Gewöhnliche Darstellung endlicher Gruppen

Matthias Künzer

Universität Stuttgart

10. September 2015

Inhalt

Vorwort

Eine Darstellung einer endlichen Gruppe G ist eine Multiplikationsoperation von G auf einem endlichdimensionalen Vektorraum V über einem Körper K. Eine solche Darstellung nennt man *gewöhnlich,* wenn $\operatorname{char} K = 0$; häufig nimmt man $K = \mathbf{C}$.

Zum Beispiel kann eine Untergruppe einer symmetrischen Gruppe durch Permutation von Basisvektoren operieren.

Allgemein liefert die Multiplikation mit einem Element g aus G auf V eine K-lineare Abbildung $V \longrightarrow V$, $v \longmapsto gv$. Die Spur dieser Abbildung heiße $\chi(g)$. Zusammengefaßt erhalten wir so den Charakter $\chi : G \longrightarrow K$, $g \longmapsto \chi(g)$ unserer Darstellung.

Über Charaktere gibt es eine reichhaltige Theorie, die wir studieren wollen. Man kann Charaktere addieren und multiplizieren, man hat ein Skalarprodukt, man kann sie zwischen verschiedenen Gruppen hin- und herschieben, etc.

Eine Anwendung ist die algebraische Aussage von Burnside, daß Gruppen, in deren Ordnung nur zwei Primfaktoren aufgehen, auflösbar ist. Eine weitere mögliche Anwendung ist die funktionentheoretische Aussage von Brauer, daß Artinsche L-Funktionen meromorph sind; wir werden uns auf die dazu nötige Darstellungstheorie beschränken und dabei getreulich [**10,** §10] folgen.

Vorausgesetzt werden Kenntnisse aus der Linearen Algebra, insbesondere die Begriffe der Gruppe, des Rings und des Moduls über einem Ring. Kenntnisse aus der Algebra sind hilfreich.

Dank geht an Nico Stein und Simon Klenk für zahlreiche Verbesserungen, sowie an Stephan Schmid, Franziska Müller, Astrid Burck, Christoph Hachtel und Simon Paridon für alternative Lösungen und weitere Hinweise.

Ein ganz herzlicher Dank geht an Inga Benner und Friederike Stoll, die mich eine Woche lang vertreten und die währenddessen nötigen Korrekturen im Skript vorgenommen haben.

Für weitere Hinweise auf Fehler und Unklarheiten bin ich dankbar.

Stuttgart, den 25.06.2013

Matthias Künzer

Konventionen.

Sei G eine Gruppe. Sei R ein kommutativer Ring. Seien A und B Ringe.

- Sei $f : X \longrightarrow Y$ eine Abbildung. Seien $U \subseteq X$ und $V \subseteq Y$ so, daß $f(U) \subseteq V$. Schreibe $f|_U^V : U \longrightarrow V$, $x \longmapsto f(x)$. Schreibe auch $f|_U := f|_U^Y$ und $f|^V := f|_X^V$, sofern anwendbar.
- Ist M eine endliche Menge, so schreiben wir $|M|$ für die Anzahl ihrer Elemente, auch ihre *Kardinalität* oder ihre *Länge* genannt. Es heißt $|G|$ üblicherweise ihre *Ordnung.*
- Sprechen wir von *zwei Elementen* x und y einer Menge, so kann auch $x = y$ sein. Etc.
- Für Elemente x und y sei $\partial_{x,y} := 1$, falls $x = y$, und $\partial_{x,y} := 0$, falls $x \neq y$.
- Für $a, b \in \mathbf{Z}$ schreiben wir $[a, b] := \{ c \in \mathbf{Z} : a \leqslant c \leqslant b \}$ für das ganzzahlige Intervall. Ferner schreiben wir $\mathbf{Z}_{\geqslant a} := \{z \in \mathbf{Z} : z \geqslant a\}$ etc.
- Sind $a, b \in \mathbf{Z}$ und ist nicht $0 \leqslant a \leqslant b$, so sei der Binomialkoeffizient $\binom{b}{a}$ gleich 0.
- Sind $x, y, r \in R$, so schreiben wir $x \equiv_{rR} y$ oder $x \equiv_r y$ für $x - y \in rR$.
- Sei I eine Menge. Sei X_i eine Menge für $i \in I$. Die äußere disjunkte Vereinigung werde

$$\bigsqcup_{i \in I} X_i \;=\; \{ (x, i) : i \in I, x \in X_i \}$$

  geschrieben. Der zweite Eintrag i in (x, i) dient lediglich der Unterscheidung.

  Unberührt davon ist die Begriff einer inneren disjunkten Vereinigung von Teilmengen, welche als gewöhnliche Vereinigungsmenge erklärt ist, falls deren Teilnehmer paarweise leere Schnittmenge haben. Diesenfalls kann man auch die äußere disjunkte Vereinigung bilden. Diese steht aber in kanonischer Bijektion zur inneren disjunkten Vereinigung. Oft unterscheidet man daher beide Begriffe nicht.
- Erschließt sich der Summationsbereich I einer Summe aus dem Kontext, so wird auch auf dessen Nennung verzichtet und wir schreiben kurz $\sum_i := \sum_{i \in I}$.
- Das Inverse eines Gruppenelements g wird als g^{-1} oder als g^- bezeichnet ("g invers"). Entsprechend die Inverse einer Bijektion.
- Ist eine Teilmenge U von G eine Untergruppe, so schreiben wir dies auch $U \leqslant G$. Wir schreiben $U < G$ für ($U \leqslant G$ und $U \neq G$). Ist U ein Normalteiler von G, so schreiben wir dies auch $U \trianglelefteqslant G$. Wir schreiben $U \lhd G$ für ($U \trianglelefteqslant G$ und $U \neq G$).
- Die triviale Gruppe wird auch $1 = \{1\}$ geschrieben.
- Für eine Menge M bezeichnet S_M die Gruppe der Bijektionen von M nach M. Insbesondere ist $\mathrm{S}_n := \mathrm{S}_{[1,n]}$ für $n \in \mathbf{Z}_{\geqslant 0}$ die *symmetrische Gruppe,* für welche wir die links komponierte Zykelschreibweise verwenden, also e.g. $(1, 2) \circ (1, 3) = (1, 3, 2)$.
- Sei $n \in \mathbf{Z}_{\geqslant 1}$. Es bezeichnet C_n die zyklische Gruppe von Ordnung n.
- Seien $g, x \in G$. Schreibe ${}^g x := gxg^-$ für das mit g von links konjugierte Element x. Entsprechend für $M \subseteq G$ sei ${}^g M = \{ {}^g m : m \in M \}$. Elemente x und y von G, für welche es ein $g \in G$ mit ${}^g x = y$ gibt, nennt man zueinander konjugiert. Auch Teilmengen M und N von G, für welche es ein $g \in G$ mit ${}^g M = N$ gibt, nennt man zueinander konjugiert.
- Sei $X \subseteq G$ eine Teilmenge. Es bezeichnet $\langle X \rangle = \bigcap_{X \subseteq U \leqslant G} U \leqslant G$ das Untergruppenerzeugnis von X, i.e. die Menge der beliebigen endlichen Produkte mit Faktoren aus X und aus der Menge ihrer Inversen. Sind $k \in \mathbf{Z}_{\geqslant 0}$ und $g_1, \ldots, g_k \in G$ gegeben, so schreiben wir auch $\langle g_1, \ldots, g_k \rangle := \langle \{g_1, \ldots, g_k\} \rangle$.

- Ein Isomorphismus $f : G \xrightarrow{\sim} G$ heißt auch Automorphismus. Gibt es ein $x \in G$ mit $f(g) = {}^x g$ für $g \in G$, so heißt der Automorphismus f inner.
- Sei p eine Primzahl. Eine endliche Gruppe, deren Ordnung eine Potenz von p ist, wird auch p-Gruppe genannt.
- Seien $m,\, n \in \mathbf{Z}_{\geqslant 0}$. Sei $R^{m\times n}$ die Menge der $m\times n$-Matrizen mit Einträgen in R. Wir identifizieren $R^{1\times 1}$ mit R.
- Für einen R-Modul V schreiben wir $\mathrm{GL}(V)$ für die Gruppe der bijektiven R-linearen Abbildungen von V nach V, mit der Komposition als Multiplikation. Ferner werde $\mathrm{GL}(R^{n\times 1})$ mit $\mathrm{GL}_n(R)$ via der Standardbasis von R^n identifiziert.
- Sei $n \in \mathbf{Z}_{\geqslant 0}$. Es bezeichne $\mathrm{E}_n := (\partial_{i,j})_{i,j} \in R^{n\times n}$ die Einheitsmatrix.
- Seien $m,\, n \geqslant 0$. Sei $i \in [1, m]$ und $j \in [1, n]$. Es bezeichnet $\mathrm{e}_{i,j} \in R^{m\times n}$ die Matrix, die an Position (i, j) den Eintrag 1 hat, und 0 sonst.
- Die Spurabbildung auf Matrizen und linearen Endomorphismen wird mit tr bezeichnet.
- Es bezeichne $\mathrm{U}(A) := \{\, a \in A \,:\, \text{es gibt ein } b \in A \text{ mit } ab = 1 \text{ und } ba = 1 \,\}$ die Einheitengruppe von A.
- Sei $n \geqslant 1$. Es bezeichne $A^{\times n} = A \times A \times \cdots \times A$ mit n direkten Faktoren und komponentenweiser Addition und Multiplikation.
- Wir schreiben $\zeta_n := \exp(2\pi\mathrm{i}/n)$ für $n \in \mathbf{Z}_{\geqslant 1}$ für die erste primitive n-te Einheitswurzel.
- Unter einem A-Modul verstehen wir einen A-Linksmodul.
- Sei M ein A-Modul. Es heißt M *unzerlegbar*, wenn $M \neq 0$ und wenn aus $M = X \oplus Y$ mit Teilmoduln $X,\, Y \subseteq M$ bereits $X = 0$ oder $Y = 0$ folgt. Es heißt M *einfach,* wenn $M \neq 0$ ist und M nur die Teilmoduln 0 und M hat. Ist M einfach, so ist M unzerlegbar.
- Ist M ein A-Modul und ist $k \in \mathbf{Z}_{\geqslant 0}$, so schreiben wir $M^{\oplus k} := \bigoplus_{i\in[1,k]} M$.
- Die Tatsache, daß M ein A-B-Bimodul ist, schreiben wir kurz ${}_A M_B$, etc.
- Für $a,\, b \in \mathbf{R}$ schreiben wir $\overline{a + b\,\mathrm{i}} := a - b\,\mathrm{i}$ für das komplex konjugierte Element.

Verzeichnis der Sätze und einiger Lemmata

Kapitel 1

Gruppen

Der Begriff der Gruppe, der Untergruppe, des Untergruppenerzeugnisses, des Normalteilers, der Nebenklassen, der Faktorgruppe und des Gruppenmorphismus werden als aus der Linearen Algebra bekannt vorausgesetzt.

Beispiele endlicher Gruppen sind die symmetrischen Gruppen S_n für $n \in \mathbf{Z}_{\geqslant 0}$ und ihre Untergruppen.

Nach dem Lemma von Cayley ist jede endliche Gruppe isomorph zu einer Untergruppe einer symmetrischen Gruppe.

1.1 Operationen von Gruppen auf Mengen

Sei G eine Gruppe.

Definition 1 Eine *G-Linksmenge,* kurz *G-Menge,* $(M, \cdot)$ besteht aus einer Menge M und einer Abbildung

$$\begin{array}{ccccc} G & \times & M & \xrightarrow{(\cdot)} & M \\ (g & , & m) & \longmapsto & g \cdot m \;=\; gm \end{array}$$

so, daß die folgenden Axiome (Op 1, 2) gelten.

(Op 1) Es ist $1 \cdot m = m$ für $m \in M$.

(Op 2) Es ist $(g \cdot h) \cdot m = g \cdot (h \cdot m)$ für $g, h \in G$ und $m \in M$.

Oft schreibt man auch $ghm := (gh)m = g(hm)$.

Unter der Kardinalität einer G-Menge $(M, \cdot)$ versteht man die Kardinalität von M. Insbesondere heißt $(M, \cdot)$ endlich, falls M endlich ist.

Oft schreibt man auch kurz $M := (M, \cdot)$. Man sagt auch, es liegt eine *G-Operation* auf M vor, oder G *operiere* auf M.

Beispiel 2

(1) Auf jeder Menge M gibt es die *triviale* G-Operation, für welche $gm = m$ für $g \in G$ und $m \in M$ ist. Auf der leeren oder auf einer einelementigen Menge ist dies auch die einzige G-Operation.

(2) Sei $n \in \mathbf{Z}_{\geqslant 0}$ und $G \leqslant \mathrm{S}_n$. Es operiert G auf $[1,n]$ vermöge $g \cdot i := g(i)$ für $g \in G$ und $i \in [1,n]$, i.e. durch Anwendung der Bijektion g auf i.

(3) Sei $U \leqslant G$. Auf der Menge der Linksnebenklassen $G/U = \{\, xU \,:\, x \in G \,\}$ operiert G via $g \cdot xU := gxU$ für $g,\, x \in G$.

Insbesondere erhalten wir für $U = 1$ die *reguläre* G-Menge $G/1 = G$.

(4) Sei I eine Menge. Sei M_i eine G-Menge für $i \in I$.

(i) Es ist die disjunkte Vereinigung $\bigsqcup_{i\in I} M_i$ eine G-Menge vermöge $g \cdot (m,i) := (gm,i)$ für $g \in G$, $i \in I$ und $m \in M_i$.

(ii) Es ist das cartesische Produkt $\prod_{i\in I} M_i = \{\, (m_i)_{i\in I} \,:\, m_i \in M_i \text{ für } i \in I \,\}$ eine G-Menge vermöge $g \cdot (m_i)_{i\in I} := (gm_i)_{i\in I}$ für $g \in G$ und $m_i \in M_i$ für $i \in I$.

(5) Sei M eine G-Menge. Sei $H \xrightarrow{f} G$ ein Gruppenmorphismus. Dann ist M eine H-Menge vermöge $h \cdot m := f(h) \cdot m$ für $h \in H$ und $m \in M$. Zur Unterscheidung werde diese H-Menge auch ${}_fM$ geschrieben.

Wir haben e.g. in (2) aus der S_n-Menge $[1,n]$ via $G \hookrightarrow \mathrm{S}_n$ eine G-Menge gemacht.

(6) Es ist G auch eine G-Menge vermöge der Konjugationsoperation $g \cdot x := {}^g x = gxg^-$. Dies ist i.a. nicht die reguläre G-Operation; cf. (3).

Definition 3 Sei M eine G-Menge. Sei $X \subseteq M$ eine Teilmenge.

(1) Es heißt $\mathrm{C}_G(X) := \{\, g \in G \,:\, gx = x \text{ für } x \in X \,\} \leqslant G$ der *Zentralisator* von X.

(2) Es heißt $\mathrm{N}_G(X) := \{\, g \in G \,:\, gX = X \,\} \leqslant G$ der *Normalisator* von X, wobei $gX := \{\, gx \,:\, x \in X \,\}$ für $g \in G$.

Es ist $\mathrm{C}_G(X) \leqslant \mathrm{N}_G(X)$.

Vgl. Aufgabe 3. Wir schreiben auch $\mathrm{C}_G(m) := \mathrm{C}_G(\{m\})$ – aber nicht immer; cf. §1.2.

E.g. ist für die Konjugationsoperation von S_3 auf S_3 zum einen $\mathrm{C}_{\mathrm{S}_3}(\langle(1,2,3)\rangle) = \langle(1,2,3)\rangle$, zum anderen, wegen $\langle(1,2,3)\rangle \trianglelefteq \mathrm{S}_3$, aber $\mathrm{N}_{\mathrm{S}_3}(\langle(1,2,3)\rangle) = \mathrm{S}_3$.

Definition 4 Seien M und N zwei G-Mengen. Eine Abbildung $f : M \longrightarrow N$ heißt *Morphismus von G-Mengen* oder *G-äquivariant,* falls

$$f(g \cdot m) \;=\; g \cdot f(m)$$

für $g \in G$ und $m \in M$.

Ist f zudem bijektiv, so heißt f ein *Isomorphismus* von G-Mengen, symbolisch $f : M \xrightarrow{\sim} N$ geschrieben. Diesenfalls ist auch f^- ein Isomorphismus von G-Mengen; cf. Aufgabe 1. Zwei G-Mengen M und N heißen *isomorph,* geschrieben $M \simeq N$, falls ein Isomorphismus von M nach N existiert.

Wir schreiben auch ${}_G(M, N) := \{\, M \xrightarrow{f} N \,:\, f \text{ ist } G\text{-äquivariant} \,\}$.

Lemma 5 (Bahnenlemma) *Gegeben seien eine G-Menge M und $m \in M$.*

Sei $Gm := \{\, gm \,:\, g \in G \,\}$ die Bahn *von m unter der Operation von G. Mittels der von M eingeschränkten G-Operation wird Gm wieder zu einer G-Menge.*

Es ist

$$\begin{array}{rcl} G/\mathrm{C}_G(m) & \xrightarrow{f} & Gm \\ x\mathrm{C}_G(m) & \longmapsto & xm \end{array}$$

ein Isomorphismus von G-Mengen, wobei $x \in G$.

Beweis. Die Abbildung f ist wohldefiniert, da für $x, y \in G$ mit $x\mathrm{C}_G(m) = y\mathrm{C}_G(m)$ gilt, daß $x^-y \in \mathrm{C}_G(m)$ und also $xm = xx^-ym = ym$ ist.

Die Abbildung f ist G-äquivariant, da für $g, x \in G$ sich $f(g \cdot x\mathrm{C}_G(m)) = gxm = g \cdot f(x\mathrm{C}_G(m))$ ergibt.

Die Abbildung f ist nach Konstruktion surjektiv. Zum Nachweis ihrer Injektivität seien $x, y \in G$ mit $xm = ym$ gegeben. Es ergibt sich $m = x^-ym$, also $x^-y \in \mathrm{C}_G(m)$ und somit $x\mathrm{C}_G(m) = y\mathrm{C}_G(m)$. ▫

Bemerkung 6 (und Definition) *Gegeben sei eine G-Menge M.*

Für $m, n \in M$ sei $m \sim n$ genau dann, wenn es ein $g \in G$ mit $gm = n$ gibt. Es ist $(\sim)$ eine Äquivalenzrelation.

Die Äquivalenzklasse von $m \in M$ bezüglich $(\sim)$ ist die Bahn Gm. Ist $R \subseteq M$ also ein Repräsentantensystem der Äquivalenzklassen, so ist $M = \bigsqcup_{r \in R} Gr$.

Besteht M aus genau einer Äquivalenzklasse bezüglich $(\sim)$, so heißt M transitiv. *Diesenfalls ist $M = Gm$ für jedes $m \in M$.*

Beweis. Wir haben zu zeigen, daß $(\sim)$ eine Äquivalenzrelation ist.

Reflexivität gilt, da $1 \cdot m = m$ und also $m \sim m$ ist für $m \in M$.

Symmetrie gilt, da für $m, n \in M$ aus $m \sim n$ folgt, daß es ein $g \in G$ mit $gm = n$ gibt, also $m = g^-n$ ist, und sich somit $n \sim m$ ergibt.

Transitivität gilt, da für $m, n, p \in M$ aus $m \sim n$ und $n \sim p$ folgt, daß es ein $g \in G$ mit $gm = n$ und ein $h \in G$ mit $hn = p$ gibt, also $hgm = hn = p$ ist, und sich somit $m \sim p$ ergibt.

Korollar 7 (zu Lemma 5 und Bemerkung 6) *Sei M eine G-Menge. Es gibt eine Teilmenge $R \subseteq M$ mit $M = \bigsqcup_{r\in R} Gr$. Für eine solche ist*

$$\begin{array}{rcl} \bigsqcup_{r\in R}(G/\mathrm{C}_G(r)) & \xrightarrow{\sim} & M \\ (g\mathrm{C}_G(r), r) & \longmapsto & gr \end{array}$$

ein Isomorphismus von G-Mengen.

1.2 Sylowsätze nach Wielandt

Sei G eine endliche Gruppe. Sei p eine Primzahl. Schreibe $|G| = p^t n$ mit $t \in \mathbf{Z}_{\geqslant 0}$ und $n \in \mathbf{Z}_{\geqslant 1}$ mit $n \not\equiv_p 0$.

Sei $s \in [0, t]$ gegeben.

Sei

$$\Omega_G(p^s) \;:=\; \{\, M \subseteq G \,:\, |M| = p^s \,\}$$

die Menge der Teilmengen von G von Kardinalität p^s. Es ist $|\Omega_G(p^s)| = \binom{p^t n}{p^s}$.

Es operiert G auf $\Omega_G(p^s)$ vermöge $g \cdot M = gM := \{\, gm \,:\, m \in M \,\}$ für $g \in G$.

Es ist $\mathrm{C}_G(\{M\}) = \{\, g \in G \,:\, gM = M \,\} \leqslant G$.

Bemerkung 8 *Sei $m \in \mathbf{Z}_{\geqslant 1}$. Sei $\mathrm{C}_m = \langle x \rangle$ die zyklische Gruppe von Ordnung m. Sei d ein Teiler von m. Es hat C_m genau eine Untergruppe von Ordnung d.*

Beweis. Cf. Aufgabe 5. ▫

Bemerkung 9 *Sei $M \in \Omega_G(p^s)$.*

Es ist $|\mathrm{C}_G(\{M\})|$ ein Teiler von p^s.

Ist $|\mathrm{C}_G(\{M\})| = p^s$, so ist $M = \mathrm{C}_G(\{M\})m$ für ein $m \in M$.

Beweis. Schreibe $U := \mathrm{C}_G(\{M\})$. Es ist $uM = M$ für $u \in U = \mathrm{C}_G(\{M\})$. Also ist $um \in M$ für $u \in U$ und $m \in M$. Also ist $Um \subseteq M$ für $m \in M$. Somit ist

$$M \;=\; \bigcup_{m\in M} Um\,.$$

Da zwei solche Rechtsnebenklassen Um und Um' aus $U\backslash G$ gleich oder disjunkt sind, gibt es ein $k \in \mathbf{Z}_{\geqslant 1}$ und $m_i \in M$ für $i \in [1, k]$ mit

$$M \;=\; \bigsqcup_{i\in[1,k]} Um_i\,.$$

Da $|Um_i| = |U|$ für $i \in [1, k]$, ist $k|U| = |M|$, insbesondere also $|U|$ ein Teiler von $|M| = p^s$.

Ist ferner $|U| = p^s$, dann ist $k = 1$ und $M = Um_1$. ▫

Bemerkung 10 *Jede Bahn der G-Menge $\Omega_G(p^s)$ enthält höchstens eine Untergruppe von G.*

Beweis. Seien $H, \tilde{H} \leqslant G$ mit $|H| = |\tilde{H}| = p^s$ und $H, \tilde{H} \in \Omega_G(p^s)$ in derselben Bahn von G. Dann gibt es ein $g \in G$ mit $gH = \tilde{H}$. Insbesondere gibt es ein $h \in H$ mit $gh = 1$. Also ist $g = h^- \in H$, und folglich $H = gH = \tilde{H}$. ▫

Bemerkung 11 *Eine Bahn der G-Menge $\Omega_G(p^s)$ enthält genau dann eine Untergruppe von G, wenn sie Länge $p^{t-s}n$ hat.*

Beweis.

$\Rightarrow$. Sei $H \leqslant G$ mit $|H| = p^s$ gegeben. Die Länge der Bahn $\{\, gH \,:\, g \in G \,\} = G/H$ des Elements $H \in \Omega_G(p^s)$ ist gleich $|G/H| = |G|/|H| = p^{t-s}n$.

