrieben $V = \mathbb{Q} \otimes_{\mathbb{Z}} \mathfrak{A} = \mathbb{Q} \otimes \mathfrak{A}$. Offenbar ist $\operatorname{rk}\mathfrak{A} = \dim V$.

(v) Sei umgekehrt ein $\mathbb{Q}G$-Modul V gegeben. Nach Minkowski existiert eine Basis $b_1, \ldots, b_n$ von V bzgl. der G durch ganzzahlige Matrizen operiert. Daher ist $\mathfrak{A} := \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n$ ein G-Gitter mit $\mathbb{Q} \otimes \mathfrak{A} = V$.

(vi) Man beachte, dass einfache G-Gitter $\mathfrak{A}$ durchaus echte G-invariante Untergruppen wie zum Beispiel $2\mathfrak{A} = \{2a : a \in \mathfrak{A}\}$ besitzen.

Lemma 13.4. *Sei $\mathfrak{A}$ ein G-Gitter und $V := \mathbb{Q} \otimes \mathfrak{A}$. Dann sind die Abbildungen $\mathfrak{B} \to \mathbb{Q} \otimes \mathfrak{B}$ und $U \mapsto U \cap \mathfrak{A}$ zueinander inverse Bijektionen zwischen der Menge der Untergitter von $\mathfrak{A}$ und der Menge der Untermoduln von V. Insbesondere ist $\mathfrak{A}$ genau dann einfach, wenn V einfach ist.*

Beweis. Ist $\mathfrak{B}$ ein Untergitter von $\mathfrak{A}$, so ist $\mathbb{Q} \otimes \mathfrak{B} \leq V$. Sei umgekehrt $U \leq V$. Dann ist $\mathfrak{B} := \mathfrak{A} \cap U$ eine G-invariante Untergruppe von $\mathfrak{A}$. Sei $a \in \mathfrak{A} \setminus \mathfrak{B}$. Angenommen es existiert ein $m \in \mathbb{N}$ mit $ma \in \mathfrak{B}$. Dann wäre $a = \frac{1}{m}ma \in \mathfrak{A} \cap U = \mathfrak{B}$. Also ist $\mathfrak{A}/\mathfrak{B}$ torsionsfrei. Dies zeigt, dass $\mathfrak{B}$ ein Untergitter von $\mathfrak{A}$ ist.

Für ein Untergitter $\mathfrak{B}$ ist offenbar $\mathfrak{B} \subseteq \mathfrak{A} \cap (\mathbb{Q} \otimes \mathfrak{B})$. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen kann man eine Basis $b_1, \ldots, b_k$ von $\mathfrak{B}$ zu einer Basis von $\mathfrak{A}$ ergänzen. Die Elemente in $\mathfrak{A} \cap (\mathbb{Q} \otimes \mathfrak{B})$ bzgl. dieser Basis sind genau die ganzzahligen Linearkombinationen von $b_1, \ldots, b_k$. Also ist $\mathfrak{B} \subseteq \mathfrak{A} \cap (\mathbb{Q} \otimes \mathfrak{B})$.

Für $U \leq V$ ist $W := \mathbb{Q} \otimes (\mathfrak{A} \cap U) \leq U$. Sei $b_1, \ldots, b_k$ eine $\mathbb{Q}$-Basis von U. Dann existiert ein $m \in \mathbb{N}$ mit $mb_i \in \mathfrak{A}$ für $i = 1, \ldots, k$. Dies zeigt $\dim W = \dim U$ und $W = U$. Daher sind die angegebenen Abbildungen zueinander invers. Sie müssen folglich Bijektionen sein. □

Bemerkung 13.5. Sei $\mathfrak{A}$ ein G-Gitter mit Untergitter $\mathfrak{B}$. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen kann man eine Basis von $\mathfrak{B}$ zu einer Basis von $\mathfrak{A}$ ergänzen. Die Operation von G auf $\mathfrak{A}$ bzgl. dieser Basis wird durch ganzzahlige Blockmatrizen der Form $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)$ beschrieben. Dabei beschreibt A die Operation auf $\mathfrak{B}$ und C die Operation auf $\mathfrak{A}/\mathfrak{B}$. Nach Maschke besitzt U ein Komplement W in V. Nun ist $\mathfrak{C} := \mathfrak{A} \cap W$ ein Untergitter von $\mathfrak{A}$, aber im Allgemeinen gilt $\mathfrak{B} + \mathfrak{C} < \mathfrak{A}$. In der Regel besitzt $\mathfrak{B}$ kein Komplement in $\mathfrak{A}$.

Beispiel 13.6. Die Gruppe $G := \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right) \rangle \cong C_2$ operiert auf dem Gitter $\mathfrak{A} := \mathbb{Z}^2$ durch Matrix-Vektor-Multiplikation. Offenbar sind $\mathfrak{B} := \mathbb{Z}(1,0)^{\mathrm{t}}$ und $\mathfrak{C} := \mathbb{Z}(1,-2)^{\mathrm{t}}$ Untergitter mit $\mathfrak{B} + \mathfrak{C} < \mathfrak{A}$. Man sieht leicht, dass $\mathfrak{B}$ in $\mathfrak{A}$ kein Komplement besitzt, d. h. $\mathfrak{A}$ ist nicht halbeinfach bzw. $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$ ist nicht in $\mathrm{GL}(2,\mathbb{Z})$ diagonalisierbar (aber in $\mathrm{GL}(2,\mathbb{Q})$).

Definition 13.7. Seien $\mathfrak{A}$ und $\mathfrak{B}$ G-Gitter. Eine Abbildung $f\colon \mathfrak{A} \to \mathfrak{B}$ heißt *Homomorphismus*, falls $f(gx+y) = gf(x) + f(y)$ für alle $g \in G$ und $x, y \in \mathfrak{A}$ gilt. Wie üblich definiert man Mono-, Epi- und Isomorphismen. Existiert ein Isomorphismus, so nennt man $\mathfrak{A}$ und $\mathfrak{B}$ *isomorph* und schreibt $\mathfrak{A} \cong \mathfrak{B}$.

Lemma 13.8. *Seien $\mathfrak{A}$ und $\mathfrak{B}$ G-Gitter. Dann existieren bis auf Isomorphie nur endlich viele Gitter $\mathfrak{C}$ mit Untergitter $\mathfrak{A}$ und $\mathfrak{C}/\mathfrak{A} \cong \mathfrak{B}$.*

Beweis. Wie in Bemerkung 13.5 wählen wir eine Basis von $\mathfrak{C}$ bzgl. der die entsprechende Darstellung $\Delta\colon G \to \mathrm{GL}(n,\mathbb{Z})$ die Form $\Delta(g) = \left(\begin{smallmatrix} A_g & B_g \\ 0 & C_g \end{smallmatrix}\right)$ für $g \in G$ hat. Die Matrizen $A_g \in \mathrm{GL}(k,\mathbb{Z})$ und $C_g \in \mathrm{GL}(l,\mathbb{Z})$ sind bis auf ganzzahlige Ähnlichkeit durch $\mathfrak{A}$ und $\mathfrak{B}$ vorgegeben. Es genügt zu zeigen, dass es bis auf Ähnlichkeit nur endlich viele Möglichkeiten für B_g gibt. Für $g, h \in G$ gilt

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

d. h. $A_gB_h = B_{gh} - B_gC_h$. Wie im Beweis von Maschke benutzen wir ein Mittelwertargument: Für

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

gilt

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

Es folgt $B_g = MC_g - A_gM$. Es genügt also die Möglichkeiten für M zu beschränken. Sei $E \in \mathbb{Z}^{k\times l}$ beliebig und $S = \left(\begin{smallmatrix} 1_k & E \\ 0 & 1_l \end{smallmatrix}\right)$. Wir können $\Delta(g)$ durch

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

ersetzen. Anschließend gilt $B_g = (M+E)C_g - A_g(M+E)$. Durch geeignete Wahl von E kann man auf diese Weise erreichen, dass alle Einträge von M zwischen 0 und 1 liegen. Da diese Einträge andererseits in $\frac{1}{|G|}\mathbb{Z}$ liegen, gibt es nur endlich viele Möglichkeiten für M. □

Beispiel 13.9. Nach Beispiel 13.6 sind $\mathbb{Z}^2$ und $\mathbb{Z}(1,0)^{\mathrm{t}} + \mathbb{Z}(1,-2)^{\mathrm{t}}$ zwei nicht-isomorphe G-Gitter mit den gleichen einfachen Bestandteilen.

Satz 13.10 (Minkowskis Linearformensatz)**.** *Sei $A \in \mathbb{Z}^{n\times n}$ und $d_1, \dots, d_n \in \mathbb{R}_+$ mit $d_1 \dots d_n \geq |\det(A)|$. Dann existiert ein $x \in \mathbb{Z}^n \setminus \{0\}$ mit $|(Ax)_i| < d_i$ für $i = 1, \dots, n$.*

Beweis (Rado). Nach der Hermite-Normalform[14] existiert ein $S \in \mathrm{GL}(n,\mathbb{Z})$, sodass AS eine untere Dreiecksmatrix ist. Erfüllt x die Behauptung für AS anstelle von A, so ist $S^{-1}x$ eine Lösung für A. Wir können daher annehmen, dass A selbst eine untere Dreiecksmatrix ist. Dann ist $d_1 \dots d_n \geq |\det(A)| = |a_{11} \dots a_{nn}|$. Für ganze Zahlen $0 \leq \alpha_i < |a_{ii}|$ und $0 \leq \delta_i \leq d_i$ betrachten wir das Gleichungssystem

[14] Siehe Skript zur linearen Algebra.

$Ax = \alpha + \delta$. Wir zeigen durch Induktion nach n, dass bei gegebenem $\delta \in \mathbb{Z}^n$ genau ein $\alpha \in \mathbb{Z}^n$ existiert, sodass das System eine ganzzahlige Lösung x besitzt. Im Fall $n = 1$ sind α_1 und x_1 durch

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

eindeutig bestimmt. Sei $n \geq 2$ und $B := A_{nn}$. Induktiv existieren eindeutige $\alpha_1, \ldots, \alpha_{n-1}$, sodass $x_1, \ldots, x_{n-1}$ eine ganzzahlige Lösung von $Bx = \alpha + \delta$ ist. Nun sind α_n und x_n durch

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

eindeutig bestimmt (wegen $a_{in} = 0$ für $i < n$ kommt x_n nur in dieser Gleichung vor).

Offenbar gibt es $(\lfloor d_1 \rfloor + 1) \ldots (\lfloor d_n \rfloor + 1) > d_1 \ldots d_n$ mögliche Vektoren δ, aber nur $|a_{11} \ldots a_{nn}| \leq d_1 \ldots d_n$ mögliche α. Zu mindestens einem α müssen also $\delta \neq \delta'$ existieren, sodass $Ay = \alpha + \delta$ und $Az = \alpha + \delta'$ ganzzahlige Lösungen $y \neq z$ haben. Jetzt erfüllt $x := y - z \neq 0$ die Behauptung, denn $|(Ax)_i| = |\delta_i - \delta_i'| \leq d_i$. □

Bemerkung 13.11. Der Linearformensatz lässt sich leicht auf reelle Matrizen A übertragen.[15] Diese Verallgemeinerung benötigen wir aber nicht.

Satz 13.12 (Jordan-Zassenhaus)**.** *Für jedes $n \in \mathbb{N}$ existieren bis auf Isomorphie nur endlich viele G-Gitter vom Rang n.*

Beweis (Gaschütz). Nach Lemma 13.8 genügt es zu zeigen, dass bis auf Isomorphie nur endlich viele *einfache* G-Gitter vom Rang n existieren. Da es bis auf Isomorphie nur endlich viele (einfache) $\mathbb{Q}G$-Moduln der Dimension n gibt, können wir einen solchen Modul $V = \mathbb{Q}^n$ festhalten und G-Gitter $\mathfrak{A} \subseteq V$ untersuchen. Nach Bemerkung 13.3 existiert eine Basis $a_1, \ldots, a_n$ von V, sodass die entsprechende Darstellung $\Delta\colon G \to \mathrm{GL}(V)$ durch ganzzahlige Matrizen realisiert wird. Sei $\mathfrak{A} = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n$ das dazugehörige Gitter. Wir bestimmen eine nur von Δ abhängige Konstante $c \in \mathbb{N}$, sodass jedes in V enthaltene G-Gitter vom Rang n zu einem Gitter $\mathfrak{C} \supseteq \mathfrak{A}$ mit $|\mathfrak{C} : \mathfrak{A}| \leq c$ isomorph ist. Wegen $\mathfrak{A} \subseteq \mathfrak{C} \subseteq \frac{1}{c}\mathfrak{A}$ und $\frac{1}{c}\mathfrak{A}/\mathfrak{A} \cong (\mathbb{Z}/c\mathbb{Z})^n$ gibt es nur endlich viele Möglichkeiten für $\mathfrak{C}$.