$\Leftarrow$. Sei $M \in \Omega_G(p^s)$ mit $|\{\, gM \,:\, g \in G \,\}| = p^{t-s}n$ gegeben. Dann ist $|\mathrm{C}_G(\{M\})| = |G|/(p^{t-s}n) = p^s$; cf. Lemma 5. Also ist $M = \mathrm{C}_G(\{M\})m$ für ein $m \in M$; cf. Bemerkung 9. Folglich ist die Untergruppe $m^-\mathrm{C}_G(\{M\})m = m^-M$ in der Bahn von M in $\Omega_G(p^s)$. ▫

Bemerkung 12 *Wenn eine Bahn der G-Menge $\Omega_G(p^s)$ nicht von Länge $p^{t-s}n$ ist, dann ist ihre Länge ein Vielfaches von $p^{t-s+1}n$.*

Beweis. Sei $M \in \Omega_G(p^s)$. Es ist

$$\frac{|G|}{|\{\, gM \,:\, g \in G \,\}|} \overset{\text{L. 5}}{=} |\mathrm{C}_G(\{M\})|$$

ein Teiler von p^s ; cf. Bemerkung 9. I.e. es gibt ein $v \in \mathbf{Z}_{\geqslant 0}$ mit

$$\frac{p^t n}{|\{\, gM \,:\, g \in G \,\}|} \cdot p^v \;=\; p^s \;,$$

i.e.

$$|\{\, gM \,:\, g \in G \,\}| \;=\; p^{t-s+v}n \;.$$

Ist nun $|\{\, gM \,:\, g \in G \,\}| \neq p^{t-s}n$, so ist $v \geqslant 1$. ▫

Satz 13 (Sylow-Wielandt)
Weiterhin sei G eine endliche Gruppe, p eine Primzahl, $|G| = p^t n$ mit $n \not\equiv_p 0$, sowie $s \in [0, t]$.

Es ist $|\{\, H \leqslant G \,:\, |H| = p^s \,\}| \equiv_p 1$.

Insbesondere gibt es in G wenigstens eine Untergruppe der Ordnung p^s.

Beweis. Sei

$$\Omega_G(p^s) \;=\; \bigsqcup_{i\in[1,b]} \{\, gM_i \,:\, g\in G\,\}$$

mit $b\in\mathbf{Z}_{\geqslant 1}$ und $M_i\in\Omega_G(p^s)$ für $i\in[1,b]$ die disjunkte Zerlegung der G-Menge $\Omega_G(p^s)$ in Bahnen; so sortiert, daß es ein $a\in[0,b]$ gibt mit

$$|\{\, gM_i \,:\, g\in G\,\}| \;=\; p^{t-s}n \;\iff\; i\in[1,a]\;.$$

Für $i\in[1,b]$ enthält die Bahn $\{\, gM_i \,:\, g\in G\,\}$ also genau dann eine Untergruppe von G, wenn $i\in[1,a]$; cf. Bemerkung 11. Folglich ist $a=|\{\, H\leqslant G \,:\, |H|=p^s\,\}|$; cf. Bemerkung 10. Es wird

$$\begin{aligned}\tbinom{p^tn}{p^s} \;=\; |\Omega_G(p^s)| \;=\; \textstyle\sum_{i\in[1,b]} |\{\, gM_i \,:\, g\in G\,\}| &\overset{\text{B. 12}}{\equiv}_{p^{t-s+1}n} \textstyle\sum_{i\in[1,a]} |\{\, gM_i \,:\, g\in G\,\}| \\ &= |\{\, H\leqslant G \,:\, |H|=p^s\,\}|\cdot p^{t-s}n\;.\end{aligned}$$

Da man so für jede Gruppe der Ordnung p^tn schließen kann, also auch für C_{p^tn}, wird

$$\begin{aligned}|\{\, H\leqslant G \,:\, |H|=p^s\,\}|\cdot p^{t-s}n \;\equiv_{p^{t-s+1}n}\; \tbinom{p^tn}{p^s} \;\equiv_{p^{t-s+1}n}\; |\{\, H\leqslant \mathrm{C}_{p^tn} \,:\, |H|=p^s\,\}|\cdot p^{t-s}n \\ \overset{\text{B. 8}}{=}\; p^{t-s}n\;.\end{aligned}$$

Kürzen von $p^{t-s}n$ liefert hieraus

$$|\{H\leqslant G \,:\, |H|=p^s\}| \;\equiv_p\; 1\;.$$

□

Lemma 14 *Sei K eine p-Gruppe. Sei M eine endliche K-Menge.*

Dann ist $|M|\equiv_p |\{\, m\in M \,:\, xm=m \text{ für } x\in K\,\}|$.

Falls $|M|\not\equiv_p 0$ ist, dann gibt es also ein $m\in M$, für welches $xm=m$ ist für $x\in K$.

Beweis. Schreibe $|K|=p^a$ für ein $a\in\mathbf{Z}_{\geqslant 0}$.

Zerlege $M=\bigsqcup_{i\in[1,\ell]} Km_i$ mit $\ell\in\mathbf{Z}_{\geqslant 0}$ und $m_i\in M$ für $i\in[1,\ell]$.

Es ist $|Km_i|=\frac{|K|}{|\mathrm{C}_K(m_i)|}$ ein Teiler von $|K|=p^a$ für $i\in[1,\ell]$; cf. Lemma 5. Insbesondere ist $|Km_i|\equiv_p 0$ für $i\in[1,\ell]$ mit $|Km_i|\neq 1$. Auf der anderen Seite ist $|Km_i|=1$ genau dann, wenn $xm_i=m_i$ ist für $x\in K$; umgekehrt liegt jedes Element $m\in M$, für welches $xm=m$ ist für $x\in K$, in einer Bahn der Länge 1 von M unter der Operation von K. Also wird

$$|M| \;=\; \textstyle\sum_{i\in[1,\ell]} |Km_i| \;\equiv_p\; \sum_{i\in[1,\ell],\,|Km_i|=1} |Km_i| \;=\; |\{\, m\in M \,:\, xm=m \text{ für } x\in K\,\}|\;.$$

□

Satz 15 (Sylow)
Weiterhin sei G eine endliche Gruppe, p eine Primzahl und $|G| = p^t n$ mit $n \not\equiv_p 0$.

Eine Untergruppe $H \leqslant G$ mit $|H| = p^t$ heißt auch p-Sylowgruppe *von G.*

(1) *Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.*

(2) *Je zwei p-Sylowgruppen von G sind zueinander konjugiert in G.*

Beweis. Es gibt eine p-Sylowgruppe $H \leqslant G$; cf. Satz 13. Seien $s \in [0, t]$ und $K \leqslant G$ mit $|K| = p^s$ gegeben. Für (1) und (2) genügt es zu zeigen, daß K in einer zu H konjugierten Untergruppe enthalten ist.

Es wird die G-Menge G/H zu einer K-Menge durch Einschränken; cf. Beispiel 2.(5). Es ist $|G/H| = |G|/|H| = n \not\equiv_p 0$. Also gibt es ein $g \in G$ mit $xgH = gH$ für alle $x \in K$; cf. Lemma 14. Somit ist $g^- xg \in H$ für alle $x \in K$, also $g^- Kg \leqslant H$ und also $K \leqslant {}^g H$. ▫

Beispiel 16 Wir betrachten die 2-Untergruppen der Gruppe S_4. Es ist $|\mathrm{S}_4| = 2^3 \cdot 3$.

Ordnung	Untergruppen	Anzahl der Untergruppen
2^0	1	1
2^1	$\langle(1,2)\rangle$, $\langle(1,3)\rangle$, $\langle(1,4)\rangle$, $\langle(2,3)\rangle$, $\langle(2,4)\rangle$, $\langle(3,4)\rangle$, $\langle(1,2)(3,4)\rangle$, $\langle(1,3)(2,4)\rangle$, $\langle(1,4)(2,3)\rangle$	9
2^2	$\langle(1,2),(3,4)\rangle$, $\langle(1,3),(2,4)\rangle$, $\langle(1,4),(2,3)\rangle$, $\langle(1,2)(3,4),(1,3)(2,4)\rangle$, $\langle(1,2,3,4)\rangle$, $\langle(1,2,4,3)\rangle$, $\langle(1,3,2,4)\rangle$	7
2^3 (2-Sylowgruppen)	$\langle(1,2,3,4),(1,3)\rangle$, $\langle(1,2,4,3),(1,4)\rangle$, $\langle(1,3,2,4),(1,2)\rangle$	3

Hierbei ist e.g.

$$\langle(1,2,3,4),(1,3)\rangle \;=\; \{\mathrm{id}, (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,3), (1,4)(2,3), (2,4), (1,2)(3,4)\}\,.$$

Nach Sylow-Wielandt ist die Anzahl der Untergruppen mit einer festen 2-Potenz als Ordnung kongruent zu 1 modulo 2, was wir bestätigt finden; cf. Satz 13.

Ferner erkennen wir, daß jede 2-Untergruppe in einer 2-Sylowgruppe enthalten ist und daß je zwei 2-Sylowgruppen zueinander konjugiert sind; cf. Satz 15.

Schließlich erkennen wir, daß i.a. nicht je zwei Untergruppen einer 2-Potenz-Ordnung zueinander konjugiert sind.

1.3 Präsentationen

1.3.1 Freie Gruppen

Sei X eine Menge. Sei $X^{\pm} := X \sqcup X = \{(x,i) \,:\, x \in X,\ i \in \{1,2\}\}$. Schreibe $x^{+1} := (x,1)$ und $x^{-1} := (x,2)$ für $x \in X$.

> Später wird x^{-1} in der Tat die Rolle des Inversen von x^{+1} spielen.

Sei $\mathrm{F}_0(X)$ die Menge der endlichen Wörter in $X^{\pm}$. Ein Element von $\mathrm{F}_0(X)$ ist also von der Form $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}$ mit $n \in \mathbf{Z}_{\geqslant 0}$, $x_i \in X$ und $\varepsilon_i \in \{-1,+1\}$ für $i \in [1,n]$. Das leere Wort werde zur Kenntlichmachung mit $\emptyset$ bezeichnet.

Sind $u,\, v \in \mathrm{F}_0(X)$, so bezeichne uv deren Aneinandersetzung.

Sei auf $\mathrm{F}_0(X)$ die Relation $(\rightsquigarrow)$ dadurch erklärt, daß für $u,\, v \in \mathrm{F}_0(X)$, $x \in X$ und $\varepsilon \in \{-1,+1\}$ gelte, daß $ux^{\varepsilon}x^{-\varepsilon}v \rightsquigarrow uv$.

Sei $(\approx)$ die Äquivalenzrelation auf $\mathrm{F}_0(X)$, die von $(\rightsquigarrow)$ erzeugt werde. Diese wollen wir nun auch konkret beschreiben.

Sei dazu auf $\mathrm{F}_0(X)$ die Relation $(\overset{\rightsquigarrow}{=})$ dadurch erklärt, daß für $u,\, v \in \mathrm{F}_0(X)$ genau dann $u \overset{\rightsquigarrow}{=} v$ gelte, wenn $u \rightsquigarrow v$ oder $u = v$.

Für $u,\, v \in \mathrm{F}_0(X)$ ist also $u \approx v$ genau dann, wenn es $n \in \mathbf{Z}_{\geqslant 1}$ und $w_i \in \mathrm{F}_0(X)$ für $i \in [1,n]$ und $w_i' \in \mathrm{F}_0(X)$ für $i \in [1,n-1]$ so gibt, daß, pars pro toto für $n = 4$,

$$\begin{array}{rcccc}
u & = & w_1 & \overset{\rightsquigarrow}{=} & w_1' \\
 & & & & \| \\
 & & w_2 & \overset{\rightsquigarrow}{=} & w_1' \\
 & & \| & & \\
 & & w_2 & \overset{\rightsquigarrow}{=} & w_2' \\
 & & & & \| \\
 & & w_3 & \overset{\rightsquigarrow}{=} & w_2' \\
 & & \| & & \\
 & & w_3 & \overset{\rightsquigarrow}{=} & w_3' \\
 & & & & \| \\
v & = & w_4 & \overset{\rightsquigarrow}{=} & w_3'
\end{array}$$

Bezeichne $[u]$ die Äquivalenzklasse von $u \in \mathrm{F}_0(X)$. Sei

$$\mathrm{F}(X) \;:=\; \mathrm{F}_0(X)/{\approx} \;=\; \{\, [u] \,:\, u \in \mathrm{F}_0(X) \,\}$$

die Menge der Äquivalenzklassen auf $\mathrm{F}_0(X)$ bezüglich $(\approx)$. Wir haben die Abbildung

$$\begin{array}{ccc}
X & \xrightarrow{\ \iota\ } & \mathrm{F}(X) \\
x & \longmapsto & [x^{+1}]\,.
\end{array}$$

Bemerkung 17 *Die Abbildung*

$$\begin{array}{ccccc} \mathrm{F}(X) & \times & \mathrm{F}(X) & \xrightarrow{(\cdot)} & \mathrm{F}(X) \\ ([u] & , & [v]) & \longmapsto & [u]\cdot[v] \;=\; [u][v] \;:=\; [uv]\,, \end{array}$$

Multiplikation genannt, ist wohldefiniert.

Beweis. Wir haben Repräsentantenunabhängigkeit zu zeigen. Es genügt zu zeigen, daß aus $u \rightsquigarrow \tilde{u}$ bereits $[uv] = [\tilde{u}v]$ folgt und daß aus $v \rightsquigarrow \tilde{v}$ bereits $[uv] = [u\tilde{v}]$ folgt, wobei $u,\, \tilde{u},\, v,\, \tilde{v} \in \mathrm{F}_0(X)$.

Zeigen wir ersteres; zweiteres ist dann analog zu behandeln.

Seien also $u,\, \tilde{u},\, v \in \mathrm{F}_0(X)$ mit $u \rightsquigarrow \tilde{u}$ gegeben. Dann gibt es $u',\, u'' \in \mathrm{F}_0(X)$, $x \in X$ und $\varepsilon \in \{-1,+1\}$ mit $u = u'x^{\varepsilon}x^{-\varepsilon}u''$ und $\tilde{u} = u'u''$. Dann aber ist auch

$$uv \;=\; u'x^{\varepsilon}x^{-\varepsilon}u''v \;\rightsquigarrow\; u'u''v \;=\; \tilde{u}v\,,$$

insbesondere also $[uv] = [\tilde{u}v]$. ▫

Lemma 18 (und Definition)
Zusammen mit der Multiplikation von Bemerkung 17 *ist* $\mathrm{F}(X)$ *eine Gruppe, genannt die* freie Gruppe *auf* X.

Hierbei ist $1 = 1_{\mathrm{F}(X)} = [\emptyset]$. *Ferner ist* $[x^{\varepsilon}]^{-} = [x^{-\varepsilon}]$ *für* $x \in X$ *und* $\varepsilon \in \{-1,+1\}$.

Beweis. Zur Assoziativität. Es wird

$$([u][v])[w] \;=\; [uv][w] \;=\; [uvw] \;=\; [u][vw] \;=\; [u]([v][w])\,.$$

für $u,\, v,\, w \in \mathrm{F}_0(X)$.

Zum Einselement. Es wird $[\emptyset][u] = [\emptyset u] = [u]$ und $[u][\emptyset] = [u\emptyset] = [u]$ für $u \in \mathrm{F}_0(X)$.

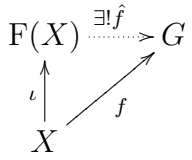
Zum inversen Element. Sei $u \in \mathrm{F}_0(X)$ gegeben. Schreibe $u = x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}$ mit $n \in \mathbf{Z}_{\geqslant 0}$, $x_i \in X$ und $\varepsilon_i \in \{-1,+1\}$ für $i \in [1,n]$. Setze $v := x_n^{-\varepsilon_n}\ldots x_1^{-\varepsilon_1}$. Es wird

$$\begin{array}{rcl} uv & = & x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}\, x_n^{-\varepsilon_n}\ldots x_1^{-\varepsilon_1} \\ & \rightsquigarrow & x_1^{\varepsilon_1}\ldots x_{n-1}^{\varepsilon_{n-1}}\, x_{n-1}^{-\varepsilon_{n-1}}\ldots x_1^{-\varepsilon_1} \\ & \rightsquigarrow & x_1^{\varepsilon_1}\ldots x_{n-2}^{\varepsilon_{n-2}}\, x_{n-2}^{-\varepsilon_{n-2}}\ldots x_1^{-\varepsilon_1} \\ & \rightsquigarrow & \ldots \\ & \rightsquigarrow & x_1^{\varepsilon_1}\, x_1^{-\varepsilon_1} \\ & \rightsquigarrow & \emptyset\,, \end{array}$$

sodaß $[u][v] = [uv] = [\emptyset] = 1$. Analog wird auch $[v][u] = 1$. ▫

Lemma 19 (Universelle Eigenschaft einer freien Gruppe)
Sei G eine Gruppe. Sei $f : X \longrightarrow G$ eine Abbildung.

Dann gibt es genau einen Gruppenmorphismus $\hat{f} : \mathrm{F}(X) \longrightarrow G$ mit $\hat{f} \circ \iota = f$.



Hierbei ist

$$\hat{f}([x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}]) \;=\; f(x_1)^{\varepsilon_1} \cdots f(x_n)^{\varepsilon_n} \;,$$

wobei $n \in \mathbf{Z}_{\geqslant 0}$, $x_i \in X$ und $\varepsilon_i \in \{-1, +1\}$ für $i \in [1, n]$.

Beweis.

Zur Eindeutigkeit. Sei $h : \mathrm{F}(X) \longrightarrow G$ ein Gruppenmorphismus mit $h \circ \iota = f$, i.e. mit $h([x^{+1}]) = f(x)$ für $x \in X$. Es folgt $h([x^{-1}]) = h([x^{+1}]^-) = h([x^{+1}])^- = f(x)^-$; cf. Lemma 18. Also ist

$$h([x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}]) \;=\; h([x_1^{\varepsilon_1}] \cdots [x_n^{\varepsilon_n}]) \;=\; h([x_1^{\varepsilon_1}]) \cdots h([x_n^{\varepsilon_n}]) \;=\; f(x_1)^{\varepsilon_1} \cdots f(x_n)^{\varepsilon_n}$$

für $n \in \mathbf{Z}_{\geqslant 0}$, $x_i \in X$ und $\varepsilon_i \in \{-1, +1\}$ für $i \in [1, n]$. Somit ist h durch Angabe von f festgelegt.

Zur Existenz. Wir definieren zunächst $\tilde{f} : \mathrm{F}_0(X) \longrightarrow G$ durch

$$\tilde{f}(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}) \;:=\; f(x_1)^{\varepsilon_1} \cdots f(x_n)^{\varepsilon_n}$$

für $n \in \mathbf{Z}_{\geqslant 0}$, $x_i \in X$ und $\varepsilon_i \in \{-1, +1\}$ für $i \in [1, n]$.

Wir wollen zeigen, daß $\hat{f} : \mathrm{F}(X) \longrightarrow G$, $[u] \longmapsto \tilde{f}(u)$ wohldefiniert ist.

Seien v, $w \in \mathrm{F}_0(X)$, $x \in X$ und $\varepsilon \in \{-1, +1\}$. Wir haben zu zeigen, daß

$$\tilde{f}(vx^{\varepsilon}x^{-\varepsilon}w) \;\stackrel{!}{=}\; \tilde{f}(vw) \;.$$

Schreibe $v = {y_1}^{\alpha_1} \dots {y_k}^{\alpha_k}$ und $w = {z_1}^{\beta_1} \dots {z_\ell}^{\beta_\ell}$, wobei $k, \ell \in \mathbf{Z}_{\geqslant 0}$, $y_i, z_j \in X$ und $\alpha_i, \beta_j \in \{-1, +1\}$ für $i \in [1, k]$ und $j \in [1, \ell]$. Wir erhalten in der Tat

$$\begin{aligned}
\tilde{f}(vx^{\varepsilon}x^{-\varepsilon}w) &= \tilde{f}({y_1}^{\alpha_1} \dots {y_k}^{\alpha_k} x^{\varepsilon} x^{-\varepsilon} {z_1}^{\beta_1} \dots {z_\ell}^{\beta_\ell}) \\
&= f(y_1)^{\alpha_1} \cdots f(y_k)^{\alpha_k} f(x)^{\varepsilon} f(x)^{-\varepsilon} f(z_1)^{\beta_1} \cdots f(z_\ell)^{\beta_\ell} \\
&= f(y_1)^{\alpha_1} \cdots f(y_k)^{\alpha_k} f(z_1)^{\beta_1} \cdots f(z_\ell)^{\beta_\ell} \\
&= \tilde{f}({y_1}^{\alpha_1} \dots {y_k}^{\alpha_k} {z_1}^{\beta_1} \dots {z_\ell}^{\beta_\ell}) \\
&= \tilde{f}(vw) \;.
\end{aligned}$$

Es ist $\hat{f}([x^{+1}]) = \tilde{f}(x^{+1}) = f(x)$ für $x \in X$, i.e. $\hat{f} \circ \iota = f$.

Bleibt zu verifizieren, daß $\hat{f}$ ein Gruppenmorphismus ist. Seien $v, w \in \mathrm{F}_0(X)$ in der Notation von eben gegeben. Dann wird

$$\begin{aligned}
\hat{f}([v][w]) &= \hat{f}([vw]) \\
&= \tilde{f}(vw) \\
&= \tilde{f}({y_1}^{\alpha_1} \dots {y_k}^{\alpha_k} {z_1}^{\beta_1} \dots {z_\ell}^{\beta_\ell}) \\
&= f(y_1)^{\alpha_1} \cdots f(y_k)^{\alpha_k} \cdot f(z_1)^{\beta_1} \cdots f(z_\ell)^{\beta_\ell} \\
&= \tilde{f}({y_1}^{\alpha_1} \dots {y_k}^{\alpha_k}) \cdot \tilde{f}({z_1}^{\beta_1} \dots {z_\ell}^{\beta_\ell}) \\
&= \tilde{f}(v) \cdot \tilde{f}(w) \\
&= \hat{f}([v]) \cdot \hat{f}([w]) \, .
\end{aligned}$$

□

Notation 20 Für $x \in X$ schreiben wir unter Mißbrauch von Notation kurz

$$x \;:=\; \iota(x) \;=\; [x^{+1}] \, .$$

Damit schreibt sich insbesondere $x^- = [x^{+1}]^- = [x^{-1}]$ für $x \in X$ und also $[x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}] = [x_1^{\varepsilon_1}] \cdots [x_n^{\varepsilon_n}] = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$, wobei $n \in \mathbf{Z}_{\geqslant 0}$, $x_i \in X$ und $\varepsilon_i \in \{-1, +1\}$ für $i \in [1, n]$.

1.3.2 Präsentationen via Erzeuger und Relationen

Bemerkung 21 (und Definition)
Sei H eine Gruppe. Sei $T \subseteq H$. Sei

$$\langle\!\langle\, T \,\rangle\!\rangle \;:=\; \bigcap_{T \subseteq N \trianglelefteqslant H} N \;\trianglelefteqslant\; H \, .$$

das Normalteilererzeugnis *von T in H.*

Es liegt $\langle\!\langle\, T \,\rangle\!\rangle$ in jedem Normalteiler von H, der T enthält.

Es ist $\langle\!\langle\, T \,\rangle\!\rangle = \langle \bigcup_{h \in H} {}^hT \rangle$. Also ist jedes Element von $\langle\!\langle\, T \,\rangle\!\rangle$ ein Produkt von Konjugierten von Elementen von T und ihrer Inversen.

Beweis. Wir haben zu zeigen, daß $\langle\!\langle\, T \,\rangle\!\rangle \overset{!}{\trianglelefteqslant} H$. In der Tat ist der Schnitt einer beliebigen Menge von Normalteilern einer Gruppe wieder ein Normalteiler dieser Gruppe.

Nach Konstruktion liegt $\langle\!\langle\, T \,\rangle\!\rangle$ in jedem Normalteiler von H, der T enthält.

Wir haben zu zeigen, daß $\langle\!\langle\, T \,\rangle\!\rangle \overset{!}{=} \langle \bigcup_{h \in H} {}^hT \rangle$.

Zu $\overset{!}{\leqslant}$. Es enthält $\langle \bigcup_{h \in H} {}^hT \rangle$ die Teilmenge T und ist invariant unter Konjugation.

Zu $\overset{!}{\geqslant}$. Es ist $T \subseteq \langle\!\langle\, T \,\rangle\!\rangle$. Da $\langle\!\langle\, T \,\rangle\!\rangle \trianglelefteqslant H$ ist, ist auch ${}^hT \subseteq \langle\!\langle\, T \,\rangle\!\rangle$ für $h \in H$. Da $\langle\!\langle\, T \,\rangle\!\rangle \leqslant H$ ist, folgt schließlich $\langle \bigcup_{h \in H} {}^hT \rangle \leqslant \langle\!\langle\, T \,\rangle\!\rangle$. □

Definition 22 Seien $n,\, m \geqslant 0$.

Sei $X = \{x_1\,, \ldots, x_n\}$ eine endliche Menge, wobei $x_i \neq x_j$ für $i,\, j \in [1,n]$ mit $i \neq j$.

Seien $r_1\,, \ldots,\, r_m \in \mathrm{F}(X)$.

Schreibe

$$\langle\, x_1\,, \ldots, x_n \,:\, r_1\,, \ldots,\, r_m \,\rangle \;:=\; \mathrm{F}(X)/\langle\!\langle\, \{r_1, \ldots, r_m\} \,\rangle\!\rangle\ .$$

Die Elemente x_i für $i \in [1,n]$ heißen *Erzeuger.* Die Elemente r_j für $j \in [1,m]$ heißen *Relationen.* Die eben definierte Gruppe heißt durch diese Erzeuger und diese Relationen *präsentiert.*

Nach Konstruktion ist das Bild einer Relation r_j in $\langle\, x_1\,, \ldots, x_n \,:\, r_1\,, \ldots,\, r_m \,\rangle$ gleich 1.

Notation 23 Unter Mißbrauch von Notation schreiben wir für $i \in [1,n]$ das Bild eines Elements x_i in $\langle\, x_1\,, \ldots, x_n \,:\, r_1\,, \ldots,\, r_m \,\rangle$ wieder

$$x_i \;:=\; x_i\langle\!\langle\, \{r_1\,, \ldots, r_m\} \,\rangle\!\rangle \;\overset{\text{N. 20}}{=}\; [x_i^{+1}]\langle\!\langle\, \{r_1\,, \ldots, r_m\} \,\rangle\!\rangle\ .$$

Die beiden Surjektionen

$$\begin{array}{ccccc} \mathrm{F}_0(X) & \longrightarrow & \mathrm{F}(X) & \longrightarrow & \langle\, x_1\,, \ldots, x_n \,:\, r_1\,, \ldots,\, r_m \,\rangle \\ u & \longmapsto & u & \longmapsto & u\langle\!\langle\, \{r_1\,, \ldots, r_m\} \,\rangle\!\rangle \end{array}$$

zeigen, daß in dieser Notation jedes Element in $\langle\, x_1\,, \ldots, x_n \,:\, r_1\,, \ldots,\, r_m \,\rangle$ von der Form $x_{i_1}^{\varepsilon_1} \cdots x_{i_k}^{\varepsilon_k}$ mit $k \in \mathbf{Z}_{\geqslant 0}$ und $i_j \in [1,n]$, $\varepsilon_j \in \{-1, +1\}$ für $j \in [1,k]$ ist.

Satz 24 (Universelle Eigenschaft einer präsentierten Gruppe)
Wir befinden uns weiterhin in der Situation von Definition 22.

Sei G eine Gruppe. Sei $f : X \longrightarrow G$ eine Abbildung.

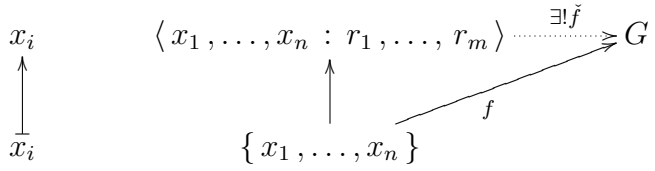
Wir erinnern daran, daß die Abbildung $\hat{f} : \mathrm{F}(X) \longrightarrow G$ ein Element $r = x_{i_1}^{\varepsilon_1} \cdots x_{i_k}^{\varepsilon_k}$ für $k \in \mathbf{Z}_{\geqslant 0}$ und $i_j \in [1,n]$, $\varepsilon_j \in \{-1, +1\}$ für $j \in [1,k]$ auf

$$\hat{f}(r) \;=\; f(x_{i_1})^{\varepsilon_1} \cdots f(x_{i_k})^{\varepsilon_k}$$

schickt; cf. Lemma 19.

Sei nun an f noch vorausgesetzt, daß $\hat{f}(r_j) = 1_G$ für $j \in [1,m]$.

Dann gibt es genau einen Gruppenmorphismus $\check{f} : \langle\, x_1\,, \ldots, x_n \,:\, r_1\,, \ldots,\, r_m \,\rangle \longrightarrow G$ so, daß $\check{f}(x_i) = f(x_i)$ für $i \in [1,n]$.



Beweis.

Eindeutigkeit. Sei $h : \langle x_1, \ldots, x_n : r_1, \ldots, r_m \rangle \longrightarrow G$ ein Gruppenmorphismus mit $h(x_i) = f(x_i)$ für $i \in [1,n]$. Dann ist

$$h(x_{i_1}^{\varepsilon_1} \cdots x_{i_k}^{\varepsilon_k}) \;=\; h(x_{i_1})^{\varepsilon_1} \cdots h(x_{i_k})^{\varepsilon_k} \;=\; f(x_{i_1})^{\varepsilon_1} \cdots f(x_{i_k})^{\varepsilon_k} \;,$$

wobei $k \in \mathbf{Z}_{\geqslant 0}$ und $i_j \in [1,n]$, $\varepsilon_j \in \{-1,+1\}$ für $j \in [1,k]$. Also ist h durch Angabe von f festgelegt.

Existenz. Wir verfügen über den Gruppenmorphismus $\hat{f} : \mathrm{F}(X) \longrightarrow G$ mit $\hat{f}(x_i) = f(x_i)$ für $i \in [1,n]$; cf. Lemma 19. Schreibe $A := \langle\!\langle \{r_1, \ldots, r_m\} \rangle\!\rangle \trianglelefteqslant \mathrm{F}(X)$. Nach Voraussetzung ist $\hat{f}(r_j) = 1$ für $j \in [1,m]$. Es folgt $\hat{f}(A) = 1$, da jedes Element von A ein Produkt von Konjugierten von Elementen der Form r_j und ihrer Inversen ist; cf. Bemerkung 21.

Wir haben zu zeigen, daß die Abbildung

$$\begin{array}{rcl} \langle x_1, \ldots, x_n : r_1, \ldots, r_m \rangle \;=\; \mathrm{F}(X)/A & \xrightarrow{\check{f}} & G \\ uA & \longmapsto & \hat{f}(u) \end{array}$$

ein wohldefinierter Gruppenmorphismus ist, der x_i nach $f(x_i)$ schickt für $i \in [1,n]$.

Zur Wohldefiniertheit. Sind $u, u' \in \mathrm{F}(X)$ mit $uA = u'A$ gegeben, so ist $u^- u' \in A$ und also $\hat{f}(u) = \hat{f}(u)\hat{f}(u^- u') = \hat{f}(uu^- u') = \hat{f}(u')$.

Zur Gruppenmorphie. Sind $u, u' \in \mathrm{F}(X)$ gegeben, dann wird

$$\check{f}(uA \cdot u'A) \;=\; \check{f}(uu'A) \;=\; \hat{f}(uu') \;=\; \hat{f}(u) \cdot \hat{f}(u') \;=\; \check{f}(uA) \cdot \check{f}(u'A) \;.$$

Schließlich wird $\check{f}(x_i) \overset{\text{N. 23}}{=} \check{f}(x_i A) = \hat{f}(x_i) \overset{\text{L. 19}}{=} f(x_i)$ für $i \in [1,n]$. ▫

Beispiel 25 Sei $\mathrm{D}_8 := \langle a, b : a^4, b^2, (ba)^2 \rangle$.

In D_8 ist jedes Element ein Produkt von Elementen a und b. Denn aus $a^4 = 1$ folgt $a^- = a^3$, und aus $b^2 = 1$ folgt $b^- = b$. Ferner ist $baba = 1$, und also auch $ba = a^- b^- = a^3 b$.

In D_8 ist jedes Element von der Form $a^i b^j$ mit $i \in [0,3]$ und $j \in [0,1]$. Denn in einem Produkt von Elementen a und b können wir unter Verwendung von $ba = a^3 b$ die Faktoren b nach rechts tauschen; e.g. wird $baabab = a^3 babab = a^3 a^3 bbab = a^2 1ab = a^3 b$. Insbesondere ist $|\mathrm{D}_8| \leqslant 8$.

Sei

$$\begin{array}{rcl} \{a,b\} & \xrightarrow{f} & \mathrm{S}_4 \\ a & \longmapsto & (1,2,3,4) \\ b & \longmapsto & (1,3) \;. \end{array}$$

Betrachten wir $\hat{f} : \mathrm{F}(\{a,b\}) \longrightarrow \mathrm{S}_4$, so wird

$$\begin{array}{lcllcl} \hat{f}(a^4) & = & f(a)^4 & = & (1,2,3,4)^4 & = \mathrm{id} \\ \hat{f}(b^2) & = & f(b)^2 & = & (1,3)^2 & = \mathrm{id} \\ \hat{f}((ba)^2) & = & (f(b) \circ f(a))^2 & = & (\underbrace{(1,2,3,4) \circ (1,3)}_{=(1,4)(2,3)})^2 & = \mathrm{id} \;. \end{array}$$

Also ist Satz 24 anwendbar, und wir erhalten einen Gruppenmorphismus

$$\begin{array}{rcl} \mathrm{D}_8 & \xrightarrow{\check{f}} & \mathrm{S}_4 \\ a & \longmapsto & (1,2,3,4) \\ b & \longmapsto & (1,3)\ . \end{array}$$

Sein Bild ist die 2-Sylowgruppe $H := \langle (1,2,3,4),\ (1,3) \rangle$ von S_4, hat also Ordnung 8; cf. Beispiel 16. Insbesondere ist $|\mathrm{D}_8| \geqslant 8$.

Zusammengenommen ist also $|\mathrm{D}_8| = 8$.

Es folgt, daß $\check{f}|^H : \mathrm{D}_8 \longrightarrow H$ ein Gruppenisomorphismus ist.

Es ergibt sich auch, daß in D_8 aus $a^i b^j = a^{\tilde{i}} b^{\tilde{j}}$ mit $i,\ \tilde{i} \in [0,3]$ und $j,\ \tilde{j} \in [0,1]$ folgt, daß $i = \tilde{i}$ und $j = \tilde{j}$.

Es heißt D_8 auch die *Diedergruppe* von Ordnung 8.

> Im allgemeinen kann man von einer präsentierten Gruppe die Ordnung nicht bestimmen. Noch nicht einmal das *Wortproblem,* zu entscheiden, ob ein gegebenes Element einer präsentierten Gruppe gleich 1 ist, ist allgemein lösbar.

Beispiel 26 Sei

$$\begin{array}{rcl} \{a,b\} & \xrightarrow{u} & \mathrm{D}_8 \\ a & \longmapsto & a \\ b & \longmapsto & ab\ . \end{array}$$

Betrachten wir $\hat{u} : \mathrm{F}(\{a,b\}) \longrightarrow \mathrm{D}_8$, so wird

$$\begin{array}{lllllll} \hat{u}(a^4) & = & u(a)^4 & = & a^4 & = & 1 \\ \hat{u}(b^2) & = & u(b)^2 & = & (ab)^2 & = & abab \ = \ aa^3bb \ = \ 1 \\ \hat{u}((ba)^2) & = & (u(b)u(a))^2 & = & (aba)^2 & = & abaaba \ = \ aa^3a^3bba \ = \ 1\ . \end{array}$$

Also ist Satz 24 anwendbar, und wir erhalten einen Gruppenmorphismus

$$\begin{array}{rcl} \mathrm{D}_8 & \xrightarrow{\check{u}} & \mathrm{D}_8 \\ a & \longmapsto & a \\ b & \longmapsto & ab\ . \end{array}$$

Da $\mathrm{D}_8 = \langle a,b \rangle = \langle a, ab \rangle$ ist, ist $\check{u}$ surjektiv. Da eine Selbstabbildung einer endlichen Menge vorliegt, ist $\check{u}$ bijektiv, also ein Gruppenisomorphismus von D_8 nach D_8, auch Automorphismus von D_8 genannt.

Automorphismen, die durch Konjugation mit einem Gruppenelement entstehen, heißen inner. Nun wird aber ${}^{a^i b^j}b = {}^{a^i}b = a^i b a^{-i} = a^{2i} b \neq ab$ für alle $i \in [0,3]$ und $j \in [0,1]$. Also ist $\check{u}$ nicht inner.

Beispiel 27 Sei $n \geqslant 1$. Setze

$$\mathrm{S}_{\mathrm{P},n} := \left\langle s_1, \ldots, s_{n-1} \;:\; \begin{array}{ll} s_i^2 & \text{für } i \in [1, n-1] \\ (s_i s_{i+1})^3 & \text{für } i \in [1, n-2] \\ (s_i s_j)^2 & \text{für } i,\, j \in [1, n-1] \text{ mit } |i-j| \geqslant 2 \end{array} \right\rangle$$

Es ist

$$\begin{array}{rcll} \mathrm{S}_{\mathrm{P},n} & \xrightarrow{\sim} & \mathrm{S}_n & \\ s_i & \longmapsto & (i, i+1) & \text{für } i \in [1, n-1]\,. \end{array}$$

Dies verifizieren wir in Aufgabe 9.

1.4 Auflösbar, überauflösbar, nilpotent

Sei G eine endliche Gruppe.

Definition 28 Sei

$$\begin{array}{rcl} \mathrm{Z}(G) & := & \{\, z \in G \,:\, zg = gz \text{ für } g \in G\} \\ & = & \{\, z \in G \,:\, z = {}^g z \text{ für } g \in G\} \\ & = & \{\, z \in G \,:\, g = {}^z g \text{ für } g \in G\} \end{array}$$

das *Zentrum* von G.

Es ist $\mathrm{Z}(G) \leqslant G$, da für $z,\, w \in \mathrm{Z}(G)$ und $g \in G$ gilt, daß ${}^g(z^- w) = ({}^g z)^- {}^g w = z^- w$ und also $z^- w \in \mathrm{Z}(G)$; und da $1 \in \mathrm{Z}(G)$.

Es ist $\mathrm{Z}(G) \trianglelefteq G$, da jedes Element $\mathrm{Z}(G)$ unter Konjugation mit G sogar fest bleibt.

Es ist $\mathrm{Z}(G)$ abelsch.

Cf. Aufgabe 6.

Beispiel 29 Sei $n \in \mathbf{Z}_{\geqslant 3}$. Es ist $\mathrm{Z}(\mathrm{S}_n) = 1$. Denn sei $\sigma \in \mathrm{Z}(\mathrm{S}_n)$. Dann wird $(1, 2, \ldots, n)$ von $\sigma \in \mathrm{S}_n$ auf sich konjugiert. Ist also $\sigma(1) = k$ für ein $k \in [1, n]$, dann ist $\sigma(i) = \overline{i + k - 1}$, wobei für $t \in \mathbf{Z}$ gelte, daß $t =: \overline{t} + n \cdot \underline{t}$ mit $\overline{t} \in [1, n]$ und $\underline{t} \in \mathbf{Z}$. Es folgt $\sigma = (1, 2, \ldots, n)^{k-1}$. Sodann impliziert $(1, 2) = {}^{\sigma}(1, 2) = {}^{(1,2,\ldots,n)^{k-1}}(1, 2) = (k, \overline{k+1})$ und $n \geqslant 3$, daß $k = 1$.

Definition 30

(1) Gibt es ein $n \in \mathbf{Z}_{\geqslant 0}$ und eine Kette

$$1 \;=\; G_n \;\trianglelefteq\; G_{n-1} \;\trianglelefteq\; G_{n-2} \;\trianglelefteq\; \cdots \;\trianglelefteq\; G_1 \;\trianglelefteq\; G_0 \;=\; G$$

mit G_i / G_{i+1} abelsch für $i \in [0, n-1]$, dann heißt G *auflösbar*.

Eine solche Kette heißt dann *auflösende Kette* von G.

(2) Gibt es ein $n \in \mathbf{Z}_{\geqslant 0}$ und eine Kette

$$1 \;=\; G_n \;\trianglelefteqslant\; G_{n-1} \;\trianglelefteqslant\; G_{n-2} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; G_1 \;\trianglelefteqslant\; G_0 \;=\; G$$

mit G_i/G_{i+1} zyklisch für $i \in [0, n-1]$ und $G_i \trianglelefteqslant G$ für $i \in [0, n]$, dann heißt G *überauflösbar.*

Eine solche Kette heißt dann *überauflösende Kette* von G.

(3) Gibt es ein $n \in \mathbf{Z}_{\geqslant 0}$ und eine Kette

$$1 \;=\; G_n \;\trianglelefteqslant\; G_{n-1} \;\trianglelefteqslant\; G_{n-2} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; G_1 \;\trianglelefteqslant\; G_0 \;=\; G$$

mit $G_i \trianglelefteqslant G$ für $i \in [0, n]$ und $G_i/G_{i+1} \leqslant \mathrm{Z}(G/G_{i+1})$ für $i \in [0, n-1]$, dann heißt G *nilpotent.*

Eine solche Kette heißt dann *nilpotent auflösende Kette* von G.

Man nennt G_i/G_{i+1} auch den i-ten *Subfaktor* der jeweiligen Kette.

Bemerkung 31 *Wir haben die Implikationen*

$$G \text{ nilpotent} \quad \Longrightarrow \quad G \text{ überauflösbar} \quad \Longrightarrow \quad G \text{ auflösbar .}$$

Beweis. Zu zeigen ist nur, daß G überauflösbar ist, falls G nilpotent ist.

Sei also ein $n \in \mathbf{Z}_{\geqslant 0}$ und eine nilpotent auflösende Kette

$$1 \;=\; G_n \;\trianglelefteqslant\; G_{n-1} \;\trianglelefteqslant\; G_{n-2} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; G_1 \;\trianglelefteqslant\; G_0 \;=\; G$$

gegeben; i.e. sei $G_i \trianglelefteqslant G$ für $i \in [0, n]$ und $G_{i-1}/G_i \leqslant \mathrm{Z}(G/G_i)$ für $i \in [1, n]$.

Wir wollen mit Induktion zeigen, daß G/G_i überauflösbar ist für $i \in [0, n]$. Dies trifft für $i = 0$ zu. Sei $i \in [1, n]$ und sei G/G_{i-1} überauflösbar. Wir haben G/G_i als überauflösbar nachzuweisen.

Da $G_{i-1}/G_i \leqslant \mathrm{Z}(G/G_i)$ und da $G/G_{i-1} \simeq (G/G_i)/(G_{i-1}/G_i)$, folgt dies mit Aufgabe 12.(4).

Insbesondere ist nun $G \simeq G/G_n$ als überauflösbar nachgewiesen. ▫

Bemerkung 32 *Sei H eine Gruppe.*

Setze $UV := \{\, uv \,:\, u \in U,\, v \in V \,\} \subseteq H$ für $U, V \leqslant H$.

Seien nun $N \trianglelefteqslant H$ und $U \leqslant H$ gegeben.

Es ist $UN = NU \leqslant H$.

Wir haben den Gruppenisomorphismus

$$\begin{array}{rcl} U/(U \cap N) & \xrightarrow{\sim} & (UN)/N \\ u(U \cap N) & \longmapsto & uN\,. \end{array}$$

Falls H endlich ist, ist insbesondere $|UN| = \frac{|U||N|}{|U\cap N|}$.

Ist schließlich zudem $U \trianglelefteq H$, so ist $UN \trianglelefteq H$.

Beweis. Zur Untergruppeneigenschaft. Es ist $1 \in UN$. Sind $n, \tilde{n} \in N$ und $u, \tilde{u} \in U$, so wird

$$(nu)(\tilde{n}\tilde{u})^- \;=\; nu\tilde{u}^-\tilde{n}^- \;=\; n({}^{u\tilde{u}^-}\tilde{n})^-u\tilde{u}^- \;\in\; NU\;.$$

Ferner ist $nu = u({}^{u^-}n) \in UN$, also $NU \leqslant UN$. Genauso ist $NU \geqslant UN$. Also ist $NU = UN$.

Zur Isomorphie. Die angegebene Abbildung ist wohldefiniert und injektiv, da für $u \in U$ genau dann $u \in U \cap N$ ist, wenn $u \in N$ ist. Nach Konstruktion ist sie surjektiv und ein Gruppenmorphismus.

Ist zudem $U \trianglelefteq H$, so ist ${}^h(un) = {}^hu\,{}^hn \in UN$ für $u \in U$, $n \in N$ und $h \in H$. ▫

Beispiel 33

(1) Ist G abelsch, so ist G nilpotent, wie die nilpotent auflösende Kette $1 \trianglelefteq G$ zeigt.

(2) Sei p eine Primzahl. Ist G eine p-Gruppe, so ist G nilpotent, wie wir mit Induktion über $|G|$ begründen wollen. Ist $|G| = 1$, so ist nichts zu zeigen. Sei $|G| > 1$. Dann ist $\mathrm{Z}(G) \neq 1$; cf. Aufgabe 6.(1). Nach Induktion ist $G/\mathrm{Z}(G)$ nilpotent. Also ist G nilpotent; cf. Aufgabe 12.(7).

(3) Es hat S_3 die Normalteiler S_3, A_3 und 1; und nur diese.

Es ist S_3 überauflösbar, da $\mathrm{S}_3/\mathrm{A}_3 \simeq \mathrm{C}_2$ und $\mathrm{A}_3 \simeq \mathrm{C}_3$.

Es ist S_3 nicht nilpotent, da diesenfalls der letzte nichttriviale Subfaktor im Zentrum liegen müßte, aber $\mathrm{Z}(\mathrm{S}_3) = \{\mathrm{id}\}$ gilt; cf. Beispiel 29.

(4) Es hat S_4 die Normalteiler S_4, A_4, $\mathrm{V}_4 := \langle (1,2)(3,4), (1,3)(2,4)\rangle$ und 1; und nur diese. Insbesondere ist

$$1 \;\trianglelefteq\; \mathrm{V}_4 \;\trianglelefteq\; \mathrm{A}_4 \;\trianglelefteq\; \mathrm{S}_4\;.$$

Es ist S_4 auflösbar, da $\mathrm{S}_4/\mathrm{A}_4 \simeq \mathrm{C}_2$, $\mathrm{A}_4/\mathrm{V}_4 \simeq \mathrm{C}_3$ und $\mathrm{V}_4 \simeq \mathrm{C}_2 \times \mathrm{C}_2$.

Es ist S_4 nicht überauflösbar, da V_4 nicht zyklisch ist, und wir also keine Kette von Normalteilern der S_4 finden können, deren letzter Subfaktor zyklisch ist.

(5) Sei $n \geqslant 5$. Es hat S_n die Normalteiler S_n, A_n und 1; und nur diese. Denn ist $1 < N \lhd \mathrm{S}_n$, so ist $N \cap \mathrm{A}_n \trianglelefteq \mathrm{A}_n$, also $N \cap \mathrm{A}_n = 1$ oder $N \cap \mathrm{A}_n = \mathrm{A}_n$; cf. Aufgabe 11.(2). Letzterenfalls folgt aus $\mathrm{A}_n \leqslant N < \mathrm{S}_n$, daß $N = \mathrm{A}_n$. Ersterenfalls folgt aus $N \simeq N/(N \cap \mathrm{A}_n) \simeq (N\mathrm{A}_n)/\mathrm{A}_n$, daß $|N| = 2$ und also $N \leqslant \mathrm{Z}(\mathrm{S}_n) = 1$; dieser Widerspruch zeigt, daß dieser Fall nicht eintritt. Cf. Bemerkung 32; Beispiel 29.

Es ist A_n nicht auflösbar, da A_n einfach und nichtabelsch ist, ersteres dank Aufgabe 11.(2), letzteres e.g. wegen $(1,2,3) \circ (2,3,4) = (1,2)(3,4) \neq (1,3)(2,4) = (2,3,4) \circ (1,2,3)$. Da $\mathrm{A}_n \leqslant \mathrm{S}_n$ ist, impliziert A_n nicht auflösbar, daß S_n nicht auflösbar ist; cf. Aufgabe 12.(2).

Definition 34 Sei I eine Menge. Sei für $i \in I$ eine Gruppe H_i gegeben. Sei auf dem cartesischen Produkt

$$\prod_{i\in I} H_i \;=\; \{\, (x_i)_i \,:\, x_i \in H_i \text{ für } i \in I \,\}$$

eine Multiplikation durch

$$(x_i)_i \cdot (y_i)_i \;:=\; (x_i \cdot y_i)_i$$

erklärt, wobei $(x_i)_i\,,\ (y_i)_i \;\in\; \prod_{i\in I} H_i$. Mit dieser Multiplikation wird $\prod_{i\in I} H_i$ zu einer Gruppe, dem *(äußeren) direkten Produkt* von $(H_i)_{i\in I}$.

Dabei ist $1_{\prod_i H_i} = (1_{H_i})_i$ und $((x_i)_i)^- = (x_i^-)_i$ für $(x_i)_i \in \prod_i H_i$.