Sei $\mathfrak{B} \subseteq V$ ein G-Gitter vom Rang n. Indem man $\mathfrak{B}$ durch $d\mathfrak{B} \cong \mathfrak{B}$ für ein geeignetes d ersetzt, kann man $\mathfrak{B} \subseteq \mathfrak{A}$ annehmen. Da $\mathfrak{A}$ und $\mathfrak{B}$ freie abelsche Gruppen vom gleichen Rang sind, gilt $D := |\mathfrak{A} : \mathfrak{B}| < \infty$. Eine Basis $b_1, \ldots, b_n$ von $\mathfrak{B}$ lässt sich in der Form $b_i := \sum_{j=1}^n \beta_{ji} a_j$ mit $B = (\beta_{ij}) \in \mathbb{Z}^{n \times n}$ schreiben. Bekanntlich (Algebra) gilt $|\det(B)| = D$. Nach dem Linearformensatz existiert ein $x \in \mathbb{Z}^n \setminus \{0\}$ mit $|(Bx)_i| \leq \sqrt[n]{D}$ für $i = 1, \ldots, n$. Für $s := Bx \in \mathbb{Z}^n$ gilt

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

O. B. d. A. sei $s_1 \neq 0$. Sei $\varphi \in \mathrm{End}(V)$ mit $\varphi(a_1) = t$ und $\varphi(a_i) = 0$ für $i = 2, \ldots, n$. Dann ist

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

ein Endomorphismus von $\mathbb{Q}G$-Moduln mit $\psi(\mathfrak{A}) \subseteq \mathfrak{B}$. Wegen $\mathrm{tr}(\psi) = \sum_{g \in G} \mathrm{tr}(\varphi) = |G| s_1 \neq 0$ ist $\psi \neq 0$. Nach Schurs Lemma ist ψ ein Automorphismus. Sei $M \in \mathrm{GL}(n, \mathbb{Q})$ die Matrix von ψ bezüglich $a_1, \ldots, a_n$. Dann gilt $|\mathfrak{A} : \psi(\mathfrak{A})| = |\det(M)|$. Jeder Eintrag von M ist eine Linearkombination von $s_1, \ldots, s_n$ mit Koeffizienten, die nur von Δ abhängen. Nach der Leibniz-Formel für Determinanten ist

[15] Siehe Skript zur linearen Algebra.

$\det(M)$ eine Linearkombination von Termen der Form $s_{i_1} \dots s_{i_n}$ mit $1 \leq i_1, \dots, i_n \leq n$ und Koeffizienten, die nur von Δ abhängen. Nach Wahl von s gilt $|s_{i_1} \dots s_{i_n}| \leq D$. Die Dreiecksungleichung zeigt $|\mathfrak{A} : \psi(\mathfrak{A})| = |\det(M)| \leq cD = c|\mathfrak{A} : \mathfrak{B}|$ für eine Konstante c. Für $\mathfrak{C} := \psi^{-1}(\mathfrak{B}) \cong \mathfrak{B}$ gilt jetzt $\mathfrak{A} = \psi^{-1}(\psi(\mathfrak{A})) \subseteq \psi^{-1}(\mathfrak{B}) = \mathfrak{C}$ und

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

wie behauptet. □

Beispiel 13.13.

(i) Sei $G := \langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle \cong S_3$ mit der natürlichen Darstellung auf $V := \mathbb{Q}^2$. Offenbar sind $\mathfrak{A} := \mathbb{Z}^2$ und $\mathfrak{B} := \mathbb{Z}(1,-1)^{\mathrm{t}} + \mathbb{Z}(2,1)^{\mathrm{t}}$ einfache G-Gitter in V. Angenommen es existiert ein Isomorphismus $\varphi\colon \mathfrak{A} \to \mathfrak{B}$. Da V absolut irreduzibel ist, gilt $\varphi = k\,\mathrm{id}$ für ein $k \in \mathbb{Z}$ nach Satz 12.7. Dann wäre aber

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

Also gilt $\mathfrak{A} \ncong \mathfrak{B}$. In Aufgabe 42 wird gezeigt, dass es keine weiteren nicht-isomorphen G-Gitter in V gibt. Da V der einzige einfache $\mathbb{Q}G$-Modul der Dimension 2 ist, gibt es generell keine weiteren einfachen G-Gitter vom Rang 2.

(ii) Sei $\zeta := e^{2\pi \mathrm{i}/n} \in \mathbb{C}$. Dann operiert $G = \langle \zeta \rangle \cong C_n$ durch Multiplikation auf $K := \mathbb{Q}(\zeta) = \mathbb{Q}_n \cong \mathbb{Q}^{\varphi(n)}$. Die G-Gitter in K sind die sogenannten *gebrochenen* Ideale. Sei $\varphi\colon \mathfrak{A} \to \mathfrak{B}$ ein Isomorphismus zwischen solchen Gittern. Dann gilt $\varphi(\zeta x) = \zeta\varphi(x)$ für $x \in \mathfrak{A}$. Da K von ζ erzeugt wird, gilt sogar $\varphi(\lambda x) = \lambda\varphi(x)$ für alle $\lambda \in K$. Sei $a \in \mathfrak{A} \setminus \{0\}$ und $c := \varphi(a)/a \in K$. Für alle $x \in \mathfrak{A}$ gilt

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

d. h. $\varphi(x) = cx$ und $\mathfrak{B} = c\mathfrak{A}$. Umgekehrt ist $\mathfrak{A}$ zu allen Vielfachen isomorph. Insbesondere ist $\mathfrak{A}$ zu einem Ideal des Ganzheitsrings

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

isomorph. Die Anzahl der Isomorphieklassen von Gittern nennt man die *Klassenzahl* $h(K)$ von K. Genau dann ist $h(K) = 1$, wenn $\mathbb{Z}[\zeta]$ ein Hauptidealring ist. Dies ist äquivalent zu

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

(nur 30 verschiedene Körper wegen $\mathbb{Q}_{2q} = \mathbb{Q}_q$ für ungerades q). Andererseits ist $h(\mathbb{Q}_{23}) = 3$ (ohne Beweis).

(iii) Für beliebige $\mathbb{Z}G$-Moduln ist der Satz von Jordan-Zassenhaus falsch, da es mit $\mathbb{Z}/k\mathbb{Z}$ für $k \in \mathbb{N}$ bereits unendlich viele (triviale) $\mathbb{Z}G$-Moduln vom Rang 1 gibt.

Bemerkung 13.14.

(i) Der Satz von Jordan-Zassenhaus gilt allgemeiner für den Ganzheitsring $\mathbb{Z}_K$ eines Zahlkörpers K, anstelle von $\mathbb{Z}$. Tatsächlich kann man KG durch eine halbeinfache K-Algebra ersetzen.

(ii) Der nächste Satz verbessert Folgerung 7.7.

Folgerung 13.15. *Für jedes n besitzen* $\mathrm{GL}(n, \mathbb{Q})$ *und* $\mathrm{GL}(n, \mathbb{Z})$ *nur endlich viele Konjugationsklassen von endlichen Gruppen.*

Beweis. Nach Satz 7.6 genügt es die Aussage für $\mathrm{GL}(n,\mathbb{Z})$ zu beweisen. Nach Folgerung 7.7 können wir die Isomorphieklasse einer endlichen Gruppe $G \leq \mathrm{GL}(n,\mathbb{Z})$ festhalten. Nach Jordan-Zassenhaus existieren nur endlich viele nicht-isomorphe G-Gitter $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$. Sei $\Delta_i \colon G \to \mathrm{GL}(n,\mathbb{Z})$ eine Darstellung zu $\mathfrak{A}_i$ und $G_i := \Delta(G)$ für $i = 1, \ldots, k$. Sei $\varphi \colon G \to H \leq \mathrm{GL}(n,\mathbb{Z})$ ein beliebiger Isomorphismus. Dann wird $\mathfrak{B} := \mathbb{Z}^n$ durch $gz := \varphi(g)z$ für $z \in \mathfrak{B}$ zu einem G-Gitter. O. B. d. A. existiert ein Isomorphismus $\gamma \colon \mathfrak{A}_1 \to \mathfrak{B}$. Bzgl. einer geeigneten Basis lässt sich γ durch eine Matrix $A \in \mathrm{GL}(n,\mathbb{Z})$ realisieren. Dabei gilt

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

für alle $x \in \mathfrak{A}$. Es folgt $A^{-1}gA = \varphi(g)$ und $A^{-1}GA = H$. □

Beispiel 13.16. Wir bestimmen die Konjugationsklassen von Untergruppen der Ordnung 2 in $\mathrm{GL}(2,\mathbb{Z})$. Sei $A \in \mathrm{GL}(2,\mathbb{Z})$ der Ordnung 2. Da es keinen einfachen $\mathbb{Q}G$-Modul der Dimension 2 gibt, besitzt jedes G-Gitter vom Rang 2 nach Lemma 13.4 ein Untergitter vom Rang 1. Wir können also $A = \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ annehmen. Aus $A^2 = 1_2$ folgt $a, c \in \{\pm 1\}$ und $(a+c)b = 0$. Im Fall $a = c$ muss $b = 0$ sein. Dann erhält man $A = -1_2$ in seiner eigenen Konjugationsklasse $\{A\}$. Sei nun $ac = -1$. Für $b = 0$ entstehen zwei Matrizen, die durch Konjugation mit $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ ineinander übergehen. Sei also $b \neq 0$. Wegen

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

kann man $a = 1 = -c$ annehmen. Wegen

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

für $s \in \mathbb{Z}$ kann man $b = 1$ annehmen. Insgesamt erhält man drei Matrizen -1_2, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$, die nach Beispiel 13.6 nicht konjugiert sind.

Bemerkung 13.17. Für unendliche Gruppen G gilt Folgerung 13.15 nicht (Aufgabe 43). Jedoch gilt folgende Variante: Ist $A \in \mathrm{GL}(n,\mathbb{Z})$ in $\mathrm{GL}(n,\mathbb{C})$ diagonalisierbar, so zerfällt die $\mathrm{GL}(n,\mathbb{Q})$-Konjugationsklasse von A in endlich viele Konjugationsklassen in $\mathrm{GL}(n,\mathbb{Z})$. Dies liegt daran, dass $\mathbb{Q}(A) := \{\gamma(A) : \gamma \in \mathbb{Q}[X]\} \subseteq \mathbb{Q}^{n\times n}$ eine halbeinfache Algebra ist (siehe Bemerkung 13.14).

Aufgaben

Aufgabe 1 (2+2+3 Punkte)**.** Sei G eine endliche Gruppe und K ein Körper. Sei V ein K-Vektorraum mit Basis $\{v_g : g \in G\}$. Für $g, x \in G$ sei $\Delta(g) \colon V \to V$, $v_x \mapsto v_{gx}$ linear.

(a) Zeigen Sie, dass $\Delta \colon G \to \mathrm{GL}(V)$ eine treue Darstellung von G ist.

(b) Berechnen Sie den Charakter von Δ.

(c) Sei $\operatorname{char} K$ ein Teiler von $|G|$ und $s := \sum_{g\in G} v_g \in V$. Zeigen Sie, dass Ks ein Δ-invarianter Unterraum ist, der kein Δ-invariantes Komplement in V besitzt.

Man nennt Δ die *reguläre* Darstellung von G.