Ist $I = [1,k]$ für ein $k \in \mathbf{Z}_{\geqslant 0}$, so schreiben wir auch $\prod_{i\in[i,k]} H_i =: H_1 \times \cdots \times H_k$.

Bemerkung 35 *Sei H eine Gruppe. Sei $k \in \mathbf{Z}_{\geqslant 0}$.*

Seien $N_i \trianglelefteq H$ für $i \in [1,k]$ so gegeben, daß

$$H \;=\; N_1 N_2 \cdots N_k$$

und daß

$$N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_k) \;=\; 1 \qquad \text{für } i \in [1,k]\,.$$

Dann haben wir den Gruppenisomorphismus

$$\begin{array}{ccc} \prod_i N_i & \xrightarrow[\sim]{f} & H \\ (n_i)_i & \longmapsto & n_1 n_2 \cdots n_k \end{array}$$

Man sagt auch, H sei ein (inneres) direktes Produkt *von $(N_i)_i$.*

Beweis. Seien $i,\ j \;\in\; [1,k]$ mit $i \neq j$ gegeben. Sei $n_i \in N_i$ und $n_j \in N_j$. Es ist $n_i n_j n_i^- n_j^- \in N_i \cap N_j = 1$, und also $n_i n_j = n_j n_i$. Somit ist f ein Gruppenmorphismus.

Nach Voraussetzung ist f surjektiv.

Zeigen wir, daß f injektiv ist. Sei $(n_i)_i \in \prod_i N_i$ mit $1 = f((n_i)_i) = n_1 n_2 \cdots n_k$ gegeben.

Dann ist $n_1 \in N_1 \cap (N_2 \cdots N_k) = 1$, also $n_1 = 1$ und $1 = n_2 n_3 \cdots n_k$.

Dann ist $n_2 \in N_2 \cap (N_3 \cdots N_k) = 1$, also $n_2 = 1$ und $1 = n_3 n_4 \cdots n_k$.

Usf.

Es folgt $(n_i)_i = (1_{N_i})_i$. Dies zeigt die Injektivität von f. ▫

Dem Beweis von Bemerkung 35 kann man entnehmen, daß die asymmetrische Bedingung, stets $N_i \cap (N_{i+1} \cdots N_k) \;=\; 1$ zu haben, genügt hätte.

Lemma 36 *Sei G weiterhin eine endliche Gruppe. Sei p eine Primzahl. Sei $H \trianglelefteq G$. Sei $H \leqslant K \leqslant G$ so, daß K/H eine p-Sylowgruppe von G/H ist.*

(1) *Es gibt eine p-Sylowgruppe $Q \leqslant G$ mit $QH = K$.*

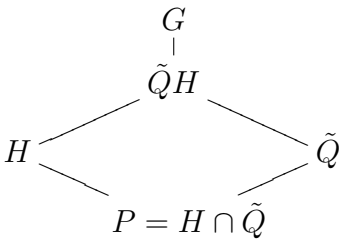
(2) *Ist $\tilde{Q} \leqslant G$ eine p-Sylowgruppe, so ist $(\tilde{Q}H)/H \leqslant G/H$ eine p-Sylowgruppe.*

(3) *Ist $H \leqslant \mathrm{Z}(G)$, dann gibt es genau eine p-Sylowgruppe $Q \leqslant G$ mit $QH = K$.*

(4) *Ist $H \leqslant \mathrm{Z}(G)$ und hat G/H nur eine p-Sylowgruppe, dann hat auch G nur eine p-Sylowgruppe.*

Beweis.

Zu (1). Sei $P \leqslant H$ eine p-Sylowgruppe. Sei $\tilde{Q} \leqslant G$ eine p-Sylowgruppe mit $P \leqslant \tilde{Q} \leqslant G$; cf. Satz 15.(1). Es ist $P \leqslant \tilde{Q} \cap H$ und also $P = \tilde{Q} \cap H$, da $\tilde{Q} \cap H$ eine p-Untergruppe von H ist.



Ein Vergleich der Ordnungen zeigt, daß $\tilde{Q}H/H \overset{\text{B.32}}{\simeq} \tilde{Q}/(\tilde{Q}\cap H) = \tilde{Q}/P$ eine p-Sylowgruppe von G/H ist. Also gibt es ein $x \in G$ mit

$$K/H = {}^{xH}(\tilde{Q}H/H) = (xH)(\tilde{Q}H/H)(x^{-}H) = (x\tilde{Q}Hx^{-})/H = {}^{x}(\tilde{Q}H)/H = ({}^{x}\tilde{Q}\,{}^{x}H)/H = ({}^{x}\tilde{Q}\,H)/H\ ;$$

cf. Satz 15.(2). Es folgt ${}^{x}\tilde{Q}\,H = K$, sodaß $Q := {}^{x}\tilde{Q}$ eine p-Sylowgruppe von G wie gesucht ist.

Zu (2). Sei $Q \leqslant G$ eine p-Sylowgruppe mit $QH/H = K/H$; cf. (1). Dann gibt es ein $x \in G$ mit $\tilde{Q} = {}^{x}Q$; cf. Satz 15.(2). Es wird

$$(\tilde{Q}H)/H = ({}^{x}QH)/H = (xQHx^{-})/H = (xH)(QH/H)(x^{-}H) = (xH)(K/H)(x^{-}H)$$

ebenfalls eine p-Sylowgruppe von G/H.

Zu (3). Dank (1) bleibt nur die Eindeutigkeit zu zeigen. Seien Q und $\tilde{Q}$ zwei p-Sylowgruppen von G mit $QH = K = \tilde{Q}H$. Es sind Q und $\tilde{Q}$ auch p-Sylowgruppen von K. Also gibt es ein $x \in K$ mit ${}^{x}\tilde{Q} = Q$. Schreibe $x = \tilde{q}h$ mit $\tilde{q} \in \tilde{Q}$ und $h \in H$. Es wird

$$Q = {}^{x}\tilde{Q} = {}^{\tilde{q}h}\tilde{Q} \overset{H \leqslant \mathrm{Z}(G)}{=} {}^{\tilde{q}}\tilde{Q} = \tilde{Q}\,.$$

Zu (4). Seien $Q, \tilde{Q} \leqslant G$ zwei p-Sylowgruppen. Wir haben zu zeigen, daß $Q \overset{!}{=} \tilde{Q}$. Es sind $(QH)/H$ und $(\tilde{Q}H)/H$ beides p-Sylowgruppen von G/H; cf. (2). Da G/H nur eine

p-Sylowgruppe hat, folgt $(QH)/H = K/H = (\tilde{Q}H)/H$. Also ist $QH = K = \tilde{Q}H$. Dank (3) folgt schließlich $Q = \tilde{Q}$. ▫

Satz 37 (Sylowzerlegung nilpotenter Gruppen)
Weiterhin sei G eine endliche Gruppe. Sei $\pi(G)$ die Menge der Primteiler von $|G|$.

Für alle $p \in \pi(G)$ wählen wir eine p-Sylowgruppe $Q_p \leqslant G$.

Es ist

$$G \text{ nilpotent} \qquad \Longleftrightarrow \qquad G \simeq \prod_{p\in\pi(G)} Q_p \,.$$

Kurz, G ist genau dann nilpotent, wenn G direktes Produkt seiner Sylowgruppen ist.

Beweis.

Zu $\Leftarrow$. Als p-Gruppe ist Q_p nilpotent für alle Primteiler p von $|G|$; cf. Beispiel 33.(2). Ferner ist ein direktes Produkt nilpotenter Gruppen nilpotent, da eine nilpotent auflösende Kette als direktes Produkt der vorliegenden nilpotent auflösenden Ketten der direkten Faktoren gebildet werden kann. Also ist G isomorph zu einer nilpotenten Gruppe, mithin selbst nilpotent.

Zu $\Rightarrow$. Sei ein $n \in \mathbf{Z}_{\geqslant 0}$ und eine nilpotent auflösende Kette

$$1 = G_n \trianglelefteqslant G_{n-1} \trianglelefteqslant G_{n-2} \trianglelefteqslant \cdots \trianglelefteqslant G_1 \trianglelefteqslant G_0 = G$$

gegeben; i.e. sei $G_i \trianglelefteqslant G$ für $i \in [0,n]$ und $G_i/G_{i+1} \leqslant \mathrm{Z}(G/G_{i+1})$ für $i \in [0,n-1]$.

Sei p eine Primzahl. Wir wollen mit Induktion zeigen, daß G/G_i genau eine p-Sylowgruppe hat für $i \in [0,n]$. Dies trifft für $i = 0$ zu. Sei $i \in [1,n]$ und habe G/G_{i-1} genau eine p-Sylowgruppe. Wir haben zu zeigen, daß G/G_i genau eine p-Sylowgruppe hat.

Da $G_{i-1}/G_i \leqslant \mathrm{Z}(G/G_i)$ und $(G/G_i)/(G_{i-1}/G_i) \simeq G/G_{i-1}$, folgt dies mit Lemma 36.(4).

Der Fall $i = n$ zeigt nun insbesondere, daß Q_p die einzige p-Sylowgruppe von G ist für $p \in \pi(G)$. Also ist $Q_p \trianglelefteqslant G$ für $p \in \pi(G)$; cf. Aufgabe 7.(1).

Sortiere $\pi(G) = \{p_1, \ldots, p_\ell\}$, wobei $\ell \in \mathbf{Z}_{\geqslant 0}$ und $p_i \neq p_j$ für $i, j \in [1,\ell]$ mit $i \neq j$. Schreibe kurz $Q_i := Q_{p_i}$ für $i \in [1,\ell]$.

Für $i \in [1,\ell]$ ist $|Q_1 \cdots Q_{i-1}Q_{i+1} \cdots Q_\ell|$ ein Teiler von $|Q_1 \cdots Q_{i-1}Q_{i+1} \cdots Q_{\ell-1}||Q_\ell|$, dies ist ein Teiler von $|Q_1 \cdots Q_{i-1}Q_{i+1} \cdots Q_{\ell-2}||Q_{\ell-1}||Q_\ell|$, usf.; cf. Bemerkung 32. Insgesamt ist $|Q_1 \cdots Q_{i-1}Q_{i+1} \cdots Q_\ell|$ also ein Teiler von $|Q_1| \cdots |Q_{i-1}||Q_{i+1}| \cdots |Q_\ell|$. Daher ist $|Q_i|$ teilerfremd zu $|Q_1 \cdots Q_{i-1}Q_{i+1} \cdots Q_\ell|$. Folglich ist

$$Q_i \cap (Q_1 \cdots Q_{i-1}Q_{i+1} \cdots Q_\ell) = 1 \,.$$

Ferner ist

$$\begin{aligned}
|Q_1 \cdots Q_\ell| &\overset{\text{B. 32}}{=} \tfrac{|Q_1 \cdots Q_{\ell-1}||Q_\ell|}{|(Q_1 \cdots Q_{\ell-1}) \cap Q_\ell|} \\
&= |Q_1 \cdots Q_{\ell-1}||Q_\ell| \\
&\overset{\text{B. 32}}{=} \tfrac{|Q_1 \cdots Q_{\ell-2}||Q_{\ell-1}|}{|(Q_1 \cdots Q_{\ell-2}) \cap Q_{\ell-1}|} |Q_\ell| \\
&= |Q_1 \cdots Q_{\ell-2}||Q_{\ell-1}||Q_\ell| \\
&= \cdots \\
&= |Q_1| \cdots |Q_\ell| \\
&= |G| \ ,
\end{aligned}$$

i.e. $Q_1 \cdots Q_\ell = G$.

Nun können wir Bemerkung 35 anwenden und erhalten den Gruppenisomorphismus

$$\begin{array}{rcl}
\prod_{i \in [1,\ell]} Q_i & \xrightarrow[\sim]{f} & G \\
(q_i)_i & \longmapsto & q_1 q_2 \cdots q_k \ .
\end{array}$$

□

Kapitel 2

Darstellungen und Moduln

Die Begriffe eines (Links-)Moduls über einem Ring A, der A-linearen Abbildungen zwischen A-Moduln, sowie der Teil- und der Faktormoduln von A-Moduln werden als bekannt vorausgesetzt.

Ist A ein Körper, so ist ein A-Modul dasselbe wie ein A-Vektorraum.

Sei G eine Gruppe.

Sei R ein kommutativer Ring mit $R \neq 0$.

Für einen R-Modul V schreiben wir $\mathrm{GL}(V)$ für die Gruppe der bijektiven R-linearen Abbildungen von V nach V, mit der Komposition als Multiplikation. Ferner werde $\mathrm{GL}(R^{n\times 1})$ mit $\mathrm{GL}_n(R)$ via der Standardbasis von R^n identifiziert, wobei $n \geqslant 0$.

2.1 Darstellungen

Definition 38 Eine *Darstellung* (V, ρ) von G (über R) besteht aus einem R-Modul V und einem Gruppenmorphismus $\rho : G \longrightarrow \mathrm{GL}(V)$.

Man spricht auch von einer Darstellung ρ von G auf V (über R).

Man kann auch G-Mengen als bestehend aus einer Menge M und einem Gruppenmorphismus $G \to \mathrm{S}_M$ auffassen; cf. Aufgabe 8.(2).

Beispiel 39

(1) Es gibt die *triviale* Darstellung $G \longrightarrow \mathrm{GL}_1(R)$, $g \longmapsto (1)$ auf R über R.

(2) Sei $n \in \mathbf{Z}_{\geqslant 1}$. Sei $G = \mathrm{C}_n := \langle\, a \,:\, a^n \,\rangle$ die zyklische Gruppe von Ordnung n.
Sei $k \in [0, n-1]$. Da $\zeta_n^n = 1$, gibt es die Darstellung $\mathrm{C}_n \longrightarrow \mathrm{GL}_1(\mathbf{C})$, $a \longmapsto (\zeta_n^k)$ über $\mathbf{C}$.

(3) Sei $n \in \mathbf{Z}_{\geqslant 0}$. Sei $G = \mathrm{S}_n$.

Es gibt, wie stets, die triviale Darstellung $\mathrm{S}_n \longrightarrow \mathrm{GL}_1(R)$, $\sigma \longmapsto (1)$ über R.

Ferner gibt es die Signumsdarstellung $\mathrm{S}_n \longrightarrow \mathrm{GL}_1(R)$, $\sigma \longmapsto (\operatorname{sgn}\sigma)$ über R.

In der Tat ist $\operatorname{sgn}(\sigma \circ \tau) = (\operatorname{sgn}\sigma) \cdot (\operatorname{sgn}\tau)$ für $\sigma, \tau \in \mathrm{S}_n$.

(4) Es definiert

$$\begin{array}{rcl} \mathrm{S}_3 & \longrightarrow & \mathrm{GL}_2(\mathbf{Z}) \\ (1,2) & \longmapsto & \left(\begin{smallmatrix} -2 & -1 \\ 3 & 2 \end{smallmatrix}\right) \\ (2,3) & \longmapsto & \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right) \end{array}$$

eine Darstellung von S_3 auf $\mathbf{Z}^{2\times 1}$ über $\mathbf{Z}$; cf. Aufgabe 14.

Der Ring $\mathbf{Z}$ kann hierin auch durch $\mathbf{Q}$ oder $\mathbf{C}$ ersetzt werden.

Definition 40 (und Bemerkung)
Sei M eine endliche G-Menge. Sei

$$RM \;:=\; \{\, \textstyle\sum_{m\in M} r_m\, m \;:\; r_m \in R \text{ für } m \in M \,\}$$

der freie R-Modul mit R-linearer Basis M [1].

Wir haben eine injektive Abbildung $M \longrightarrow RM$, $m \longmapsto \sum_{n\in M} \partial_{n,m}\, n$, welche wir zur Identifikation verwenden und so M als Teilmenge von RM betrachten, insbesondere also $m = \sum_{n\in M} \partial_{n,m}\, n$ schreiben.

Es definiert

$$\begin{array}{rcl} G & \xrightarrow{\rho_{RM}} & \mathrm{GL}(RM) \\ g & \longmapsto & (m \mapsto gm) \end{array}$$

eine Darstellung von G auf RM über R.

Es ist dann $\rho_{RM}(g)(\sum_{m\in M} r_m\, m) = \sum_{m\in M} r_m\, gm$.

Eine solche Darstellung heißt *Permutationsdarstellung.* Denn wenn man $\mathrm{GL}(RM)$ mit $\mathrm{GL}_{|M|}(R)$ identifiziert vermöge der Basis M von RM, so wird jedes Gruppenelement auf eine Permutationsmatrix in $\mathrm{GL}_{|M|}(R)$ abgebildet.

Beweis. Es ist $\rho_{RM}(g)$ eine R-lineare bijektive Abbildung von RM nach RM, induziert von der bijektiven Abbildung $M \longrightarrow M$, $m \longmapsto gm$ der Basis M auf sich.

Seien $g, \tilde{g} \in G$ gegeben. Es ist

$$(\rho_{RM}(g\tilde{g}))(m) \;=\; (g\tilde{g})(m) \;=\; g(\tilde{g}m) \;=\; (\rho_{RM}(g) \circ \rho_{RM}(\tilde{g}))(m)$$

für $m \in M$. Da also $\rho_{RM}(g\tilde{g})$ und $\rho_{RM}(g) \circ \rho_{RM}(\tilde{g})$ auf einer Basis übereinstimmende R-lineare Abbildungen sind, sind sie gleich. ▫

[1] Formal gesprochen sind die Elemente von RM Abbildungen von M nach R, i.e. $\sum_{m\in M} r_m\, m$ ist nur eine symbolische Schreibweise für die Abbildung $M \to R$, $m \mapsto r_m$.

Beispiel 41 Wir haben die S_3-Menge $\{1,2,3\}$; cf. Beispiel 2.(2). Die zugehörige Permutationsdarstellung wird, nach Identifikation von $\mathrm{GL}(R\{1,2,3\})$ mit $\mathrm{GL}_3(R)$ vermöge der R-linearen Basis $\{1,2,3\}$, zu

$$\begin{array}{rcl} \mathrm{S}_3 & \overset{\rho_{R\{1,2,3\}}}{\longrightarrow} & \mathrm{GL}_3(R) \\ (1,2) & \longmapsto & \left(\begin{smallmatrix} 0&1&0 \\ 1&0&0 \\ 0&0&1 \end{smallmatrix}\right) \\ (2,3) & \longmapsto & \left(\begin{smallmatrix} 1&0&0 \\ 0&0&1 \\ 0&1&0 \end{smallmatrix}\right) . \end{array}$$

2.2 Gruppenringe

Sei die Gruppe G nun als endlich vorausgesetzt.

Definition 42 (und Bemerkung) Sei

$$RG \;:=\; \{\, \textstyle\sum_{g\in G} r_g\, g \;:\; r_g \in R \text{ für } g \in G \,\}$$

der freie R-Modul mit Basis G, bestehend aus formalen R-Linearkombinationen in G ([2]). Insbesondere können wir Elemente aus RG addieren und mit Elementen aus R multiplizieren.

Wir haben eine injektive Abbildung $G \longrightarrow RG$, $h \longmapsto \sum_g \partial_{g,h}\, g$, welche wir zur Identifikation verwenden und so G als Teilmenge von RG betrachten. Wir schreiben also $h = \sum_{g\in G} \partial_{g,h}\, g$ für $h \in G$.

Wir haben eine injektive Abbildung $R \longrightarrow RG$, $r \longmapsto r1_G$, welche wir zur Identifikation verwenden und so R als Teilmenge von RG betrachten. Wir schreiben also $r = r1_G$ für $r \in R$.

Wir definieren eine R-bilineare Multiplikationsabbildung auf $RG \times RG$ durch Angabe der Abbildungsvorschrift auf der Basis G in beiden Einträgen, nämlich als

$$\begin{array}{rcccl} RG & \times & RG & \longrightarrow & RG \\ (g & , & h) & \longmapsto & g \underset{RG}{\cdot} h \;=\; g \cdot h \;=\; gh \;:=\; g \underset{G}{\cdot} h\,, \end{array}$$

wobei $g,\, h \in G$. Somit wird

$$\left(\sum_{g\in G} r_g\, g\right) \underset{RG}{\cdot} \left(\sum_{h\in G} s_h\, h\right) \;=\; \sum_{(g,h)\in G\times G} r_g s_h\; g \underset{G}{\cdot} h \;\overset{x\,:=\,gh}{=}\; \sum_{x\in G} \left(\sum_{g\in G} r_g s_{g^-x}\right) x\,,$$

wobei $r_g\,,\; s_g \;\in\; R$ für $g \in G$.

[2]Formal gesprochen sind die Elemente von RG Abbildungen von G nach R, i.e. $\sum_{g\in G} r_g\, g$ ist nur eine symbolische Schreibweise für die Abbildung $G \to R$, $g \mapsto r_g$.

Es ist $RG = (RG, +, \underset{RG}{\cdot})$ ein Ring, genannt der *Gruppenring* von G mit Koeffizienten in R; cf. Aufgabe 15.

Es ist R ein Teilring von RG. Wie zu erwarten, ist

$$g \underset{RG}{\cdot} r \;=\; g \underset{RG}{\cdot} r1_G \;=\; r(g \underset{G}{\cdot} 1_G) \;=\; rg \;=\; r(1_G \underset{G}{\cdot} g) \;=\; r1_G \underset{RG}{\cdot} g \;=\; r \underset{RG}{\cdot} g$$

für $g \in G$ und $r \in R$. Das neutrale Element der Addition ist $0_{RG} = \sum_{g\in G} 0g \in RG$.

Das neutrale Element der Multiplikation ist $1_{RG} = 1_G = \sum_{g\in G} \partial_{g,1}\, g \in RG$.

Beispiel 43 In $\mathbf{Z}\mathrm{S}_3$ ist

$$\begin{array}{lcl}
(\mathrm{id} - 2(1,3,2))(3(1,2,3) + (1,2)) & = & 3(1,2,3) - 6\,\mathrm{id} + (1,2) - 2(2,3) \\
(\mathrm{id} - (1,2,3))(\mathrm{id} + (1,2,3) + (1,3,2)) & = & \mathrm{id} + (1,2,3) + (1,3,2) - (1,2,3) - (1,3,2) - \mathrm{id} \;=\; 0 \\
((1,2,3) - (1,3,2) + (1,2) - (1,3))^2 & = & 0\,.
\end{array}$$

Nennen wir das zuletzt quadrierte Element ξ, so folgt speziell, daß $(\mathrm{id} + \xi)(\mathrm{id} - \xi) = \mathrm{id}$ und $(\mathrm{id} + \xi)^k = \mathrm{id} + k\xi \neq \mathrm{id}$ ist für $k \in \mathbf{Z}_{\geqslant 1}$. Folglich ist $1 + \xi$ ein invertierbares Element in $\mathbf{Z}\mathrm{S}_3$ ohne endliche multiplikative Ordnung.

Lemma 44 (Darstellungen und Moduln)

(1) *Sei (V, ρ) eine Darstellung von G über R. Wir definieren eine R-bilineare Abbildung auf $RG \times V$ durch Angabe der Abbildungsvorschrift auf der Basis im ersten und eines beliebigen Elements im zweiten Eintrag, nämlich*

$$\begin{array}{ccccc}
RG & \times & V & \longrightarrow & V \\
(g & , & v) & \longmapsto & (\rho(g))(v)
\end{array}$$

Da $\rho(g)$ eine R-lineare Abbildung ist, ist diese Abbildung auch in der zweiten Variablen R-linear.

Allgemein ist also $(\sum_{g\in G} r_g\, g)v = \sum_{g\in G} r_g(\rho(g))(v)$, wobei $r_g \in R$ für $g \in G$.

Zusammen mit dieser Multiplikation wird V zu einem RG-Modul.

(2) *Sei V ein RG-Modul. Schränken wir V zu einem R-Modul ein, um $\mathrm{GL}(V)$ zu bilden, und setzen wir*

$$\begin{array}{ccc}
G & \xrightarrow{\rho} & \mathrm{GL}(V) \\
g & \longmapsto & (v \mapsto gv)\,,
\end{array}$$

so ist (V, ρ) eine Darstellung von G über R. Wir schreiben auch $\rho_V := \rho$.

(3) *Ist (V, ρ) eine Darstellung von G über R, bilden wir den zugehörigen RG-Modul via (1) und dann die dazu gehörige Darstellung von G über R via (2), so erhalten wir die ursprüngliche Darstellung zurück.*

Ist umgekehrt V ein RG-Modul, bilden wir die zugehörige Darstellung von G über R via (2) und dann den dazu gehörigen RG-Modul via (1), so erhalten wir den ursprünglichen RG-Modul zurück.