Aufgabe 2 (2 Punkte)**.** Bestimmen Sie die irreduziblen $\mathbb{C}$-Darstellungen einer endlichen zyklischen Gruppe.

Aufgabe 3 (2 + 2 Punkte)**.** Sei $n \in \mathbb{N}$ gerade und $G = D_{2n} = \langle \sigma, \tau \rangle$ die Diedergruppe der Ordnung $2n$. Zeigen Sie:

(a) Für alle $\epsilon, \mu \in \{\pm 1\}$ existiert eine Darstellung Δ von G mit $\Delta(\sigma) = \epsilon$ und $\Delta(\tau) = \mu$.

(b) Es gibt (mindestens) $\frac{n-2}{2}$ paarweise nicht-ähnliche irreduzible $\mathbb{R}$-Darstellungen von G vom Grad 2.

Aufgabe 4 (2 Punkte)**.** Sei Δ eine $\mathbb{C}$-Matrixdarstellung einer endlichen Gruppe G, und sei $g \in G$. Zeigen Sie, dass $\Delta(g)$ diagonalisierbar ist.
Hinweis: Man kann das Minimalpolynom oder Satz 2.2 der Vorlesung benutzen.

Aufgabe 5 (2 + 2 + 2 Punkte)**.** Sei Δ eine $\mathbb{C}$-Matrixdarstellung von G mit Charakter χ.

(a) Zeigen Sie, dass auch $\overline{\Delta}$ mit $\overline{\Delta}(g) := \overline{\Delta(g)}$ für $g \in G$ eine Matrixdarstellung von G ist. Dabei ist $\overline{\Delta(g)}$ das komplex Konjugierte von $\Delta(g)$.

(b) Δ ist genau dann irreduzibel, wenn $\overline{\Delta}$ irreduzibel ist.

(c) $\overline{\Delta}$ hat Charakter $\overline{\chi}$ mit $\overline{\chi}(g) := \overline{\chi(g)} = \chi(g^{-1})$ für $g \in G$.
Hinweis: Man kann Aufgabe 4 verwenden.

Aufgabe 6 (2 Punkte)**.** Seien $\chi, \psi \in \mathrm{Irr}(G)$ mit $\chi(1) = 1$. Zeigen Sie: $\chi\psi \in \mathrm{Irr}(G)$.

Aufgabe 7 (2 Punkte)**.** Bestimmen Sie die Charaktertafel von D_{4n} für $n \in \mathbb{N}$.

Aufgabe 8 (2 + 2 + 2 Punkte)**.** Sei $\Delta \colon G \to \mathrm{GL}(n, \mathbb{R})$ eine Darstellung. Zeigen Sie:

(a) $S := \sum_{g \in G} \Delta(g)\Delta(g)^{\mathrm{t}}$ ist symmetrisch und positiv definit.

(b) Es existiert $T \in \mathrm{GL}(n, \mathbb{R})$ mit $T^2 = S$.
Hinweis: Spektralsatz.

(c) $T^{-1}\Delta(x)T$ ist eine orthogonale Matrix für alle $x \in G$.

Bemerkung: Jede $\mathbb{R}$-Darstellung ist also zu einer *orthogonalen* Darstellung $G \to \mathrm{O}(n, \mathbb{R})$ ähnlich.

Aufgabe 9 (2 + 2 + 3 Punkte)**.** Sei

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

die *Quaternionengruppe*. Zeigen Sie:

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

(b) Bestimmen Sie die Charaktertafel von Q_8 und vergleichen Sie mit D_8 (Aufgabe 7).

(c) Zeigen Sie, dass die Einbettung $Q_8 \hookrightarrow \mathrm{GL}(2, \mathbb{C})$ zu keiner $\mathbb{R}$-Darstellung ähnlich ist, obwohl der Charakter reellwertig ist.
Hinweis: Aufgabe 8.
Bemerkung: Daraus folgt $Q_8 \ncong D_8$.

Aufgabe 10 (2 + 2 + 2 + 2 Punkte)**.** Zeigen Sie:

(a) Für Charaktere χ, ψ von G gilt: $\operatorname{Ker}(\chi + \psi) = \operatorname{Ker}(\chi) \cap \operatorname{Ker}(\psi)$.

(b) Jeder Normalteiler von G ist der Kern eines Charakters.

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

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

Aufgabe 11 (3 Punkte)**.** Bestimmen Sie die Charaktertafel von S_3 mit dem Burnside-Algorithmus (Satz 3.19).

Aufgabe 12 (2 Punkte)**.** Finden Sie ein normiertes, ganzzahliges Polynom mit Nullstelle $\sqrt{2} + \sqrt[3]{3}$.

Aufgabe 13 (3 Punkte)**.** Sei A eine abelsche Untergruppe von G und $\chi \in \operatorname{Irr}(G)$. Zeigen Sie:

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

Hinweis: Frobenius-Reziprozität.

Aufgabe 14 (3 Punkte)**.** Eine *Permutationsmatrix* hat die Form $P = (\delta_{i\pi(j)})_{i,j} \in \mathbb{Z}^{n \times n}$, wobei $\pi \in S_n$ und δ_{ij} das Kronecker-Delta ist. Bestimmen Sie die Eigenwerte von P in Abhängigkeit von π.

Aufgabe 15 (2 + 1 + 3 + 2 Punkte)**.** Sei $N \trianglelefteq G$, $g \in G$ und ψ ein Charakter von N. Zeigen Sie:

(a) Die Abbildung ${}^g\psi \colon N \to \mathbb{C}$, $x \mapsto \psi(g^{-1}xg)$ ist ein Charakter von N.

(b) Durch $(g, \psi) \mapsto {}^g\psi$ operiert G auf $\operatorname{Irr}(N)$.

(c) (Clifford) Für $\chi \in \operatorname{Irr}(G)$ existieren $e \in \mathbb{N}$ und $\psi \in \operatorname{Irr}(N)$ mit

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

wobei G_ψ der Stabilisator von ψ in G ist.
Bemerkung: Man nennt e den *Verzweigungsindex* von χ bzgl. N.

(d) Genau dann gilt $\psi^G \in \operatorname{Irr}(G)$, wenn $\psi \in \operatorname{Irr}(N)$ und $G_\psi = N$.