Vermöge Lemma 44 können wir also RG-Moduln und Darstellungen von G über R miteinander identifizieren.

Beweis.

Zu (1). Es ist $1_{RG} \cdot v = 1_G \cdot v = (\rho(1_G))(v) = \mathrm{id}_V(v) = v$.

Es ist

$$\begin{aligned} & (\textstyle\sum_g r_g\, g)((\sum_h s_h\, h)v) \\ = \; & (\textstyle\sum_g r_g\, g)\big(\sum_h s_h(\rho(h))(v)\big) \\ = \; & \textstyle\sum_g r_g\, \rho(g)\big(\sum_h s_h(\rho(h))(v)\big) \\ = \; & \textstyle\sum_g r_g \sum_h s_h(\rho(g) \circ \rho(h))(v) \\ = \; & \textstyle\sum_g r_g \sum_h s_h(\rho(gh))(v) \\ = \; & (\textstyle\sum_{g,h} r_g s_h\, gh)v \\ = \; & ((\textstyle\sum_g r_g\, g)(\sum_h s_h\, h))v\ , \end{aligned}$$

wobei $r_g\,,\ s_g \in R$ für $g \in G$ und $v \in V$.

Es ist

$$\begin{aligned} & ((\textstyle\sum_g r_g\, g) + (\sum_g s_g\, g))(v+w) \\ = \; & (\textstyle\sum_g (r_g + s_g)g)(v+w) \\ = \; & \textstyle\sum_g (r_g + s_g)(\rho(g))(v+w) \\ = \; & \textstyle\sum_g (r_g + s_g)(\rho(g))(v) + \sum_g (r_g + s_g)(\rho(g))(w) \\ = \; & \textstyle\sum_g r_g(\rho(g))(v) + \sum_g s_g(\rho(g))(v) + \sum_g r_g(\rho(g))(w) + \sum_g s_g(\rho(g))(w) \\ = \; & (\textstyle\sum_g r_g\, g)v + (\sum_g s_g\, g)v + (\sum_g r_g\, g)w + (\sum_g s_g\, g)w\ , \end{aligned}$$

wobei $r_g\,,\ s_g \in R$ für $g \in G$ und $v,\ w \in V$.

Zu (2). Es ist $V \to\!\!\!\!\to V,\ v \mapsto\!\!\!\!\to gv$ bijektiv für $g \in G$, da von $V \to\!\!\!\!\to V,\ v \mapsto\!\!\!\!\to g^- v$ beidseitig invertiert. Es ist diese Abbildung auch R-linear, da $g(rv + sw) = g(rv) + g(sw) = (gr)v + (gs)w = (rg)v + (sg)w = r(gv) + s(gw)$ für $r,\ s \in R$ und $v,\ w \in V$.

Es ist ρ ein Gruppenmorphismus, da $(\rho(gh))(v) = (gh)v = g(hv) = (\rho(g) \circ \rho(h))(v)$ für $g,\ h \in G$ und $v \in V$.

Zu (3). Beginnt man mit einer Darstellung (V, ρ), so ist auf dem zugehörigen RG-Modul die Multiplikationsabbildung mit $g \in G$ auf V durch $\rho(g)$ gegeben, was man, geht man wieder zu einer Darstellung über, auch als Bild von g zu nehmen hat.

Beginnt man mit einem RG-Modul V, so ist das Bild von g in $\mathrm{GL}(V)$ unter der zugehörigen Darstellung auf V die Multiplikationsabbildung mit g auf V, sodaß man, geht man wieder zum RG-Modul über, als Produkt von $g \in G$ mit $v \in V$ wieder denselben Wert wie eingangs erhält.

Nach Distributivität eines Moduls ist nun aber $(\sum_g r_g\, g)v = \sum_g r_g(gv)$ für $r_g \in R$ für $g \in G$, und also bestimmt auf V, gesehen als R-Modul, die Einschränkung der Multiplikationsabbildung $(\cdot) : RG \times V \longrightarrow\!\!\!\!\to V$ auf $G \times V$ bereits die ganze Abbildung. ▫

Bemerkung 45
Sei V ein RG-Modul. Sei $\rho_V : G \longrightarrow \mathrm{GL}(V)$ die zugehörige Darstellung auf V.

Sei W ein RG-Modul. Sei $\rho_W : G \longrightarrow \mathrm{GL}(W)$ die zugehörige Darstellung auf W.

Sei $f : V \longrightarrow W$ eine R-lineare Abbildung.

Es ist f genau dann RG-linear, wenn $\rho_W(g) \circ f = f \circ \rho_V(g)$ für $g \in G$.

Insbesondere sind V und W genau dann als RG-Moduln isomorph, wenn es eine R-lineare Bijektion $f : V \longrightarrow W$ gibt mit $\rho_W(g) \circ f = f \circ \rho_V(g)$ für $g \in G$; oder, äquivalent hierzu, mit $\rho_W(g) = f \circ \rho_V(g) \circ f^-$.

Beweis. Da f ohnehin R-linear ist, also mit Summen und mit Faktoren aus R vertauscht, ist f genau dann RG-linear, wenn $f(gv) = gf(v)$ ist für $g \in G$ und $v \in V$, i.e. wenn $(f \circ \rho_V(g))(v) = (\rho_W(g) \circ f)(v)$ ist für $g \in G$ und $v \in V$, i.e. wenn $f \circ \rho_V(g) = \rho_W(g) \circ f$ ist für $g \in G$; cf. Lemma 44. ▫

Definition 46 (und Bemerkung) Sei A ein Ring.

Das *Zentrum* von A ist gegeben durch

$$\mathrm{Z}(A) \;:=\; \{\, z \in A \,:\, \text{es ist } za = az \text{ für } a \in A \,\}\,.$$

Es ist $\mathrm{Z}(A)$ ein kommutativer Teilring von A. Denn $1_A \in \mathrm{Z}(A)$, und aus $z, w \in \mathrm{Z}(A)$ folgt $(z-w)a = a(z-w)$ und $zwa = azw$ für $a \in A$, und somit $z - w,\, zw \in \mathrm{Z}(A)$.

Beispiel 47 Es ist $\mathrm{Z}(R^{n\times n}) = \{\, r \cdot \mathrm{E}_n \,:\, r \in R \,\}$ für $n \in \mathbf{Z}_{\geqslant 0}$; cf. Aufgabe 16.

Bemerkung 48 (Universelle Eigenschaft von RG) *Sei A ein Ring.*

Sei $f : G \longrightarrow \mathrm{U}(A)$ ein Gruppenmorphismus. Sei $\varphi : R \longrightarrow \mathrm{Z}(A)$ ein Ringmorphismus.

Dann gibt es genau einen Ringmorphismus $\hat{f} : RG \longrightarrow A$, der folgendes Diagramm kommutativ macht.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & \mathrm{Z}(A) \\ \downarrow & & \downarrow \\ RG & \overset{\exists!\hat{f}}{\dashrightarrow} & A \\ \uparrow & & \uparrow \\ G & \xrightarrow[f]{} & \mathrm{U}(A) \end{array}$$

Hierbei ist $\hat{f}(\sum_g r_g\, g) \;:=\; \sum_g \varphi(r_g) \cdot f(g)$ für $r_g \in R$ für $g \in G$.

In der Anwendung ist meist φ selbstverständlich gegeben, und f interessant.

Beweis.

Eindeutigkeit. Sei $u : RG \longrightarrow A$ ein Ringmorphismus mit $u(r) = \varphi(r)$ für $r \in R$ und $u(g) = f(g)$ für $g \in G$. Dann wird

$$u(\textstyle\sum_g r_g\, g) \;=\; \sum_g u(r_g) \cdot u(g) \;=\; \sum_g \varphi(r_g) \cdot f(g)\ .$$

Also ist u durch Angaben von φ und f festgelegt.

Existenz. Setze

$$\hat{f}(\textstyle\sum_g r_g\, g) \;:=\; \sum_g \varphi(r_g) \cdot f(g)\ ,$$

wobei $r_g \in R$ für $g \in G$.

Dies ist ein Ringmorphismus. Denn es ist $\hat{f}(1_{RG}) = \hat{f}(1_R \cdot 1_G) = \varphi(1_R) \cdot f(1_G) = 1_A \cdot 1_A = 1_A$; es ist

$$\begin{aligned}&\hat{f}((\textstyle\sum_g r_g\, g) + (\sum_g s_g\, g)) \;=\; \hat{f}(\sum_g (r_g + s_g) g) \;=\; \sum_g \varphi(r_g + s_g) \cdot f(g) \;=\; \sum_g (\varphi(r_g) + \varphi(s_g)) \cdot f(g)\\ &=\; \textstyle\sum_g \varphi(r_g) \cdot f(g) + \sum_g \varphi(s_g) \cdot f(g) \;=\; \hat{f}(\sum_g r_g\, g) + \hat{f}(\sum_g s_g\, g)\ ;\end{aligned}$$

und es ist

$$\begin{aligned}&\hat{f}((\textstyle\sum_g r_g\, g) \cdot (\sum_h s_h\, h)) \;=\; \hat{f}(\sum_x (\sum_g r_g s_{g^{-}x})\, x) \;=\; \sum_x \varphi(\sum_g r_g s_{g^{-}x}) \cdot f(x)\\ &=\; \textstyle\sum_{x,g} \varphi(r_g) \cdot \varphi(s_{g^{-}x}) \cdot f(x) \;=\; \sum_{g,h} \varphi(r_g) \cdot \varphi(s_h) \cdot f(gh) \;=\; \sum_{g,h} \varphi(r_g) \cdot \varphi(s_h) \cdot f(g) \cdot f(h)\\ &=\; \textstyle\sum_{g,h} \varphi(r_g) \cdot f(g) \cdot \varphi(s_h) \cdot f(h) \;=\; (\sum_g \varphi(r_g) \cdot f(g))(\sum_h \varphi(s_h) \cdot f(h))\\ &=\; \hat{f}(\textstyle\sum_g r_g\, g) \cdot \hat{f}(\sum_h s_h\, h)\ ;\end{aligned}$$

wobei $r_g\,,\ s_g \in R$ für $g \in G$.

Schließlich ist $\hat{f}(r) = \hat{f}(r \cdot 1_G) = \varphi(r) \cdot f(1_G) = \varphi(r)$ für $r \in R$ und $\hat{f}(g) = \hat{f}(1_R \cdot g) = \varphi(1_R) \cdot f(g) = f(g)$ für $g \in G$. ▫

Beispiel 49 Sei (V, ρ) eine Darstellung von G über R.

Wir betrachten den Endomorphismenring $\mathrm{End}_R V$ der R-linearen Abbildungen von V nach V; cf. Aufgabe 19.(2).

Wir haben einen Gruppenmorphismus $\rho : G \longrightarrow \mathrm{U}(\mathrm{End}_R V) = \mathrm{GL}(V)$.

Wir haben einen Ringmorphismus $\varphi : R \longrightarrow \mathrm{End}_R V$, $r \longmapsto (r \cdot \mathrm{id}_V : v \mapsto r \cdot v)$.

Also haben wir auch den Ringmorphismus

$$\begin{array}{rcl} RG & \stackrel{\hat{\rho}}{\longrightarrow} & \mathrm{End}_R V \\ \sum_g r_g\, g & \longmapsto & \sum_g \varphi(r_g) \cdot \rho(g)\ , \end{array}$$

wobei $r_g \in R$ für $g \in G$; cf. Bemerkung 48. Hierbei ist also

$$(\hat{\rho}(\textstyle\sum_g r_g\, g))(v) \;=\; (\sum_g \varphi(r_g) \cdot \rho(g))(v) \;=\; \sum_g r_g \cdot (\rho(g))(v) \;=\; (\sum_g r_g\, g)v$$

für $v \in V$, letzteres unter Verwendung der RG-Modulstruktur aus Lemma 44.(1).

Dies ist eine andere Sichtweise auf Lemma 44.(1), denn ein Ringmorphismus von einem Ring in einen Endomorphismenring einer abelschen Gruppe definiert auf dieser eine Modulstruktur über jenem Ring.

Beispiel 50 Sei $n \in \mathbf{Z}_{\geqslant 1}$. Schreibe $\zeta := \zeta_n$.

Wir betrachten die Gruppe $\mathrm{C}_n = \langle a \,:\, a^n \rangle$ und den Ring $\mathbf{C}^{\times n} = \mathbf{C} \times \cdots \times \mathbf{C}$, mit komponentenweiser Addition und Multiplikation. Es ist $\mathrm{U}(\mathbf{C}^{\times n}) = \mathrm{U}(\mathbf{C})^{\times n} = (\mathbf{C} \smallsetminus \{0\})^{\times n}$.

Wir haben den Gruppenmorphismus

$$\begin{array}{rcl} \mathrm{C}_n & \xrightarrow{f} & \mathrm{U}(\mathbf{C}^{\times n}) \\ a & \longmapsto & (\zeta^k)_{k\in[0,n-1]} \;=\; (\zeta^0, \ldots, \zeta^{n-1}) \,; \end{array}$$

cf. Beispiel 39.

Wir betrachten also alle in loc. cit. gefundenen Beispiele von Darstellungen von C_n simultan.

Wir haben den Ringmorphismus

$$\begin{array}{rcl} \mathbf{C} & \xrightarrow{\varphi} & \mathrm{Z}(\mathbf{C}^{\times n}) \;=\; \mathbf{C}^{\times n} \\ z & \longmapsto & (z)_{k\in[0,n-1]} \,. \end{array}$$

Also gibt es den Ringmorphismus

$$\begin{array}{rcl} \mathbf{C}\mathrm{C}_n & \xrightarrow{\hat{f}} & \mathbf{C}^{\times n} \\ \sum_{i\in[0,n-1]} z_i a^i & \longmapsto & \sum_{i\in[0,n-1]} (z_i)_k (\zeta^{k\cdot i})_k \;=\; (\sum_{i\in[0,n-1]} z_i \zeta^{k\cdot i})_k \,; \end{array}$$

cf. Bemerkung 48. Als $\mathbf{C}$-lineare Abbildung gesehen, wird $\hat{f}$ bezüglich der Basis $(a^i)_{i\in[0,n-1]}$ und der Standardbasis von $\mathbf{C}^{\times n}$ durch die Matrix

$$\begin{pmatrix} \zeta^{0\cdot 0} & \zeta^{0\cdot 1} & \zeta^{0\cdot 2} & \ldots & \zeta^{0\cdot(n-1)} \\ \zeta^{1\cdot 0} & \zeta^{1\cdot 1} & \zeta^{1\cdot 2} & \ldots & \zeta^{1\cdot(n-1)} \\ \zeta^{2\cdot 0} & \zeta^{2\cdot 1} & \zeta^{2\cdot 2} & \ldots & \zeta^{2\cdot(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ \zeta^{(n-1)\cdot 0} & \zeta^{(n-1)\cdot 1} & \zeta^{(n-1)\cdot 2} & \ldots & \zeta^{(n-1)\cdot(n-1)} \end{pmatrix}$$

beschrieben. Gemäß Vandermonde ist die Determinante dieser Matrix gegeben durch $\prod_{i,\, j\,\in\,[0,n-1],\; i<j} (\zeta^j - \zeta^i) \neq 0$; cf. auch Aufgabe 17. Also ist $\hat{f}$ bijektiv, und somit ein Ringisomorphismus.

Wir stellen mithin fest, daß $\mathbf{C}\mathrm{C}_n \simeq \mathbf{C}^{\times n}$ als Ringe, wobei die rechte Seite oft handhabbarer ist als die linke.

Im folgenden Abschnitt wollen wir diese Beobachtung von C_n auf beliebige Gruppen ausdehnen. Da für eine nichtabelsche Gruppe G der Gruppenring $\mathrm{C}G$ nichtkommutativ ist, kann auch die rechte Seite des zu konstruierenden Isomorphismus nicht kommutativ sein. Es wird sich herausstellen, daß diese die Gestalt $\prod_i \mathbf{C}^{n_i \times n_i}$ mit $n_i \in \mathbf{Z}_{\geqslant 1}$ hat, wobei in Beispiel 50 eben $n_i = 1$ zu setzen ist; cf. Satz 67 unten; cf. auch Aufgabe 18.

Kapitel 3

Wedderburn

3.1 Peirce

Sei A ein Ring.

Definition 51

(1) Ein Element $e \in A$ heißt *idempotent,* falls $e^2 = e$.

(2) Ein Idempotent $e \in A \setminus \{0\}$ heißt *primitiv,* falls aus $e = e' + e''$ mit e', e'' Idempotenten mit $e'e'' = 0$ und $e''e' = 0$ bereits $e' = 0$ oder $e'' = 0$ folgt.

(3) Sei $n \in \mathbf{Z}_{\geqslant 0}$. Ein Tupel $\underline{e} = (e_1 , \ldots , e_n)$ von Idempotenten von A heißt *orthogonale Zerlegung in Idempotente* (in A), falls $1 = e_1 + \cdots + e_n$ und falls $e_i e_j = 0$ ist für $i, j \in [1, n]$ mit $i \neq j$.

(4) Eine orthogonale Zerlegung in Idempotente $\underline{e} = (e_1 , \ldots , e_n)$ heiße *orthogonale Zerlegung in primitive Idempotente* (in A), falls e_i primitiv ist für $i \in [1, n]$.

Bemerkung 52 *Sei $n \in \mathbf{Z}_{\geqslant 0}$ und $\underline{e} = (e_1 , \ldots , e_n)$ eine orthogonale Zerlegung in Idempotente in A. Sei M ein A-Modul. Als abelsche Gruppen ist*

$$M \;=\; \bigoplus_{i \in [1,n]} e_i M \; .$$

Beweis. Wegen $1 = e_1 + \cdots + e_n$ ist $m = e_1 m + \cdots + e_n m$ für $m \in M$, und also M gleich der Summe der Untergruppen $e_i M$.

Bleibt die Direktheit dieser Summe zu zeigen. Sei also $e_1 m_1 + \cdots + e_n m_n = 0$ mit $m_i \in M$ für $i \in [1, n]$. Es wird $0 \;=\; e_i(e_1 m_1 + \cdots + e_n m_n) \;=\; e_i m_i$ für $i \in [1, m]$. ▫

Lemma 53 (Peirce-Zerlegung) *Sei $n \in \mathbf{Z}_{\geqslant 0}$ und $\underline{e} = (e_1, \ldots, e_n)$ eine orthogonale Zerlegung in Idempotente in A. Als abelsche Gruppen wird*

$$A = \bigoplus_{i,j \in [1,n]} e_i A e_j$$

Beweis. Mit Bemerkung 52 und der dazu analogen Aussage für A-Rechtsmoduln wird

$$A = \bigoplus_{i \in [1,n]} e_i A = \bigoplus_{i \in [1,n]} \Big(\bigoplus_{j \in [1,n]} e_i A e_j \Big) = \bigoplus_{i,j \in [1,n]} e_i A e_j \, .$$

Beispiel 54 Sei K ein Körper. Sei $A = K^{3\times 3}$. Wir haben die orthogonale Zerlegung in Idempotente $\underline{e} = (e_1, e_2) = (\left(\begin{smallmatrix}1&0&0\\0&0&0\\0&0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right))$ in A. Dementsprechend wird

$$A = e_1Ae_1 \oplus e_2Ae_1 \oplus e_1Ae_2 \oplus e_2Ae_2 = \left(\begin{smallmatrix}K&0&0\\0&0&0\\0&0&0\end{smallmatrix}\right) \oplus \left(\begin{smallmatrix}0&0&0\\K&0&0\\K&0&0\end{smallmatrix}\right) \oplus \left(\begin{smallmatrix}0&K&K\\0&0&0\\0&0&0\end{smallmatrix}\right) \oplus \left(\begin{smallmatrix}0&0&0\\0&K&K\\0&K&K\end{smallmatrix}\right) .$$

Es ist e_1 primitiv. Denn es ist e_1Ae_1 ein Teilring von A (mit einer anderen 1), welcher isomorph zu K ist. Aus $e_1 = e' + e''$ wie in Definition 51 folgt $e_1e' = (e' + e'')e' = e'$ etc., also $e', e'' \in e_1Ae_1$. Da e_1Ae_1 ein Körper ist, folgt aber aus $e'e'' = 0$, daß $e' = 0$ oder $e'' = 0$.
Es ist $e_2 = \left(\begin{smallmatrix}0&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&0&0\\0&1&0\\0&0&0\end{smallmatrix}\right) + \left(\begin{smallmatrix}0&0&0\\0&0&0\\0&0&1\end{smallmatrix}\right)$ nicht primitiv.

Ein A-Modul M heißt *unzerlegbar*, wenn $M \neq 0$ und wenn aus $M = X \oplus Y$ mit Teilmoduln $X, Y \subseteq M$ bereits $X = 0$ oder $Y = 0$ folgt.

Bemerkung 55 *Sei $e \in A$ ein Idempotent.*

Es ist e genau dann primitiv, wenn Ae ein unzerlegbarer A-Modul ist.

Beweis.

Sei Ae unzerlegbar. Es ist $Ae \neq 0$, also $e \neq 0$.

Sei $e = e' + e''$ mit Idempotenten e' und e'' in A so, daß $e'e'' = 0$ und $e''e' = 0$.

Es genügt zu zeigen, daß $Ae \stackrel{!}{=} Ae' \oplus Ae''$, da dann wegen Ae unzerlegbar folgt, daß $Ae' = 0$ oder $Ae'' = 0$, also auch $e' = 0$ oder $e'' = 0$, womit dann e als primitiv nachgewiesen ist.

Es ist $Ae' \subseteq Ae$, da $ae' = ae'(e' + e'') = ae'e$ für $a \in A$. Analog ist $Ae'' \subseteq Ae$.

Es ist $Ae = Ae' + Ae''$, da $ae = ae' + ae''$ für $a \in A$. Bleibt die Direktheit zu zeigen. Sei $a'e' + a''e'' = 0$ mit $a', a'' \in A$. Dann ist $0 = (a'e' + a''e'')e' = a'e'$; genauso ist $0 = a''e''$.

Sei e primitiv. Es ist $e \neq 0$, also $Ae \neq 0$. Sei $Ae = X \oplus Y$ für Teilmoduln $X, Y \subseteq Ae$. Sei $\pi : Ae = X \oplus Y \longrightarrow Ae$, $x + y \longmapsto x$, wobei $x \in X$ und $y \in Y$. Es ist π eine A-lineare Abbildung. Es ist $\pi^2 = \pi$.

Setze $e' := \pi(e)$ und $e'' := e - \pi(e)$.

Es ist $ee' = e\pi(e) = \pi(ee) = \pi(e) = e'$. Es ist $e'e = \pi(e)e = \pi(e) = e'$, da $\pi(e) \in Ae$ ist.

Es ist $e'^2 = e'\pi(e) = \pi(e'e) = \pi(e') = \pi(\pi(e)) = \pi(e) = e'$.

Es ist $e''^2 = (e - e')^2 = e^2 - ee' - e'e + e'^2 = e - e' - e' + e' = e''$.

Es ist $e'e'' = e'(e - e') = e' - e' = 0$. Es ist $e''e' = (e - e')e' = e' - e' = 0$.

Da e primitiv ist, folgt $e' = 0$ oder $e'' = 0$.

Ist $e' = 0$, dann ist $\pi(ae) = a\pi(e) = ae' = 0$ für $a \in A$. Somit ist $X = \pi(Ae) = 0$,

Ist $e'' = 0$, dann ist $e = e'$ und also $\pi(ae) = a\pi(e) = ae' = ae$ für $a \in A$. Also ist $\pi = \mathrm{id}_{Ae}$, und somit $Y = \operatorname{Kern} \pi = 0$.

Also ist Ae unzerlegbar. □

Bemerkung 56 *Sei A ein Ring. Seien e, $f \in A$ Idempotente.*

Es ist

$$\begin{array}{rcl} \mathrm{Hom}_A(Ae, Af) & \longrightarrow & eAf \\ \varphi & \longmapsto & \varphi(e) \\ (be \mapsto beaf) & \longleftarrow\!\shortmid & eaf \end{array}$$

ein Isomorphismus abelscher Gruppen, mit Inversem wie angegeben, wobei a, $b \in A$.

Beweis. Für $\varphi \in \mathrm{Hom}_A(Ae, Af)$ ist $\varphi(e) \in Af$, sowie $e\varphi(e) = \varphi(ee) = \varphi(e)$, insgesamt also $\varphi(e) \in eAf$. Die somit wohldefinierte Abbildung $\mathrm{Hom}_A(Ae, Af) \longrightarrow eAf$, $\varphi \longmapsto \varphi(e)$, ist zudem ein Morphismus abelscher Gruppen.