Aufgabe 16 (3 Punkte)**.** Sei F ein endlicher Körper mit $|F| > 2$. Für $a \in F^\times$ und $b \in F$ sei $\varphi_{a,b} \colon F \to F$, $x \mapsto ax + b$. Zeigen Sie, dass

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

eine Frobeniusgruppe ist.

Aufgabe 17 (2 + 2 + 2 + 2 Punkte)**.** Jede Operation von G auf einer Menge Ω induziert bekanntlich einen Homomorphismus $\varphi \colon G \to S_n$ mit $n = |\Omega|$. Zeigen Sie:

(a) Die Abbildung $\tau \colon S_n \to \mathrm{GL}(n, \mathbb{C})$, $\pi \mapsto (\delta_{i\pi(j)})_{i,j=1}^n$ ist ein Monomorphismus. Insbesondere ist $\Delta := \tau \circ \varphi \colon G \to \mathrm{GL}(n, \mathbb{C})$ eine Darstellung von G. (Man nennt Δ *Permutationsdarstellung*.)

(b) Für den Charakter χ von Δ gilt $\chi(g) := |\{\omega \in \Omega : {}^g\omega = \omega\}|$ für $g \in G$. (Man nennt χ *Permutationscharakter*.)

(c) Seien $\omega_1, \ldots, \omega_m \in \Omega$ Repräsentanten für die Bahnen der Operation. Dann ist

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

wobei G_ω der Stabilisator von $\omega \in \Omega$ in G ist.

(d) Es gilt $m = (\mathbb{1}_G, \chi)_G$. Insbesondere ist $\chi - \mathbb{1}_G$ ein Charakter von G, falls $n > 1$.

Aufgabe 18 (2 Punkte)**.** Zeigen Sie, dass S_n für $n \geq 2$ zu einer Untergruppe von $\mathrm{GL}(n-1, \mathbb{Z})$ isomorph ist.

Aufgabe 19 $(2 + 2 + 2$ Punkte$)$**.** Zeigen Sie:

(a) Permutationen vom gleichen Zyklentyp in S_n sind konjugiert.

(b) Sind $g, h \in S_n$ mit $\langle g \rangle = \langle h \rangle$, so sind g und h konjugiert.

(c) Die Charaktertafel von S_n ist ganzzahlig.
Hinweis: Brauers Permutationslemma.

Aufgabe 20 (3 Punkte)**.** Zeigen Sie, dass

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

als Unteralgebra von $\mathbb{C}^{2\times 2}$ eine $\mathbb{R}$-Divisionsalgebra ist. Man nennt $\mathbb{H}$ nach Hamilton *Quaternionenalgebra*.
Bemerkung: Frobenius hat gezeigt, dass $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{H}$ die einzigen Divisionsalgebren über $\mathbb{R}$ sind.

Aufgabe 21 $(2 + 2$ Punkte$)$**.** Sei A eine einfache Algebra. Zeigen Sie:

(a) $\mathrm{Z}(A)$ ist ein Körper.

(b) Je zwei einfache A-Moduln sind isomorph.

Aufgabe 22 (2 Punkte)**.** Sei A eine Algebra. Zeigen Sie, dass jeder einfache A-Modul zu einem direkten Faktor von $A/\mathrm{J}(A)$ isomorph ist. Insbesondere ist die Anzahl der Isomorphieklassen einfacher A-Moduln durch $\dim A/\mathrm{J}(A)$ beschränkt.
Bemerkung: Dies verbessert Folgerung 9.12 und wird in Folgerung 11.13 weiter verbessert.

Aufgabe 23 $(1 + 3 + 2 + 2$ Punkte$)$**.** Sei K ein Körper.

(a) Zeigen Sie, dass die Matrizen der Form

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

eine Unteralgebra A von $K^{3\times 3}$ bilden.

(b) Prüfen Sie, ob A kommutativ, halbeinfach oder lokal ist.

(c) Bestimmen Sie eine Kompositionsreihe des regulären A-Moduls.

(d) Wie viele einfache Moduln besitzt A bis auf Isomorphie?

Die folgenden Aufgaben wurden nicht gestellt:

Aufgabe 24 (2+2+2+2 Punkte)**.** Seien G, H endliche, abelsche Gruppen. Zeigen Sie:

(a) $\widehat{G} := \mathrm{Irr}(G)$ ist eine abelsche Gruppe bzgl. Multiplikation. (Man nennt $\widehat{G}$ *Charaktergruppe* von G.)

(b) $\widehat{\widehat{G}} \cong G$
Hinweis: Denken Sie an den Bidualraum. Verwenden Sie nicht (d).

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

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

Aufgabe 25 (2 Punkte)**.** Sei $x \in \mathbb{C}$ algebraisch. Zeigen Sie, dass x genau dann ganz-algebraisch ist, wenn das Minimalpolynom von x in $\mathbb{Z}[X]$ liegt.

Aufgabe 26 (2 Punkte)**.** Zeigen Sie $\gamma_{CDE} = \gamma_{DCE}$ für alle $C, D, E \in \mathrm{Cl}(G)$.

Aufgabe 27 (3 Punkte)**.** Sei $A \in K^{n\times n}$ und $B \in K^{m\times m}$. Zeigen Sie für das Kronecker-Produkt $\det(A \otimes B) = \det(A)^m \det(B)^n$.
Hinweis: Gauß-Algorithmus.

Aufgabe 28 (2 Punkte)**.** Sei $N \trianglelefteq G$ und $\chi \in \mathrm{Irr}(G)$. Zeigen Sie, dass $(\chi_N)^G = \chi\rho$ gilt, wobei ρ die Inflation des regulären Charakters von G/N ist.

Aufgabe 29 (3 Punkte)**.** Sei $H \leq G$ und Δ eine Darstellung von H mit Charakter χ. Sei $g_1, \ldots, g_n$ ein Repräsentantensystem für die Linksnebenklassen von H nach G. Sei $G \to S_n$, $x \mapsto \sigma_x$ die Operation auf G/H durch Linksmultiplikation, d. h. $xg_iH = g_{\sigma_x(i)}H$. Wir definieren die Blockmatrix

$$\Delta^G(x) := \big(\delta_{i,\sigma_x(j)}\Delta(g_i^{-1}xg_j)\big).$$

Zeigen Sie, dass Δ^G eine Darstellung von G mit Charakter χ^G ist.