Für $a \in A$ ist die Abbildung $Ae \to Af$, $be \mapsto (be)(eaf) = beaf$ für $b \in A$, in der Tat A-linear. Dies zeigt die Wohldefiniertheit der Abbildung $eAf \longrightarrow \mathrm{Hom}_A(Ae, Af)$, $eaf \longmapsto (be \mapsto beaf)$.

Bleibt zu zeigen, daß die beiden Abbildungen sich gegenseitig invertieren.

Für $\varphi \in \mathrm{Hom}_A(Ae, Af)$ ist

$$\varphi \longmapsto \varphi(e) \longmapsto (be \mapsto b\varphi(e) = \varphi(be)) = \varphi .$$

Für $a \in A$ ist

$$eaf \longmapsto (be \mapsto beaf) \longmapsto (be \mapsto beaf)(e) = eaf .$$

□

3.2 Algebren

3.2.1 Begriff der R-Algebra

Sei R ein kommutativer Ring.

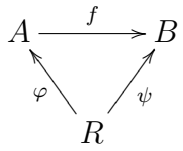
Definition 57

(1) Eine R-Algebra (A, φ) besteht aus einem Ring A und einem Ringmorphismus $\varphi : R \longrightarrow A$ mit $\varphi(R) \subseteq \mathrm{Z}(A)$.

Oft schreibt man kurz $A := (A, \varphi)$. Oft schreibt man $r := \varphi(r) \in A$ für $r \in R$, auch wenn φ nicht injektiv ist.

(2) Seien $A = (A, \varphi)$ und $B = (B, \psi)$ zwei R-Algebren.

Ein Ringmorphismus $f : A \longrightarrow B$ heißt *R-Algebrenmorphismus* oder *Morphismus von R-Algebren,* falls $f \circ \varphi = \psi$.



Ein bijektiver R-Algebrenmorphismus heißt auch *Isomorphismus von R-Algebren.* Diesenfalls ist auch sein Inverses ein Isomorphismus von R-Algebren; cf. Aufgabe 19.(3). Es heißen die R-Algebren A und B *isomorph,* geschrieben $A \simeq B$, wenn es zwischen ihnen einen Isomorphismus gibt.

Eine (R-)*Teilalgebra* von A ist ein Teilring $\tilde{A} \subseteq A$ so, daß $\varphi(R) \subseteq \tilde{A}$, zusammen mit $\varphi|^{\tilde{A}}$. Dann ist die Inklusionsabbildung $\tilde{A} \longrightarrow A$ ein R-Algebrenmorphismus.

Bemerkung 58 Sei I eine Menge. Sei $A_i = (A_i, \varphi_i)$ eine R-Algebra für $i \in I$.

Es wird auch $\prod_{i\in I} A_i = \{ (a_i)_i : a_i \in A_i \text{ für } i \in I \}$ zu einer R-Algebra vermöge

$$\begin{array}{rcrcl} (a_i)_i & + & (b_i)_i & := & (a_i + b_i)_i \\ (a_i)_i & \cdot & (b_i)_i & := & (a_i \cdot b_i)_i \end{array}$$

für $(a_i)_i, (b_i)_i \in \prod_{i\in I} A_i$, und vermöge

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & \prod_{i\in I} A_i \\ r & \longmapsto & (\varphi_i(r))_i \,. \end{array}$$

Es heißt $\prod_{i\in I} A_i$ das (äußere) direkte Produkt des Tupels von Algebren $(A_i)_{i\in I}$; für $j \in I$ heißt A_j ein *direkter Faktor* von $\prod_{i\in I} A_i$.

Ist $I = [1, k]$ für ein $k \in \mathbf{Z}_{\geqslant 1}$, so schreiben wir auch $\prod_{i\in[1,k]} A_i = A_1 \times A_2 \times \cdots \times A_k$.

Beispiel 59

(1) Für jeden Ring A gibt es genau einen Ringmorphismus $\mathbf{Z} \longrightarrow A$, sein Bild ist in $\mathrm{Z}(A)$. Also ist jeder Ring eine $\mathbf{Z}$-Algebra auf eindeutige Weise, und jeder Ringmorphismus ist ein $\mathbf{Z}$-Algebrenmorphismus.

(2) Sei p eine Primzahl. Für jeden Ring A mit $\operatorname{char} A = p$ gibt es genau einen Ringmorphismus $\mathbf{F}_p \longrightarrow A$, sein Bild ist in $\mathrm{Z}(A)$. Also ist jeder Ring von Charakteristik p eine $\mathbf{F}_p$-Algebra auf eindeutige Weise, und jeder Ringmorphismus zwischen Ringen von Charakteristik p ist ein $\mathbf{F}_p$-Algebrenmorphismus.

(3) Für $n \in \mathbf{Z}_{\geqslant 0}$ ist $R^{n\times n}$ eine R-Algebra vermöge $\varphi : R \longrightarrow \mathrm{Z}(R^{n\times n})$, $r \longmapsto r\mathrm{E}_n$; cf. Beispiel 47. Insbesondere ist R via $\mathrm{id} : R \longrightarrow R$ eine R-Algebra.

Für $t \in \mathbf{Z}_{\geqslant 1}$ und $n_i \in \mathbf{Z}_{\geqslant 1}$ für $i \in [1,t]$ ist $\prod_{i\in[1,t]} R^{n_i\times n_i}$ eine R-Algebra; cf. Bemerkung 58.

(4) Der Gruppenring RG ist eine R-Algebra via $R \longrightarrow RG$, $r \longmapsto r = r \cdot 1_G$; cf. Definition 42.

Ist $H \leqslant G$, so ist RH eine Teilalgebra von RG.

Lemma 60 (Universelle Eigenschaft der Gruppenalgebra)
Sei G eine Gruppe. Sei A eine R-Algebra. Sei $f : G \longrightarrow \mathrm{U}(A)$ ein Gruppenmorphismus.

Dann gibt es genau einen R-Algebrenmorphismus $\hat{f} : RG \longrightarrow A$, der folgendes Diagramm kommutativ macht.

$$\begin{array}{ccc} RG & \overset{\exists!\hat{f}}{\dashrightarrow} & A \\ \uparrow & & \uparrow \\ G & \xrightarrow[f]{} & \mathrm{U}(A) \end{array}$$

Beweis. Dies ist Bemerkung 48 in neuen Begriffen. ▫

Bemerkung 61 *Sei R ein kommutativer Ring.*
Seien $A = (A, \varphi)$ und $B = (B, \psi)$ zwei R-Algebren.

(1) *Via $r \cdot a = ra := \varphi(r)a$ für $r \in R$ und $a \in A$ wird A zu einem R-Modul.*

(2) *Sei $f : A \longrightarrow B$ ein Ringmorphismus. Es ist f genau dann ein R-Algebrenmorphismus, wenn f eine R-lineare Abbildung ist.*

Beweis. Siehe Aufgabe 19.(1, 2). ▫

Definition 62 Sei K ein Körper. Sei $A = (A, \varphi)$ eine K-Algebra.

(1) Es heißt A *endlichdimensional,* falls A als K-Vektorraum endlichdimensional ist.

(2) Sei M ein A-Modul. Eingeschränkt via $K \xrightarrow{\varphi} A$ wird M zu einem K-Vektorraum.
Es heißt M *endlichdimensional,* wenn M als K-Vektorraum endlichdimensional ist.

3.2.2 Halbeinfachheit von K-Algebren

Sei K ein Körper. Sei $A = (A, \varphi)$ eine endlichdimensionale K-Algebra. Sei $A \neq 0$.

Ein A-Modul M heißt *einfach,* wenn $M \neq 0$ ist und M nur die Teilmoduln 0 und M hat.

Definition 63 Die Algebra A heißt *halbeinfach,* wenn Ae ein einfacher A-Modul ist für jedes primitive Idempotent $e \in A$.

Bemerkung 64 *Es gibt eine orthogonale Zerlegung in primitive Idempotente in A.*

Beweis. Annahme, es gibt keine orthogonale Zerlegung in primitive Idempotente in A.

Behauptung. Für alle $n \in \mathbf{Z}_{\geqslant 1}$ gibt es eine orthogonale Zerlegung in Idempotente $\underline{e} = (e_1, \ldots, e_n)$ in A mit $e_i \neq 0$ für $i \in [1, n]$.

Induktion über $n \geqslant 1$.

Induktionsanfang. Es ist (1) eine orthogonale Zerlegung in Idempotente in A.

Induktionsschritt. Sei $\underline{e} = (e_1, \ldots, e_n)$ eine orthogonale Zerlegung in Idempotente in A mit $e_i \neq 0$ für $i \in [1, n]$.

Es gibt ein $k \in [1, n]$ mit e_k nicht primitiv. Also gibt es Idempotente $e' \neq 0$ und $e'' \neq 0$ in A mit $e_k = e' + e''$ und $e'e'' = e''e' = 0$.

Da $e_i \neq 0$ für $i \in [1, n] \smallsetminus \{k\}$ und da $e' \neq 0$ und $e'' \neq 0$, genügt es zu zeigen, daß

$$(e_1, \ldots, e_{k-1}, e', e'', e_{k+1}, \ldots, e_n)$$

eine orthogonale Zerlegung in Idempotente ist.

Dieses Tupel besteht aus Idempotenten.

Seine Summe ist 1.

Es ist $e'e'' = e''e' = 0$.

Es ist $e_ie_j = 0$ für $i, j \in [1, n] \smallsetminus \{k\}$ mit $i \neq j$.

Es ist $e'e_i = e'(e' + e'')e_i = e'e_ke_i = 0$ für $i \in [1, n] \smallsetminus \{k\}$.

Genauso ist auch $e_ie' = 0$, $e''e_i = 0$ und $e_ie'' = 0$ für $i \in [1, n] \smallsetminus \{k\}$.

Dies zeigt die *Behauptung.*

Setze $n := 1 + \dim_K A$ und wähle eine orthogonale Zerlegung $(e_1, \ldots, e_n)$ in Idempotente in A. Es ist $A = \bigoplus_{i \in [1,n]} Ae_i$; cf. Bemerkung 52. Es ist $0 \neq e_i \in Ae_i$ und somit $\dim_K Ae_i \geqslant 1$ für $i \in [1, n]$. Zusammen ist also

$$n - 1 \;=\; \dim_K A \;=\; \sum_{i \in [1,n]} \dim_K Ae_i \;\geqslant\; n \,,$$

und wir haben einen Widerspruch. □

Lemma 65 *Die folgenden Aussagen* (1), (2), (3) *und* (4) *sind äquivalent.*

(1) *Es ist A halbeinfach.*

(2) *Es gibt ein $n \in \mathbf{Z}_{\geqslant 1}$ und eine orthogonale Zerlegung in primitive Idempotente $\underline{e} = (e_1\,,\,\ldots\,,\,e_n)$ in A so, daß $A = \bigoplus_{i\in[1,n]} Ae_i$ und Ae_i ein einfacher A-Modul ist für $i \in [1,n]$.*

(3) *Es gibt ein $n \in \mathbf{Z}_{\geqslant 1}$ und eine Zerlegung $A = \bigoplus_{i\in[1,n]} S_i$ mit einfachen A-Teilmoduln $S_i \subseteq A$ für $i \in [1,n]$.*

(4) *Für jeden endlichdimensionalen A-Modul M und jeden Teilmodul $N \subseteq M$ gibt es einen Teilmodul $X \subseteq M$ so, daß $M = N \oplus X$.*

Beweis.

Zu (4) $\Rightarrow$ (1). Sei $e \in A$ ein primitives Idempotent. Sei $N \subset Ae$ ein Teilmodul. Wir haben $N \stackrel{!}{=} 0$ zu zeigen. Nach (4) gibt es einen Teilmodul $X \subseteq Ae$ mit $Ae = N \oplus X$. Da $N \neq Ae$ ist, ist $X \neq 0$. Da Ae unzerlegbar ist, folgt $N = 0$; cf. Bemerkung 55.

Zu (1) $\Rightarrow$ (2). Es gibt eine orthogonale Zerlegung in primitive Idempotente $\underline{e} = (e_1\,,\,\ldots\,,\,e_n)$ in A ; cf. Bemerkung 64. Es ist $A = \bigoplus_{i\in[1,n]} Ae_i$; cf. Bemerkung 52. Nach (1) ist Ae_i einfach für $i \in [1,n]$.

Zu (2) $\Rightarrow$ (3). Setze $S_i := Ae_i$ für $i \in [1,n]$.

Zu (3) $\Rightarrow$ (4). Sei M ein endlichdimensionaler A-Modul. Sei $(m_1, \ldots, m_\ell)$ eine K-lineare Basis von M. Es ist

$$\begin{array}{rcl} A^{\oplus\ell} & \xrightarrow{\ f\ } & M \\ (a_1\,,\,\ldots\,,\,a_\ell) & \longmapsto & \sum_{i\in[1,\ell]} a_i m_i \end{array}$$

eine surjektive A-lineare Abbildung.

Ist $T \subseteq A^{\oplus\ell}$ ein einfacher Teilmodul, so ist $f(T)$ isomorph zu T oder zu 0, da der Kern von $f|_T$ gleich 0 oder gleich T ist; und somit ist $f(T)$ einfach oder gleich 0.

Nach (3) gibt es eine Zerlegung $A = \bigoplus_{i\in[1,n]} S_i$, wobei S_i ein einfacher A-Modul ist für $i \in [1,n]$. Also ist $A^{\oplus\ell} = \bigoplus_{j\in[1,\ell n]} T_j$ für gewisse einfache Teilmoduln T_j . Wir erhalten

$$M \;=\; f(A^{\oplus\ell}) \;=\; f(\,{}_A\langle\, T_j \,:\, j \in [1,\ell n]\,\rangle) \;=\; {}_A\langle\, f(T_j) \,:\, j \in [1,\ell n]\,\rangle\ .$$

Folglich ist M das A-lineare Erzeugnis seiner einfachen Teilmoduln.

Wegen M endlichdimensional hat jede nichtleere Teilmenge von

$$\{Y \subseteq M \;:\; Y \text{ ist Teilmodul}\}$$

ein bezüglich Inklusion maximales Element.

Sei nun $N \subseteq M$ ein Teilmodul. Sei $X \subseteq M$ maximal unter den Teilmoduln von M, die Schnitt 0 mit N haben. Wir wollen $N \oplus X \stackrel{!}{=} M$ zeigen. *Annahme,* $N \oplus X \subset M$. Dann

gibt es einen einfachen Teilmodul $T \subseteq M$ mit $T \not\subseteq N \oplus X$, da M von seinen einfachen Teilmoduln erzeugt wird. Es ist $(N \oplus X) \cap T \subset T$. Wegen T einfach folgt hieraus, daß $(N \oplus X) \cap T = 0$. Dies liefert $N \oplus X \oplus T \subseteq M$, und also $N \cap (X \oplus T) = 0$, im *Widerspruch* zur Maximalität von X. ▫

Lemma 66 (Schur)
Seien M und N einfache A-Moduln.

(1) *Jeder nichtverschwindende Morphismus von M nach N ist ein Isomorphismus.*

(2) *Ist $M \not\simeq N$, so ist* $\mathrm{Hom}_A(M,N) = 0$.

(3) *Es ist* $\mathrm{End}_A(M)$ *ein Schiefkörper.*

(4) *Ist K algebraisch abgeschlossen, so haben wir einen Isomorphismus $K \xrightarrow{\sim} \mathrm{End}_A(M)$, $\lambda \longmapsto (m \mapsto \lambda m = \varphi(\lambda)m)$ von K-Algebren.*

Beweis. Siehe Aufgabe 20.(1, 2, 5). ▫

Das Argument zu folgendem Satz 67 von Wedderburn kann wie folgt heuristisch skizziert werden.

Sei A eine endlichdimensionale Algebra über einem algebraisch abgeschlossenen Körper K.

Sei $(e_1, \ldots, e_n)$ eine orthogonale Zerlegung in primitive Idempotente, so sortiert, daß $Ae_i \simeq Ae_j$ als A-Moduln und $i \leqslant k \leqslant j$ implizieren, daß auch $Ae_i \simeq Ae_k \simeq Ae_j$ als A-Moduln. Zwecks graphischer Darstellung sei einmal pars pro toto $n = 6$ und

$$Ae_1 \;\simeq\; Ae_2 \;\not\simeq\; Ae_3 \;\simeq\; Ae_4 \;\simeq\; Ae_5 \;\not\simeq\; Ae_6\,,$$

und $Ae_1 \not\simeq Ae_6$. Dann wird

$$A \overset{\text{L. 53}}{=} \begin{pmatrix} e_1Ae_1 & e_1Ae_2 & e_1Ae_3 & e_1Ae_4 & e_1Ae_5 & e_1Ae_6 \\ e_2Ae_1 & e_2Ae_2 & e_2Ae_3 & e_2Ae_4 & e_2Ae_5 & e_2Ae_6 \\ e_3Ae_1 & e_3Ae_2 & e_3Ae_3 & e_3Ae_4 & e_3Ae_5 & e_3Ae_6 \\ e_4Ae_1 & e_4Ae_2 & e_4Ae_3 & e_4Ae_4 & e_4Ae_5 & e_4Ae_6 \\ e_5Ae_1 & e_5Ae_2 & e_5Ae_3 & e_5Ae_4 & e_5Ae_5 & e_5Ae_6 \\ e_6Ae_1 & e_6Ae_2 & e_6Ae_3 & e_6Ae_4 & e_6Ae_5 & e_6Ae_6 \end{pmatrix}$$

Es ist $e_iAe_j \simeq \mathrm{Hom}(Ae_i, Ae_j)$ stets; cf. Bemerkung 56.

Da A halbeinfach ist, ist Ae_i stets einfach; cf. Definition 63.

Nach Schurs Lemma 66.(2) ist $e_iAe_j = 0$, falls $Ae_i \not\simeq Ae_j$. Also wird

$$A \;=\; \begin{pmatrix} e_1Ae_1 & e_1Ae_2 & & & & \\ e_2Ae_1 & e_2Ae_2 & & & & \\ & & e_3Ae_3 & e_3Ae_4 & e_3Ae_5 & \\ & & e_4Ae_3 & e_4Ae_4 & e_4Ae_5 & \\ & & e_5Ae_3 & e_5Ae_4 & e_5Ae_5 & \\ & & & & & e_6Ae_6 \end{pmatrix}$$

Nach Schurs Lemma 66.(4) ist $K \simeq \mathrm{Hom}(Ae_i, Ae_i) \simeq e_iAe_i$.

Ist $Ae_i \simeq Ae_j$, dann wird $K \simeq \mathrm{Hom}(Ae_i, Ae_i) \simeq \mathrm{Hom}(Ae_i, Ae_j) \simeq e_iAe_j$.

Also wird

$$A \simeq \begin{pmatrix} K & K & & & & & \\ K & K & & & & & \\ & & K & K & K & & \\ & & K & K & K & & \\ & & K & K & K & & \\ & & & & & K & \end{pmatrix} \simeq K^{2\times 2} \times K^{3\times 3} \times K^{1\times 1}$$

als K-Algebren.

Die dubiosen Isomorphismen in dieser Skizze müssen nun genauer betrachtet werden.

Satz 67 (Wedderburn) *Sei K algebraisch abgeschlossen.*

Weiterhin sei A eine endlichdimensionale K-Algebra ungleich 0.

Die folgenden Aussagen (1) und (2) sind äquivalent.

(1) *Es ist A halbeinfach.*

(2) *Es gibt $t \in \mathbf{Z}_{\geqslant 1}$ und $m_s \in \mathbf{Z}_{\geqslant 1}$ für $s \in [1,t]$ so, daß als K-Algebren*

$$A \simeq K^{m_1\times m_1} \times \cdots \times K^{m_t \times m_t}$$

ist. Ein zugehöriger Isomorphismus heißt auch Wedderburnisomorphismus.

Beweis.

Zu (2) $\Rightarrow$ (1). Es ist $K^{m_s\times m_s}$ halbeinfach für $s \in [1,t]$; cf. Aufgabe 21.(1).

Also ist $K^{m_1\times m_1} \times \cdots \times K^{m_t\times m_t}$ halbeinfach; cf. Aufgabe 21.(2).

Somit ist auch A halbeinfach; cf. Aufgabe 21.(3).

Zu (1) $\Rightarrow$ (2). Sei $(e_1, \ldots, e_n)$ eine orthogonale Zerlegung in primitive Idempotente in A; cf. Bemerkung 64. Es ist Ae_i ein einfacher A-Modul für $i \in [1,n]$, da A halbeinfach ist.

Heißen $i, j \in [1,n]$ äquivalent, geschrieben $i \sim j$, wenn $Ae_i \simeq Ae_j$ als A-Moduln. Seien die e_i o.E. so angeordnet, daß die Äquivalenzklassen Intervalle sind. Seien die Äquivalenzklassen gegeben durch $[n_0+1, n_1]$, $[n_1+1, n_2]$, $\ldots$, $[n_{t-1}+1, n_t]$ mit $t \in \mathbf{Z}_{\geqslant 0}$ und $0 = n_0 < n_1 < \cdots < n_{t-1} < n_t = n$.

Wähle einen Isomorphismus $\alpha_{i,n_s} : Ae_{n_s} \xrightarrow{\sim} Ae_i$ von A-Moduln für alle $s \in [1,t]$ und alle $i \in [n_{s-1}+1, n_s]$. Wähle dabei $\alpha_{n_s,n_s} := \mathrm{id}_{Ae_{n_s}}$.

Wir setzen $\alpha_{j,i} := \alpha_{j,n_s} \circ \alpha_{i,n_s}^{-1} : Ae_i \xrightarrow{\sim} Ae_j$ für $s \in [1,t]$ und $i, j \in [\, n_{s-1}+1\,,\, n_s]$. Ist $i = n_s$, so stimmt dies mit der bisherigen Wahl überein. Es wird

$$\alpha_{k,j} \circ \alpha_{j,i} \;=\; \alpha_{k,n_s} \circ \alpha_{j,n_s}^{-1} \circ \alpha_{j,n_s} \circ \alpha_{i,n_s}^{-1} \;=\; \alpha_{k,n_s} \circ \alpha_{i,n_s}^{-1} \;=\; \alpha_{k,i}$$

für $s \in [1,t]$ und $i, j, k \in [\, n_{s-1}+1\,,\, n_s]$.

Sei $B := K^{(n_1-n_0)\times(n_1-n_0)} \times K^{(n_2-n_1)\times(n_2-n_1)} \times \cdots \times K^{(n_t-n_{t-1})\times(n_t-n_{t-1})}$.

Ist $s \in [1,t]$ und sind $i,\, j \,\in\, [n_{s-1}+1\,,\, n_s]$, so sei $\eta_{i,j}$ das Element von B, dessen s-ter Tupeleintrag an Matrixposition $(i-n_{s-1}\,,\, j-n_{s-1})$ eine 1 aufweist, und Nullen sonst, und dessen übrige Tupeleinträge alles Nullmatrizen sind. Es ist

$$\big(\,\eta_{i,j}\,:\,i,\,j\,\in\,[1,n],\;i\sim j\,\big)$$

eine K-lineare Basis von B.

Wir erhalten eine K-lineare Abbildung durch die Setzung

$$\begin{array}{ccc} B & \stackrel{\omega}{\longrightarrow} & A \\ \eta_{i,j} & \longmapsto & \alpha_{j,i}(e_i) \end{array}$$

für $i,\, j \,\in\, [1,n]$ mit $i \sim j$.

Beachte, daß dabei stets $\alpha_{j,i}(e_i)$ in e_iAe_j liegt, da es ohnehin in Ae_j liegt und zudem $e_i\alpha_{j,i}(e_i) = \alpha_{j,i}(e_ie_i) = \alpha_{j,i}(e_i)$ ist.

Wir wollen zeigen, daß ω ein K-Algebrenisomorphismus ist.

Injektivität. Es ist $A = \bigoplus_{i,\,j\,\in\,[1,n]} e_iAe_j$ und $\alpha_{j,i}(e_i) \in e_iAe_j \smallsetminus \{0\}$ für $i \sim j$; cf. Lemma 53. Also ist das Bild unserer Basis linear unabhängig und ω somit injektiv.

Surjektivität. Es genügt zu zeigen, daß

$$\dim_K A \;\stackrel{!}{=}\; \dim_K B \;=\; \sum_{s\in[1,t]} (n_s - n_{s-1})^2\;.$$

Wegen $A = \bigoplus_{i,\,j\,\in\,[1,n]} e_iAe_j$ und $|\{\,(i,j) \in [1,n]\times[1,n]\;:\;i\sim j\,\}| = \sum_{s\in[1,t]}(n_s-n_{s-1})^2$ genügt es zu zeigen, daß $\dim_K e_iAe_j \stackrel{!}{=} 0$ für $i \not\sim j$ und $\dim_K e_iAe_j \stackrel{!}{=} 1$ für $i \sim j$; cf. Lemma 53.

Für $i \not\sim j$ ist $e_iAe_j \simeq \mathrm{Hom}_A(Ae_i\,,\,Ae_j) = 0$; cf. Bemerkung 56, Lemma 66.(2). Also ist $\dim_K e_iAe_j = 0$.

Für $i \sim j$ schränkt der A-lineare Isomorphismus $\alpha_{j,i} : Ae_i \xrightarrow{\sim} Ae_j$ zu einem K-linearen Isomorphismus $e_iAe_i \xrightarrow{\sim} e_iAe_j$ ein. Ferner ist $e_iAe_i \simeq \mathrm{Hom}_A(Ae_i\,,\,Ae_i) \simeq K$; cf. Bemerkung 56, Lemma 66.(4); wobei die Isomorphie insgesamt $\lambda e_i \longmapsto (ae_i \mapsto \lambda ae_i) \longmapsto \lambda$ abbildet und somit K-linear ist. Also ist $\dim_K e_iAe_j = 1$.

K-Algebrenmorphismus. Um zu zeigen, daß die K-lineare Abbildung ω ein K-Algebrenmorphismus ist, bleibt zu zeigen, daß $\omega(\eta_{i,j}\cdot\eta_{k,\ell}) \stackrel{!}{=} \omega(\eta_{i,j})\cdot\omega(\eta_{k,\ell})$ für $i,\, j,\, k,\, \ell \,\in\, [1,n]$ mit $i \sim j$ und $k \sim \ell$, und daß $\omega(1_B) \stackrel{!}{=} 1_A$; cf. Bemerkung 61.(2).

Ist $j \neq k$, so wird zum einen $\omega(\eta_{i,j}\cdot\eta_{k,\ell}) = \omega(0) = 0$, und zum anderen $\omega(\eta_{i,j})\cdot\omega(\eta_{k,\ell}) \in e_iAe_j \cdot e_kAe_\ell = 0$.

Ist $j = k$, so wird zum einen

$$\omega(\eta_{i,j}\cdot\eta_{j,\ell}) \;=\; \omega(\eta_{i,\ell}) \;=\; \alpha_{\ell,i}(e_i)\;,$$

und zum anderen

$$\omega(\eta_{i,j})\cdot\omega(\eta_{j,\ell}) \;=\; \alpha_{j,i}(e_i)\cdot\alpha_{\ell,j}(e_j) \;=\; \alpha_{\ell,j}\big(\overbrace{\alpha_{j,i}(e_i)}^{\in e_iAe_j}e_j\big) \;=\; \alpha_{\ell,j}\big(\alpha_{j,i}(e_i)\big) \;=\; \alpha_{\ell,i}(e_i)\;.$$

Schließlich ist $\alpha_{i,i} = \alpha_{i,n_s}\circ\alpha_{i,n_s}^{-1} = \mathrm{id}_{Ae_i}$ für $i\in[1,n]$, mit $s\in[1,t]$ so, daß $i\sim n_s$, und also

$$\omega(1_B) \;=\; \omega(\textstyle\sum_{i\in[1,n]}\eta_{i,i}) \;=\; \sum_{i\in[1,n]}\omega(\eta_{i,i}) \;=\; \sum_{i\in[1,n]}\alpha_{i,i}(e_i) \;=\; \sum_{i\in[1,n]}e_i \;=\; 1_A\;.$$

□

Bemerkung 68

(1) Insbesondere folgt im Falle K algebraisch abgeschlossen aus der Symmetrie der Charakterisierung von Satz 67, daß A auch genau dann halbeinfach ist, wenn eA ein einfacher A-Rechtsmodul ist für alle primitiven Idempotente $e\in A$. Ferner gelten die Äquivalenzen von Lemma 65 entsprechend auch für Rechtsmoduln.

(2) Beispiele für Wedderburnisomorphismen haben wir schon in Beispiel 50 und Aufgabe 18.(1) gesehen; cf. auch Aufgabe 23.

3.3 Maschke

Lemma 69 (Maschke) *Sei K ein Körper. Sei G eine endliche Gruppe.*

Es ist KG halbeinfach genau dann, wenn $|G|$ kein Vielfaches von $\mathrm{char}\,K$ *ist.*

Insbesondere ist KG halbeinfach, falls $\mathrm{char}\,K = 0$.

Beweis.

$\Leftarrow$. Sei $|G|$ kein Vielfaches von $\mathrm{char}\,K$. Wir wollen zeigen, daß KG halbeinfach ist.

Sei M ein endlichdimensionaler KG-Modul. Sei $N\subseteq M$ ein Teilmodul. Wir haben zu zeigen, daß ein KG-Teilmodul $X\subseteq M$ mit $M = N\oplus X$ existiert; cf. Lemma 65.

Sei $f: M\longrightarrow N$ eine K-lineare Abbildung mit $f|_N = \mathrm{id}_N$. Sei

$$\begin{array}{rccl} f' & : & M & \longrightarrow & N \\ & & m & \longmapsto & f'(m) \;:=\; |G|^{-1}\sum_{g\in G} g f(g^-m)\;. \end{array}$$

Es ist $f'|_N = \mathrm{id}_N$, da $f'(n) = |G|^{-1}\sum_{g\in G} g\, f(\underbrace{g^-n}_{\in N}) = |G|^{-1}\sum_{g\in G} g(g^-n) = |G|^{-1}\sum_{g\in G} n = n$ für $n\in N$.

Es ist f' eine KG-lineare Abbildung, da sie K-linear ist und sich für $x\in G$ und $m\in M$

$$\begin{array}{rcl} f'(xm) & = & |G|^{-1}\sum_g g\, f(g^-xm) \\ & \overset{y=x^-g}{=} & |G|^{-1}\sum_y xy\, f(y^-m) \\ & = & x\,|G|^{-1}\sum_y y\, f(y^-m) \\ & = & x\, f'(m) \end{array}$$

ergibt.

Sei $X := \operatorname{Kern} f'$. Dies ist ein KG-Teilmodul von M als Kern einer KG-linearen Abbildung.

Es ist $N \cap X = 0$, da für ein $n \in N \cap X = N \cap \operatorname{Kern} f'$ sich $n = f'(n) = 0$ ergibt.

Es ist $M = N + X$, da wir für $m \in M$ die Zerlegung $m = f'(m) + (m - f'(m))$ mit $f'(m) \in N$ und $f'(m - f'(m)) = f'(m) - f'(\underbrace{f'(m)}_{\in N}) = f'(m) - f'(m) = 0$ erhalten.

Insgesamt ist $M = N \oplus X$.

$\Rightarrow$. Sei KG halbeinfach. Wir wollen zeigen, daß $|G|$ kein Vielfaches von $\operatorname{char} K$ ist, d.h. daß $|G| \cdot 1_K \overset{!}{\neq} 0$.

Schreibe $\sigma := \sum_{g \in G} g \in KG$. Es ist $M := KG$ ein KG-Modul. Darin ist $N := KG\sigma$ ein Teilmodul.

Es ist $h\sigma = \sigma$ für $h \in G$ und also $N = K\sigma$.

Da KG halbeinfach ist, gibt es einen KG-Teilmodul $X \subseteq M$ mit $M = N \oplus X$; cf. Lemma 65. Die Projektion $\pi : M \longrightarrow M$, $n + x \longmapsto n$, wobei $n \in N$ und $x \in X$, ist eine KG-lineare Abbildung. Sie schickt $1 \in KG = M$ nach $\pi(1) = \lambda\sigma$ für ein $\lambda \in K$. Also wird

$$\begin{aligned} \sigma &= \pi(\sigma) \\ &= \pi(\textstyle\sum_g g) \\ &= \textstyle\sum_g g\,\pi(1) \\ &= \textstyle\sum_g g\,\lambda\sigma \\ &= \textstyle\sum_g \lambda\sigma \\ &= |G|\lambda\sigma\ . \end{aligned}$$

Ein Koeffizientenvergleich bei 1 gibt $1 = |G|\lambda = (|G| \cdot 1_K)\lambda$. Es folgt $|G| \cdot 1_K \neq 0$. ▫

Kapitel 4

Charaktere

4.1 Begriff des Charakters und erste Eigenschaften

Sei G eine endliche Gruppe.

Seien V, W endlichdimensionale $\mathbf{C}$-Vektorräume.

Sei $\rho : G \longrightarrow \mathrm{GL}(V)$ eine Darstellung von G auf V über $\mathbf{C}$.

Sei $\sigma : G \longrightarrow \mathrm{GL}(W)$ eine Darstellung von G auf W über $\mathbf{C}$.

Definition 70 Die Abbildung

$$\begin{array}{ccc} G & \xrightarrow{\chi_\rho} & \mathbf{C} \\ g & \longmapsto & \chi_\rho(g) := \operatorname{tr} \rho(g) \end{array}$$

heißt *Charakter* zu ρ.

Ein *Charakter von G* ist ein Charakter zu einer Darstellung von G.

Oft schreiben wir auch $\chi_V := \chi_\rho$, insbesondere, wenn wir uns auf den zugehörigen $\mathbf{C}G$-Modul V beziehen; cf. Lemma 44.

Bemerkung 71 *Sind g, $h \in G$ zueinander konjugiert, so ist $\chi_\rho(g) = \chi_\rho(h)$.*

Also genügt es, einen Charakter auf Repräsentanten von Konjugationsklassen zu kennen.

Beweis. Sei $x \in G$ mit $h = {}^x g$ gegeben. Dann wird

$$\chi_\rho(h) \;=\; \chi_\rho({}^x g) \;=\; \operatorname{tr}(\rho({}^x g)) \;=\; \operatorname{tr}(\rho(x) \circ \rho(g) \circ \rho(x)^-) \;=\; \operatorname{tr}(\rho(g)) \;=\; \chi_\rho(g)\ .$$

□

Bemerkung 72 *Es ist $\chi_\rho(1) = \chi_V(1) = \dim_{\mathbf{C}} V$ der* Grad *des Charakters χ_ρ.*

Beweis. Es ist $\chi_\rho(1) = \operatorname{tr}\rho(1) = \operatorname{tr}\mathrm{id}_V = \dim_{\mathbf{C}} V$. □

Beispiel 73

(1) Zur trivialen Darstellung $G \longrightarrow \mathrm{GL}_1(\mathbf{C})$, $g \longmapsto (1)$ gehört der *triviale Charakter* $G \longrightarrow \mathbf{C}$, $g \longmapsto 1$.

(2) Zur Darstellung $\rho : \mathrm{S}_3 \to \mathrm{GL}_2(\mathbf{C})$, $\mathrm{id} \mapsto \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, $(1,2) \mapsto \left(\begin{smallmatrix}-2&-1\\3&2\end{smallmatrix}\right)$, $(1,2,3) \mapsto \left(\begin{smallmatrix}-2&-1\\3&1\end{smallmatrix}\right)$ aus Beispiel 39.(4) gehört der Charakter

$$\begin{array}{rcr} \mathrm{S}_3 & \xrightarrow{\chi_\rho} & \mathbf{C} \\ \mathrm{id} & \longmapsto & 2 \\ (1,2) & \longmapsto & 0 \\ (1,2,3) & \longmapsto & -1\ . \end{array}$$

(3) Ist M eine endliche G-Menge, so ist

$$\chi_{\mathbf{C}M}(g) \;=\; |\{\, m \in M \,:\, gm = m \,\}|$$

für $g \in G$. Denn die Permutationsmatrix, die sich als Bild von g unter der zugehörigen Darstellung ergibt, hat bei $m \in M$ einen Diagonaleintrag 1, falls $gm = m$, und ansonsten Diagonaleintrag 0.

(4) Sei in (3) etwa $G = \mathrm{S}_3$ und $M = \{1,2,3\}$; cf. Beispiel 41.

Dann ist $\chi_{\mathbf{C}M}(\mathrm{id}) = \operatorname{tr}\left(\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right) = 3$, $\chi_{\mathbf{C}M}((1,2)) = \operatorname{tr}\left(\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right) = 1$ und $\chi_{\mathbf{C}M}((1,2,3)) = \operatorname{tr}\left(\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right) = 0$. Es ist auch e.g. $|\{\, m \in M \,:\, (1,2)m = m \,\}| = |\{3\}| = 1$.

(5) Setzen wir $M = G$ in (3), ausgestattet mit der Operation durch G durch Linksmultiplikation; cf. Beispiel 2.(3). Wir erhalten für $g \in G$

$$\chi_{\mathbf{C}G}(g) = |\{\, x \in G \,:\, gx = x \,\}| \;=\; \partial_{g,1} \cdot |G|\ ,$$

da für $x \in G$ die Aussage $gx = x$ äquivalent ist zu $g = 1$.

(6) Ist $\dim_{\mathbf{C}} V = 1$, so ist $\chi_\rho(g) = \rho(g)$, unter Verwendung der Identifikation $\mathbf{C} = \mathbf{C}^{1\times 1}$.

Bemerkung 74 *Aus $V \simeq W$ als $\mathbf{C}G$-Moduln folgt $\chi_V = \chi_W$.*

Die Umkehrung gilt auch; cf. Bemerkung 95.(2) unten.

Beweis. Sei $f : V \xrightarrow{\sim} W$ ein Isomorphismus von $\mathbf{C}G$-Moduln.

Sei $g \in G$. Es ist $\sigma(g) = f \circ \rho(g) \circ f^-$; cf. Bemerkung 45. Also wird

$$\chi_W(g) \;=\; \operatorname{tr}\sigma(g) \;=\; \operatorname{tr}(f \circ \rho(g) \circ f^-) \;=\; \operatorname{tr}\rho(g) \;=\; \chi_V(g)\ .$$

□

Bemerkung 75 *Es ist* $\chi_{V\oplus W} = \chi_V + \chi_W$.
Also sind Summen von Charakteren wieder Charaktere.

Beweis. Für $g \in G$ ist

$$\chi_{V\oplus W}(g) \;=\; \mathrm{tr}(\rho(g)\oplus\sigma(g)) \;=\; \mathrm{tr}(\rho(g)) + \mathrm{tr}(\sigma(g)) \;=\; \chi_V(g) + \chi_W(g)\ .$$

□

Definition 76 Ist V ein einfacher $\mathbf{C}G$-Modul, so heißt der Charakter χ_V *irreduzibel.*
Ein *irreduzibler Charakter von* G ist ein Charakter zu einem einfachen $\mathbf{C}G$-Modul.

Bemerkung 77
Jeder endlichdimensionale $\mathbf{C}G$*-Modul ist direkte Summe von einfachen Teilmoduln.*
Jeder Charakter von G *ist Summe von irreduziblen Charakteren von* G*.*

Beweis. Sei M ein endlichdimensionaler $\mathbf{C}G$-Modul. Wir führen eine Induktion über $\dim_{\mathbf{C}} M$.

Ist $M = 0$ oder M einfach, so sind wir fertig.

Ist $M \neq 0$ und M nicht einfach, so gibt es einen Teilmodul $0 \subset N \subset M$. Da $\mathbf{C}G$ halbeinfach ist, gibt es einen Teilmodul $P \subseteq M$ mit $M = N \oplus P$; cf. Lemma 69, Lemma 65.(4). Da sowohl N als auch P kleinere Dimension als M haben, zerfallen beide in eine direkte Summe von einfachen Teilmoduln. Diese beiden Zerlegungen zusammengesetzt geben eine direkte Zerlegung von M in einfache Teilmoduln. □

4.2 Charaktertafel

Sei G eine endliche Gruppe.

Notation 78 Wir wählen einen Wedderburnisomorphismus von $\mathbf{C}$-Algebren

$$\begin{array}{ccccccccc} \mathbf{C}G & \xrightarrow[\sim]{\omega} & \mathbf{C}^{n_1\times n_1} & \times & \cdots & \times & \mathbf{C}^{n_t\times n_t} & =: & B \\ \xi & \longmapsto & \big(\omega^1(\xi) & , & \ldots & , & \omega^t(\xi)\big) & = & \omega(\xi)\ ; \end{array}$$

cf. Lemma 69, Satz 67. (Die oberen Indizes an ω seien hierbei keine Exponenten.)
Schreibe dabei noch $\omega^s(\xi) = (\omega^s_{i,j}(\xi))_{i,j} \in \mathbf{C}^{n_s\times n_s}$ für $\xi \in \mathbf{C}G$ und $s \in [1,t]$.
Beachte $\sum_{s\in[1,t]} n_s^2 = |G|$.

Für $s \in [1,t]$ und $i,\, j \,\in\, [1,n_s]$ schreiben wir $\mathrm{e}^s_{i,j} \in \mathbf{C}^{n_1\times n_1} \times \cdots \times \mathbf{C}^{n_t\times n_t} = B$ für das Tupel, das an Position s die Matrix mit Eintrag 1 an Position (i,j) und Nullen sonst stehen hat, und ansonsten Nullmatrizen.

Es ist $(\, \mathrm{e}^s_{i,j} \,:\, s \in [1,t],\ i,\, j \,\in\, [1,n_s]\,)$ eine $\mathbf{C}$-lineare Basis von B.

Es ist $(\, \mathrm{e}^s_{i,i} \,:\, s \in [1,t],\ i \in [1,n_s]\,)$ eine orthogonale Zerlegung in primitive Idempotente in B, da $B\mathrm{e}^s_{i,i}$ als einfacher B-Modul insbesondere unzerlegbar ist; cf. Bemerkung 55, Aufgabe 21.(1).

Vermittels ω betrachten wir kommentarlos einen B-Modul X auch als $\mathbf{C}G$-Modul. Diesenfalls ist dann $\xi \cdot x := \omega(\xi)\cdot x$ für $\xi \in \mathbf{C}G$ und $x \in X$. Umgekehrt betrachten wir einen $\mathbf{C}G$-Modul vermittels ω^- kommentarlos auch als B-Modul.

Schreibe $\chi_s(g) := \operatorname{tr}\omega^s(g)$ für $s \in [1,t]$ und $g \in G$. Insbesondere ist $\chi_s(1) = n_s$.

Für $g \in G$ schreiben wir ${}^Gg := \{\, {}^xg \,:\, x \in G\,\}$ für die Konjugationsklasse von g in G. Es ist die Relation "ist konjugiert zu" eine Äquivalenzrelation auf G; diesbezüglich ist die Konjugationsklasse ${}^Gg$ die Äquivalenzklasse.

Zerlege $G = \bigsqcup_{r\in[1,t']} {}^Gg_r$, wobei $g_1 = 1_G$, und wobei $t' \in \mathbf{Z}_{\geqslant 1}$ die Anzahl der Konjugationsklassen in G bezeichne. In anderen Worten, sei $\{\, g_r \,:\, r \in [1,t']\,\}$ ein Repräsentantensystem der Konjugationsklassen in G mit $g_1 = 1_G$.

Schreibe $\bar g_r := \sum_{x\,\in\,{}^Gg_r} x$ für $r \in [1,t']$.

Wir werden noch sehen, daß $t = t'$ ist; cf. Lemma 84 unten.

Bemerkung 79 *Sei $s \in [1,t]$. Sei $i \in [1,n_s]$. Sei $g \in G$. Es ist $\omega^s(g)$ die beschreibende Matrix des Bildes von g unter der zum $\mathbf{C}G$-Modul $B\mathrm{e}^s_{i,i}$ gehörigen Darstellung bezüglich der Basis $(\mathrm{e}^s_{1,i}\,, \mathrm{e}^s_{2,i}\,, \ldots, \mathrm{e}^s_{n_s\,,i})$.*

Beweis. Für $j \in [1,n_s]$ ist

$$g\cdot \mathrm{e}^s_{j,i} \;=\; \omega(g)\,\mathrm{e}^s_{j,i} \;=\; \textstyle\sum_{k\in[1,n_s]} \omega^s_{k,j}(g)\,\mathrm{e}^s_{k,i}\ ,$$

wobei die erste Gleichheit aus der Vereinbarung über die $\mathbf{C}G$-Moduloperation auf einem B-Modul resultiert. Also ist die beschreibende Matrix der $\mathbf{C}$-linearen Abbildung $B\mathrm{e}^s_{i,i} \twoheadrightarrow B\mathrm{e}^s_{i,i}$, $b\,\mathrm{e}^s_{i,i} \mapsto g\cdot b\,\mathrm{e}^s_{i,i}$ gleich $\omega^s(g)$. ▫

Bemerkung 80 *Sei $s \in [1,t]$.*

Es ist $B\mathrm{e}^s_{1,1}$ ein einfacher $\mathbf{C}G$-Modul.

Es ist $\chi_s = \chi_{B\mathrm{e}^s_{1,1}}$, und dies ist daher ein irreduzibler Charakter von G.

Beweis. Es ist $B\mathrm{e}^s_{1,1}$ ein einfacher $\mathbf{C}G$-Modul; cf. Aufgabe 21.(1). Also ist $\chi_{B\mathrm{e}^s_{1,1}}$ irreduzibel.

Es ist $\omega^s(g)$ eine beschreibende Matrix des Bildes von g unter der zu $B\mathrm{e}^s_{1,1}$ gehörigen Darstellung von G; cf. Bemerkung 79. Also ist $\chi_{B\mathrm{e}^s_{1,1}} = \operatorname{tr}\omega^s(g) = \chi_s(g)$. ▫

Lemma 81 *Sei V ein einfacher $\mathbf{C}G$-Modul.*

Es gibt ein $s \in [1,t]$ mit $V \simeq B\mathrm{e}^s_{1,1}$ als $\mathbf{C}G$-Moduln.

Beweis. Sei $v \in V \setminus \{0\}$ gewählt. Wir haben die surjektive B-lineare Abbildung $f : B \longrightarrow V$, $\xi \longmapsto \omega^-(\xi)v$; cf. Aufgabe 20.(3). Da $V \neq 0$ ist, ist $\operatorname{Kern} f \subset B$. Da $B = \bigoplus_{s\in[1,t]} \bigoplus_{i\in[1,n_s]} B\mathrm{e}^s_{i,i}$ ist, gibt es ein $s \in [1,t]$ und ein $i \in [1,n_s]$ mit $B\mathrm{e}^s_{i,i} \not\subseteq \operatorname{Kern} f$; cf. Bemerkung 52. Da mithin $f|_{B\mathrm{e}^s_{i,i}} : B\mathrm{e}^s_{i,i} \longrightarrow V$ nicht verschwindet und da $B\mathrm{e}^s_{i,i}$ und V einfache B-Moduln sind, ist $f|_{B\mathrm{e}^s_{i,i}}$ ein Isomorphismus; cf. Lemma 66.(1).

Ferner ist $B\mathrm{e}^s_{i,i} \longrightarrow B\mathrm{e}^s_{1,1}$, $b\,\mathrm{e}^s_{i,i} \longmapsto b\,\mathrm{e}^s_{i,i}\mathrm{e}^s_{i,1} = b\,\mathrm{e}^s_{i,1}\mathrm{e}^s_{1,1}$ ein Isomorphismus von $\mathbf{C}G$-Moduln, invertiert von $B\mathrm{e}^s_{1,1} \longrightarrow B\mathrm{e}^s_{i,i}$, $b\,\mathrm{e}^s_{1,1} \longmapsto b\,\mathrm{e}^s_{1,i}\mathrm{e}^s_{i,i}$. ▫

Es gibt in der Aussage von Lemma 81 auch genau ein solches s; cf. Aufgabe 28.

Korollar 82 *Sei χ ein irreduzibler Charakter von G.*

Dann gibt es ein $s \in [1,t]$ mit $\chi = \chi_s$.

Insbesondere tritt der triviale Charakter von G unter den χ_s auf, $s \in [1,t]$, sodaß wir durch Umsortieren erreichen können, daß χ_1 der triviale Charakter ist; cf. Beispiel 73. Dies wollen wir fürderhin auch voraussetzen.