Aufgabe 30 (2 Punkte)**.** Sei $H \leq G$ mit $\mathrm{ggT}(|H|, |G : H|) = 1$. Zeigen Sie $G' \cap \mathrm{Z}(G) \cap H \leq H'$.
Bemerkung: Dies verallgemeinert den Satz von Taunt.
Hinweis: Jede Gruppe wird von Sylowgruppen erzeugt.

Aufgabe 31 (2 Punkte)**.** Sei $G \leq \mathrm{GL}(n, \mathbb{Q})$ endlich. Zeigen Sie, dass ein Normalteiler $N \cong C_2^k$ (mit $k \in \mathbb{N}_0$) von G existiert, sodass G/N zu einer Untergruppe von $\mathrm{GL}(n, 2)$ isomorph ist.

Aufgabe 32 (3 Punkte)**.** Sei $G \leq \mathrm{GL}(2,\mathbb{R})$ endlich. Zeigen Sie: Ist $G \leq \mathrm{SL}(2,\mathbb{R})$, so ist G zyklisch und anderenfalls eine Diedergruppe.
Hinweis: Aufgabe 8.

Aufgabe 33 (Bonusaufgabe, +3 Punkte)**.** Ein *Charakter-Sudoku*: Vervollständigen Sie folgende Charaktertafel, in der die erste Spalte zum trivialen Element gehört:

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}					

Hinweis: Beispiel 3.16.

Aufgabe 34 (3 Punkte)**.** Sei K ein Körper und $n \in \mathbb{N}$. Für eine Relation $R \subseteq \{1,\dots,n\}^2$ sei

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

Zeigen Sie, dass A_R genau dann eine K-Algebra ist, wenn R reflexiv ($\forall i : (i,i) \in R$) und transitiv ($(i,j),(j,k) \in R \Rightarrow (i,k) \in R$) ist.
Bemerkung: Für die Gleichheitsrelation R erhält man die Diagonalmatrizen und für die Kleinergleich-Relation erhält man die oberen Dreiecksmatrizen.

Aufgabe 35 (3 Punkte)**.** Sei A eine Algebra. Zeigen Sie, dass A-Moduln M und N genau dann isomorph sind, wenn $\mathrm{Ann}(M) = \mathrm{Ann}(N)$ gilt.

Aufgabe 36 ($2+2+2$ Punkte)**.** Sei $e \neq 0$ ein Idempotent einer K-Algebra A. Zeigen Sie:

(a) eAe ist eine K-Algebra, aber im Allgemeinen keine Unteralgebra von A.

(b) $\mathrm{J}(eAe) = e\mathrm{J}(A)e$.

(c) $\mathrm{End}_A(Ae) \cong (eAe)^o$, wobei Ae der von e erzeugte Untermodul des regulären A-Moduls ist.

Zusatz: Gilt auch $\mathrm{Z}(eAe) = e\mathrm{Z}(A)e$?

Aufgabe 37 ($2+2$ Punkte)**.** Sei A eine Algebra und $N \leq M$ A-Moduln. Zeigen Sie:

(a) (Nakayamas Lemma) Aus $M = N + \mathrm{J}(A)M$ folgt $M = N$.

(b) $\mathrm{J}(M) := \mathrm{J}(A)M$ ist der Durchschnitt aller maximalen Untermoduln von M.

Hinweis: Beweis von Satz 9.15.

Aufgabe 38 (2 + 3 Punkte)**.** Zeigen Sie für jede endliche Gruppe G:

(a) Für $\chi \in \mathrm{Irr}(G)$ ist $\omega_\chi \colon \mathrm{Z}(\mathbb{C}G) \to \mathbb{C}$, $C^+ \mapsto \omega_\chi(C)$ ein Homomorphismus von Algebren.

(b) Jeder Homomorphismus $\mathrm{Z}(\mathbb{C}G) \to \mathbb{C}$ hat die Form ω_χ für ein $\chi \in \mathrm{Irr}(G)$.

Aufgabe 39 (3 Punkte)**.** Bestimmen Sie die Artin-Wedderburn-Zerlegung von $\mathbb{R}C_n$ für $n \in \mathbb{N}$.

Aufgabe 40 (4 Punkte)**.** Zeigen Sie, dass ein Zahlkörper K genau dann ein Zerfällungskörper für die endliche Gruppe G ist, wenn $n_1, \ldots, n_k \in \mathbb{N}$ mit $KG \cong K^{n_1 \times n_1} \times \ldots \times K^{n_k \times n_k}$ existieren.
Hinweis: Satz 12.7.

Aufgabe 41 (3 Punkte)**.** Sei K ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$ und G eine endliche Gruppe. Zeigen Sie, dass KG bis auf Isomorphie genau $|G : G'|_{p'}$ Moduln der Dimension 1 besitzt (dabei ist $|G : G'|_{p'}$ der größte zu p teilerfremde Teiler von $|G : G'|$).

Aufgabe 42 (2 + 3 + 3 + 3 Punkte)**.** Sei $G := \langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle \cong S_3$ mit der natürlichen Darstellung auf $V := \mathbb{Q}^2$. Sei $\mathfrak{A} := \mathbb{Z}^2 \subseteq V$ ein G-Gitter. Rekapitulieren Sie den Beweis von Jordan-Zassenhaus in dieser Situation:

(a) Zeigen Sie $M = 3s_1 1_2$. Man kann also $c = 9$ wählen.

(b) Konstruieren Sie alle Untergruppen in $\mathfrak{A}/9\mathfrak{A}$.

(c) Welche davon sind G-Gitter?

(d) Zeigen Sie, dass es genau sechs Isomorphieklassen von (nicht unbedingt einfachen) G-Gittern vom Rang 2 gibt.
Hinweis: Beispiel 13.16

Aufgabe 43 (2 Punkte)**.** Zeigen Sie, dass die Matrizen $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ mit $a \in \mathbb{N}$ in $\mathrm{GL}(2, \mathbb{Q})$ konjugiert sind, aber in $\mathrm{GL}(2, \mathbb{Z})$ paarweise nicht konjugiert sind.

Stichwortverzeichnis

Symbole

$(\chi, \psi)_G$, 8
$[x, y]$, 13
$\mathbb{1}_G$, 3
$\mathrm{Aff}(F)$, 60
A_n, 3
$\mathrm{Ann}(M)$, 38
A^o, 31
C^+, 48
$\mathrm{CF}(G)$, 8
$C(G)$, 12
$\mathrm{C}_G(g)$, 7
$\mathrm{Cl}(G)$, 7
$\mathrm{Cl}(g)$, 7
C_n, 13
D_{2^n}, 4
$\Delta \oplus \Gamma$, 4
Δ_H, 4
$\det \chi$, 7
E_{ij}, 9
$\mathrm{End}_A(M)$, 37
G', 13
$\gamma(A)$, 44
γ_{CDE}, 10
$\mathbb{H}$, 61
$\mathrm{Hom}_A(M, N)$, 36
$\mathrm{Irr}(G)$, 6
$\mathrm{J}(M)$, 63
$k(G)$, 7
$\mathrm{Ker}(\chi)$, 15
$K^\times$, 3
$M \simeq N$, 36
$\omega_\chi(C)$, 10
φ^G, 19
Q_8, 59
$\overline{\mathbb{Q}}$, 25
$\mathbb{Q}_n$, 21
$\mathrm{Sec}_{p'}(x)$, 49
sgn, 3
S_n, 3
$\mathrm{Z}(A)$, 31
$\mathrm{Z}(\chi)$, 15

A

Algebra, 30
  einfache, 31
  entgegengesetzte, 31
  halbeinfache, 33
  lokale, 33
Annullator, 38
Artin-Wedderburn, 42

B

Bestandteil
  irreduzibler, 11
  Vielfachheit, 11
Brauer, 50
Brauer-Charakter, 51
Brauers Induktionssatz, 25
Brauers Permutationslemma, 28
Burnside, 48
Burnside-Algorithmus, 16
Burnsides p^aq^b-Satz, 22
Burnsides Verlagerungssatz, 24

C

Charakter, 6
  Grad, 6
  induzierter, 20
  irreduzibler, 6
  linearer, 7
  treuer, 6
  trivialer, 7
  Zentrum, 15
Charakter-Sudoku, 63
Charaktergruppe, 62
Charaktertafel, 12
  D_{4n}, 59
  A_4, 14
  A_5, 29
  abelsche Gruppe, 13
  $C_2 \times C_2$, 13
  C_n, 13
  Q_8, 59
  S_n, 61
Clifford, 60

D

Darstellung
  (ir)reduzible, 5
  absolut irreduzible, 25
  einer Algebra, 37
  ganzzahlige, 53
  Grad, 3
  orthogonale, 59
  reguläre, 58
  treue, 3
  triviale, 3
  ähnlich, 4
Darstellungstyp, 53
Dedekind-Identität, 36
Deflation, 4
Δ-invariant, 5
Diedergruppe, 4
direktes Produkt, 31

Dirichlet, 7
Divisionsalgebra, 30
Dixon-Schneider-Algorithmus, 16

E
Element
    Idempotent, 34
    konjugiert, 7
    nilpotent, 34
Endomorphismenalgebra, 37

F
Feit, 27
Fitting, 43
Frobenius, 22, 61
Frobenius-Reziprozität, 19
Frobeniusgruppe, 23

G
Galois-konjugiert, 28
ganz-algebraisch, 17
Gaschütz, 56
G-Gitter, 53
    einfaches, 53
    Homomorphismus, 55
    isomorphe, 55
Grad, 3
Gruppenalgebra, 46

H
Hamilton, 61
Higman, 53
Homomorphiesatz
    für Algebren, 32
    für Moduln, 36
Homomorphismus
    von Algebren, 31
    von Moduln, 36

I
Ideal, 31
    gebrochenes, 57
    nilpotentes, 32
Idempotent, 34
    heben, 34
Inflation, 4
Involution, 14
Isomorphiesätze
    für Algebren, 32
    für Moduln, 36

J
Jacobson-Radikal, 33
Jordan, 27
Jordan-Hölder, 37
Jordan-Zassenhaus, 56

K
K-Darstellung, 3
Klassenfunktion, 8
    induzierte, 19
Klassenmultiplikationskonstante, 10
Klassensumme, 48
Klassenzahl
    Gruppe, 7
    Zahlkörper, 57
Knapp-Schmid, 22
Koh, 35
Kommutator, 13
Kommutatorgruppe, 13
Kommutatorraum, 44
Kompositionsfaktor, 37
Kompositionsreihe, 37
Konjugationsklasse, 7
Korrespondenzsatz, 32
Kroneckerprodukt, 12
Krull-Schmidt, 43

M
Maschke, 5, 47
Matrixdarstellung, 3
Minkowski, 26
Minkowskis Linearformensatz, 55
Modul, 35
    (un)zerlegbarer, 42
    einfacher, 36
    halbeinfacher, 39
    regulärer, 35
    trivialer, 35, 47

N
Nakayamas Lemma, 63

O
Operation, 3
Orthogonalitätsrelation
    erste, 9
    zweite, 11

P
p-Element, p'-Element, 49
p-Faktor, p'-Faktor, 49
p-Konjugationsklasse, 49
p'-Sektion, 49
Permutationscharakter, 61
Permutationsdarstellung, 60
Permutationsmatrix, 60
    verallgemeinerte, 27

Q
Quaternionenalgebra, 61
Quaternionengruppe, 59

R
Radikal, 33

Rado, 55
Restriktion, 4

S
Schur, 30
Schur-Relationen, 8
Schurs Lemma, 6

T
Taunt, 23
Tensorprodukt, 54

U
Unteralgebra, 30
Untergitter, 53
Untermodul, 36

V
Verzweigungsindex, 60

W
Wedderburn, 31

Z
Zahlkörper, 25
Zentralisator, 7
Zentrum, 31
Zerfällungskörper, 25