Beweis. Sei V ein einfacher $\mathbf{C}G$-Modul mit $\chi = \chi_V$. Sei $s \in [1,t]$ mit $V \simeq B\mathrm{e}^s_{1,1}$; cf. Lemma 81. Es ist

$$\chi \;=\; \chi_V \;\overset{\text{B. 74}}{=}\; \chi_{B\mathrm{e}^s_{1,1}} \;\overset{\text{B. 80}}{=}\; \chi_s \,.$$

▫

Korollar 83 *Jeder Charakter von G ist von der Form $\sum_{s\in[1,t]} z_s\,\chi_s$ mit $z_s \in \mathbf{Z}_{\geqslant 0}$ für $s \in [1,t]$.*

Die Koeffizienten z_s sind eindeutig bestimmt, wie wir in Bemerkung 92 unten sehen werden; cf. auch Bemerkung 94.(1).

Beweis. Jeder Charakter von G ist Summe irreduzibler nach Bemerkung 77; jeder irreduzible ist nach Korollar 82 in $\{\chi_1, \ldots, \chi_t\}$ enthalten. ▫

Lemma 84 *Die Anzahl t' der Konjugationsklassen in G ist gleich der Anzahl t direkten Faktoren in B. Kurz, es ist $t' = t$.*

Ferner ist $(\bar{g}_s)_{s\in[1,t]}$ eine $\mathbf{C}$-lineare Basis von $\mathrm{Z}(\mathbf{C}G)$.

Beweis. Es ist $\mathrm{Z}(B) = \mathrm{Z}(\prod_{s\in[1,t]} \mathbf{C}^{n_s\times n_s}) = \prod_{s\in[1,t]} \mathrm{Z}(\mathbf{C}^{n_s\times n_s}) = \prod_{s\in[1,t]} \mathbf{C}\langle \mathrm{E}_{n_s}\rangle$; cf. Aufgaben 16 und 27. Also ist $\dim_{\mathbf{C}} \mathrm{Z}(B) = t$.

Da $B \simeq \mathbf{C}G$ als $\mathbf{C}$-Algebren, ist auch $\mathrm{Z}(B) \simeq \mathrm{Z}(\mathbf{C}G)$ als $\mathbf{C}$-Algebren, und es bleibt zu zeigen, daß $\dim_{\mathbf{C}} \mathrm{Z}(\mathbf{C}G) \stackrel{!}{=} t'$.

Es ist das Tupel $(\bar{g}_r)_{r\in[1,t']}$ linear unabhängig. Bleibt zu zeigen, daß es $\mathrm{Z}(\mathbf{C}G)$ erzeugt.

Sei $\sum_{g\in G} z_g\, g \in \mathrm{Z}(\mathbf{C}G)$, wobei $z_g \in \mathbf{C}$ für $g \in G$. Sei $x \in G$. Es wird

$$\sum_{g\in G} z_g\, g \;=\; x(\sum_{g\in G} z_g\, g)x^- \;=\; \sum_{g\in G} z_g\, {}^x g \;\stackrel{h\,=\,{}^x g}{=}\; \sum_{h\in G} z_{({}^{x^-}h)}\, h\;,$$

woraus mit einem Koeffizientenvergleich $z_g = z_{({}^{x^-}g)}$ für $g,\, x \in G$ folgt. Somit ergibt sich

$$\begin{aligned}
\sum_{g\in G} z_g\, g &= \sum_{r\in[1,t']} \sum_{x\,\in\, {}^G g_r} z_x\, x \\
&= \sum_{r\in[1,t']} \sum_{x\,\in\, {}^G g_r} z_{g_r}\, x \\
&= \sum_{r\in[1,t']} z_{g_r} \sum_{x\,\in\, {}^G g_r} x \\
&= \sum_{r\in[1,t']} z_{g_r}\, \bar{g}_r \\
&\in \mathbf{C}\langle\, \bar{g}_r \,:\, r \in [1,t']\,\rangle\;.
\end{aligned}$$

□

Definition 85

Die Matrix $\mathrm{X}(G) := (\chi_s(g_r))_{s,r\in[1,t]} \in \mathbf{C}^{t\times t}$ heißt die *Charaktertafel* von G; cf. Lemma 84.

In ihren Zeilen sind also alle irreduziblen Charaktere von G anhand ihrer Werte auf Konjugationsklassenrepräsentanten aufgelistet; cf. Bemerkung 71.

In Korollar 82 wurde vereinbart, daß χ_1 der triviale Charakter ist. Also sind die Einträge der ersten Zeile der Charaktertafel alle gleich 1.

Der jeweilige Eintrag in der ersten Spalte der Charaktertafel ist $\chi_s(g_1) = \chi_s(1_G) = n_s$ für $s \in [1,t]$.

Somit hat die Charaktertafel von G die Form

$$\mathrm{X}(G) \;=\; \begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \vdots \\ \chi_t \end{array} \begin{array}{c} \begin{array}{cccc} g_1 = 1 & g_2 & \dots & g_t \end{array} \\ \begin{bmatrix} 1 & 1 & \dots & 1 \\ n_2 & * & \dots & * \\ \vdots & \vdots & & \vdots \\ n_t & * & \dots & * \end{bmatrix} \end{array}$$

Bis auf die festgelegte erste Zeile und die festgelegte erste Spalte können aber noch Zeilen- und Spaltenpermutationen auftreten.

> In Bemerkung 92 unten werden wir auch noch feststellen, daß $\mathrm{X}(G)$ regulär ist, ihre Zeilen also insbesondere paarweise verschieden sind. Zusammen mit Korollar 82 liefert dies dann die Unabhängigkeit von $\mathrm{X}(G)$ vom gewählten Wedderburnisomorphismus ω bis auf Zeilenpermutation. Insbesondere sind dann die n_s, $s \in [1,t]$, als bis auf Permutation unabhängig von der Wahl von ω erkannt.

Beispiel 86

(1) Die Charaktertafel von S_3 ist gegeben durch

$$\mathrm{X}(\mathrm{S}_3) \;=\; \begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \end{array} \begin{array}{c} \begin{array}{ccc} \mathrm{id} & (1,2) & (1,2,3) \end{array} \\ \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & 0 & -1 \end{bmatrix} \end{array} \;\in\; \mathbf{C}^{3\times 3}\,;$$

cf. Lösung zu Aufgabe 18.(1), Beispiel 73.(2), Beispiel 39.(3).

(2) Sei $n \in \mathbf{Z}_{\geqslant 1}$. Schreibe $\zeta := \zeta_n$. Die Charaktertafel von $\mathrm{C}_n = \langle\, a \,:\, a^n \,\rangle$ ist gegeben durch

$$\mathrm{X}(\mathrm{C}_n) \;=\; \begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \vdots \\ \chi_n \end{array} \begin{array}{c} \begin{array}{cccc} a^0 & a^1 & \dots & a^{n-1} \end{array} \\ \begin{bmatrix} \zeta^{0\cdot 0} & \zeta^{0\cdot 1} & \dots & \zeta^{0\cdot(n-1)} \\ \zeta^{1\cdot 0} & \zeta^{1\cdot 1} & \dots & \zeta^{1\cdot(n-1)} \\ \vdots & \vdots & & \vdots \\ \zeta^{(n-1)\cdot 0} & \zeta^{(n-1)\cdot 1} & \dots & \zeta^{(n-1)\cdot(n-1)} \end{bmatrix} \end{array} \;=\; (\zeta^{(s-1)\cdot(r-1)})_{s,r\in[1,n]} \;\in\; \mathbf{C}^{n\times n}\,;$$

cf. Beispiel 50.

(3) Genau dann sind alle Einträge der ersten Spalte der Charaktertafel von G gleich 1, wenn G abelsch ist.

Denn ist $n_j \geqslant 2$ für ein $j \in [1,t]$, dann ist der Block $\mathbf{C}^{n_j\times n_j}$ der Wedderburnzerlegung nichtkommutativ, folglich $\mathbf{C}G$ nichtkommutativ und also G nichtabelsch.

Ist umgekehrt $n_i = 1$ für alle $i \in [1,t]$, dann ist jeder Block $\mathbf{C}^{n_i\times n_i}$ der Wedderburnzerlegung kommutativ, folglich $\mathbf{C}G$ kommutativ und also G abelsch.

4.3 Orthogonalitäten

Sei G eine endliche Gruppe.

Wir verwenden Notation 78. Insbesondere schreiben wir $\mathbf{C}G \xrightarrow[\sim]{\omega} B := \prod_{s\in[1,t]} \mathbf{C}^{n_s\times n_s}$.

Lemma 87 *Sei $g \in G$. Es ist*

$$\sum_{s\in[1,t]} n_s\, \chi_s(g) \;=\; \chi_{\mathbf{C}G}(g) \;=\; \partial_{g,1}\,|G|\,.$$

Beweis. Es ist $\mathbf{C}G \xrightarrow[\sim]{\omega} B$ auch ein Isomorphismus von $\mathbf{C}G$-Moduln, denn es wird $\omega(\xi\cdot\eta) = \omega(\xi)\cdot\omega(\eta) = \xi\cdot\omega(\eta)$ für $\xi,\,\eta \in \mathbf{C}G$, wobei letzteres Produkt die vereinbarte $\mathbf{C}G$-Multiplikation auf dem $\mathbf{C}G$-Modul B bezeichnet.

Also ist $\chi_B(g) = \chi_{\mathbf{C}G}(g) = \partial_{g,1}\,|G|$; cf. Bemerkung 74, Beispiel 73.(5).

Wir wollen nun $\chi_B(g)$ noch auf eine zweite Art berechnen.

Wir haben die Zerlegung

$$B \;=\; \bigoplus_{s\in[1,t]} \bigoplus_{i\in[1,n_s]} B\mathrm{e}^s_{i,i}$$

in $\mathbf{C}G$-Teilmoduln. In $B\mathrm{e}^s_{i,i}$ wählen wir die $\mathbf{C}$-lineare Basis $(\mathrm{e}^s_{1,i}\,,\,\ldots\,,\,\mathrm{e}^s_{n_s\,,i})$. Diese Basen setzen wir zu einer Basis von B zusammen.

Da eine Zerlegung in $\mathbf{C}G$-Teilmoduln vorliegt, ergibt sich in dieser Basis die beschreibende Matrix von $B \to B,\ b \mapsto g \cdot b$ als Blockdiagonalmatrix mit den beschreibenden Matrizen $\omega^s(g)$ von $B\mathrm{e}^s_{i,i} \to B\mathrm{e}^s_{i,i}\,,\ b\,\mathrm{e}^s_{i,i} \mapsto g \cdot b\,\mathrm{e}^s_{i,i}$ in der Hauptdiagonalen, wobei $s \in [1,t]$ und $i \in [1,n_s]$; cf. Bemerkung 79.

Wir summieren über alle diese Diagonalblöcke und erhalten

$$\chi_B(g) \;=\; \mathrm{tr}(b \mapsto g \cdot b) \;=\; \sum_{s\in[1,t]} \sum_{i\in[1,n_s]} \mathrm{tr}\,\omega^s(g) \;=\; \sum_{s\in[1,t]} \sum_{i\in[1,n_s]} \chi_s(g) \;=\; \sum_{s\in[1,t]} n_s\,\chi_s(g)\,.$$

□

Bemerkung 88 *Für $s \in [1,t]$ schreiben wir*

$$\varepsilon_s \;:=\; \omega^-\Big(\sum_{i\in[1,n_s]} \mathrm{e}^s_{i,i}\Big) \;\in\; \mathbf{C}G\,.$$

Es ist $(\varepsilon_1\,,\,\ldots\,,\,\varepsilon_t)$ die orthogonale Zerlegung in primitive Idempotente in $\mathrm{Z}(\mathbf{C}G)$; cf. Aufgabe 22.

Beweis. Da ω ein Ringisomorphismus ist, genügt es zu zeigen, daß

$$(\omega(\varepsilon_s))_{s\in[1,t]} \;=\; \Big(\sum_{i\in[1,n_s]} \mathrm{e}^s_{i,i}\Big)_{s\in[1,t]}$$

die orthogonale Zerlegung in primitive Idempotente in $\omega(\mathrm{Z}(\mathbf{C}G)) = \mathrm{Z}(B)$ ist.

Es ist $\varphi \;:\; \mathbf{C}^{\times t} \longrightarrow \mathrm{Z}(B),\ (z_s)_s \longmapsto (z_s \mathrm{E}_{n_s})_s$ ein $\mathbf{C}$-Algebrenisomorphismus; cf. Aufgaben 16 und 27, Bemerkung 61.(2).

Schreibe $\eta_s := (0,\ldots,0,1,0,\ldots,0) \in \mathbf{C}^{\times t}$ mit der 1 an Position s für $s \in [1,t]$. Es genügt zu zeigen, daß

$$(\varphi^-\omega(\varepsilon_s))_{s\in[1,t]} \;=\; (\eta_s)_{s\in[1,t]}$$

die orthogonale Zerlegung in primitive Idempotente in $\mathbf{C}^{\times t}$ ist.

In der Tat liegt eine orthogonale Zerlegung in Idempotente vor. Diese sind primitiv, da $\dim_{\mathbf{C}} \mathbf{C}^{\times t}\eta_s = 1$ und folglich $\mathbf{C}^{\times t}\eta_s$ unzerlegbar ist für $s \in [1,t]$; cf. Bemerkung 55. □

Lemma 89 *Für $s \in [1,t]$ ist*

$$\varepsilon_s \;=\; \frac{n_s}{|G|} \sum_{g\in G} \chi_s(g^-)\, g \;.$$

Beweis. Schreibe $\varepsilon_s =: \sum_g z_{s,g}\, g$ für $s \in [1,t]$, wobei $z_{s,g} \in \mathbf{C}$.
Für $h \in G$ wird zum einen

$$\begin{array}{rcl} \sum_{r\in[1,t]} n_r \operatorname{tr}\big(\omega^r(\varepsilon_s \cdot h)\big) & = & \sum_r n_r \operatorname{tr}\big(\omega^r(\varepsilon_s)\cdot\omega^r(h)\big) \\ & = & \sum_r n_r \operatorname{tr}\big(\partial_{s,r}\,\omega^r(h)\big) \\ & = & n_s \operatorname{tr}\big(\omega^s(h)\big) \\ & = & n_s\,\chi_s(h)\;, \end{array}$$

zum anderen

$$\begin{array}{rcl} \sum_{r\in[1,t]} n_r \operatorname{tr}\big(\omega^r(\varepsilon_s \cdot h)\big) & = & \sum_r n_r \operatorname{tr}\big(\omega^r(\sum_g z_{s,g}\, gh)\big) \\ & = & \sum_g z_{s,g} \sum_r n_r \operatorname{tr}\big(\omega^r(gh)\big) \\ & = & \sum_g z_{s,g} \sum_r n_r\,\chi_r(gh) \\ & \overset{\text{L. 87}}{=} & \sum_g z_{s,g}\,\partial_{gh,1}|G| \\ & = & z_{s,h^-}|G|\;. \end{array}$$

Es folgt $z_{s,h^-} = \frac{n_s}{|G|}\,\chi_s(h)$, also auch $z_{s,g} = \frac{n_s}{|G|}\,\chi_s(g^-)$ für $g \in G$, wie zu zeigen war. ▫

Satz 90 (Orthogonalitäten)
Weiterhin sei G eine endliche Gruppe und Notation 78 in Verwendung.

(1) *Seien r, $s \in [1,t]$. Es gilt die* horizontale *Orthogonalität*

$$\sum_{g\in G} \chi_r(g)\,\overline{\chi_s(g)} \;=\; |G|\,\partial_{r,s}\;.$$

(2) *Seien g, $h \in G$. Es gilt die* vertikale *Orthogonalität*

$$\sum_{s\in[1,t]} \chi_s(g)\,\overline{\chi_s(h)} \;=\; \partial_{C_g,C_h}|G|\,|{}^Gg|^{-1} \;=\; \partial_{C_g,C_h}|\mathrm{C}_G(g)|\;.$$

Beweis.
Zu (1). Für r, $s \in [1,t]$ wird zum einen

$$\begin{array}{rcl} \varepsilon_s\,\varepsilon_r & \overset{\text{B. 88}}{=} & \partial_{r,s}\,\varepsilon_s \\ & \overset{\text{L. 89}}{=} & \partial_{r,s}\,\frac{n_s}{|G|}\sum_x \chi_s(x^-)x\;, \end{array}$$

zum anderen

$$\begin{aligned}\varepsilon_s\,\varepsilon_r &\overset{\text{L. 89}}{=} \big(\tfrac{n_s}{|G|}\textstyle\sum_g \chi_s(g^-)g\big)\big(\tfrac{n_r}{|G|}\sum_h \chi_r(h^-)h\big)\\ &= \tfrac{n_s\,n_r}{|G|^2}\textstyle\sum_x \big(\sum_{gh=x}\,\chi_s(g^-)\,\chi_r(h^-)\big)x\ .\end{aligned}$$

Koeffizientenvergleich bei $x = 1$ liefert

$$\partial_{r,s}\,\frac{n_s^2}{|G|} \;=\; \frac{n_s\,n_r}{|G|^2}\sum_g \chi_s(g^-)\chi_r(g)\ ,$$

i.e. $|G|\partial_{r,s} = \sum_g \chi_r(g)\,\chi_s(g^-)$.

Die Aussage folgt nun wegen $\chi_s(g^-) = \overline{\chi_s(g)}$; cf. Aufgabe 25.(2).

Zu (2). Wir erinnern an die Charaktertafel $X := \mathrm{X}(G) = (\chi_r(g_s))_{r,s} \in \mathbf{C}^{t\times t}$; cf. Definition 85. Sei

$$Y \;:=\; |G|^{-1/2}X\begin{pmatrix}|{}^Gg_1|^{1/2} & & \\ & \ddots & \\ & & |{}^Gg_t|^{1/2}\end{pmatrix}\ .$$

Die Aussage (1) bedeutet, daß $\sum_{q\in[1,t]} |{}^Gg_q|\,\chi_r(g_q)\,\overline{\chi_s(g_q)} \;=\; |G|\,\partial_{r,s}$ ist für $r,\ s \in [1,t]$, i.e. daß

$$\mathrm{E}_t \;=\; |G|^{-1}X\begin{pmatrix}|{}^Gg_1| & & \\ & \ddots & \\ & & |{}^Gg_t|\end{pmatrix}\bar{X}^{\mathrm{t}} \;=\; Y\bar{Y}^{\mathrm{t}}$$

ist, i.e. daß Y unitär ist. Vertauschung der Faktoren gibt

$$\mathrm{E}_t \;=\; \bar{Y}^{\mathrm{t}}Y \;=\; |G|^{-1}\begin{pmatrix}|{}^Gg_1|^{1/2} & & \\ & \ddots & \\ & & |{}^Gg_t|^{1/2}\end{pmatrix}\bar{X}^{\mathrm{t}}X\begin{pmatrix}|{}^Gg_1|^{1/2} & & \\ & \ddots & \\ & & |{}^Gg_t|^{1/2}\end{pmatrix}\ ,$$

i.e.

$$\bar{X}^{\mathrm{t}}X \;=\; |G|\begin{pmatrix}|{}^Gg_1|^{-1} & & \\ & \ddots & \\ & & |{}^Gg_t|^{-1}\end{pmatrix}\ ,$$

i.e.

$$\sum_q \overline{\chi_q(g_r)}\,\chi_q(g_s) \;=\; \partial_{r,s}|G||{}^Gg_r|^{-1}$$

für $r,\ s \in [1,t]$, i.e.

$$\sum_q \chi_q(g)\,\overline{\chi_q(h)} \;=\; \partial_{{}^Gg,{}^Gh}|G||{}^Gg|^{-1} \overset{\text{L. 5}}{=} \partial_{{}^Gg,{}^Gh}|\mathrm{C}_G(g)|$$

für $g,\ h \in G$. □

Es ist Lemma 87 ein Spezialfall von Satz 90.(2).

Definition 91

(1) Eine Abbildung $f : G \longrightarrow \mathbf{C}$ heißt eine *Klassenfunktion* auf G, wenn $f(g) = f({}^x g)$ ist für $g,\, x \in G$, wenn also f konstant auf Konjugationsklassen ist.

E.g. ist jeder Charakter von G eine Klassenfunktion auf G; cf. Bemerkung 71.

Die Menge $\mathrm{Kf}(G)$ der Klassenfunktionen auf G ist ein $\mathbf{C}$-Unterraum des Raums aller $\mathbf{C}$-wertigen Funktionen auf G.

Da $(\, (G \to \mathbf{C}, h \mapsto \partial_{{}^G h, {}^G g_r}) : r \in [1,t]\,)$ eine Basis von $\mathrm{Kf}(G)$ ist, ist $\dim_{\mathbf{C}} \mathrm{Kf}(G) = t$.

(2) Wir definieren das hermitesche Skalarprodukt

$$\begin{array}{ccccc} \mathrm{Kf}(G) & \times & \mathrm{Kf}(G) & \stackrel{{}_G(-,=)}{\longrightarrow} & \mathbf{C} \\ (\varphi & , & \psi) & \longmapsto & {}_G(\varphi,\psi) := |G|^{-1} \sum_{g\in G} \varphi(g)\,\overline{\psi(g)}\,. \end{array}$$

Bemerkung 92

(1) Es besagt Satz 90.(1) gerade, daß ${}_G(\chi_r\,, \chi_s) = \partial_{r,s}$ ist für $r,\, s \in [1,t]$.

Mit anderen Worten, es ist $(\chi_1\,, \ldots, \chi_t)$ eine Orthonormalbasis des $\mathbf{C}$-Vektorraums der Klassenfunktionen bezüglich ${}_G(-,=)$.

Insbesondere ist die Charaktertafel $\mathrm{X}(G)$ eine invertierbare Matrix.

(2) Für praktische Zwecke beachte, daß wir für $\varphi,\, \psi \in \mathrm{Kf}(G)$

$$\begin{array}{rcl} {}_G(\varphi,\psi) & = & |G|^{-1} \sum_{g\in G} \varphi(g)\,\overline{\psi(g)} \\ & = & |G|^{-1} \sum_{r\in[1,t]} |{}^G g_r|\, \varphi(g_r)\,\overline{\psi(g_r)} \\ & \stackrel{\text{L. 5}}{=} & \sum_{r\in[1,t]} |\mathrm{C}_G(g_r)|^{-1}\, \varphi(g_r)\,\overline{\psi(g_r)} \end{array}$$

erhalten.

(3) Für $\varphi,\, \psi \in \mathrm{Kf}(G)$ ist ${}_G(\varphi,\psi) = \overline{{}_G(\psi,\varphi)}$.

Beispiel 93

(1) Die Charaktertafel von S_3 ist gegeben durch

$$\mathrm{X}(\mathrm{S}_3) = \begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \end{array} \begin{array}{c} \begin{array}{ccc} \mathrm{id} & (1,2) & (1,2,3) \\ 1 & 3 & 2 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & 0 & -1 \end{bmatrix} \end{array},$$

wobei direkt unter den Konjugationsklassenrepräsentanten die Länge ihrer Konjugationsklassen notiert wurde; cf. Beispiel 86.(1).

Es wird e.g. ${}_{\mathrm{S}_3}(\chi_2\,,\chi_3) = \frac{1}{6}(1\cdot 1\cdot 2 + 3\cdot(-1)\cdot 0 + 2\cdot 1\cdot(-1)) = 0$ und ${}_{\mathrm{S}_3}(\chi_3\,,\chi_3) = \frac{1}{6}(1\cdot 2\cdot 2 + 3\cdot 0\cdot 0 + 2\cdot(-1)\cdot(-1)) = 1$.

Es wird e.g. $\sum_{s\in[1,3]} \chi_s((1,2))\,\overline{\chi_s((1,2,3))} = (1\cdot 1 + (-1)\cdot 1 + 0\cdot(-1)) = 0$ und $\sum_{s\in[1,3]} \chi_s((1,2))\,\overline{\chi_s((1,2))} = 1\cdot 1 + (-1)\cdot(-1) + 0\cdot 0 = 2 = |\mathrm{S}_3|\,|^{\mathrm{S}_3}(1,2)|^{-1} = |\mathrm{C}_{\mathrm{S}_3}((1,2))|$.

(2) Sei $n \geqslant 1$. Schreibe $\zeta := \zeta_n$.

Die Charaktertafel von C_n ist gegeben durch $\mathrm{X}(\mathrm{C}_n) = (\zeta^{(s-1)(r-1)})_{s,r\in[1,n]}$.

Die horizontale Orthogonalität wird für $r,\, s \in [1,n]$ zu

$$\begin{aligned} {}_{\mathrm{C}_n}(\chi_r\,,\chi_s) &= |\mathrm{C}_n|^{-1} \textstyle\sum_{q\in[1,n]} |{}^G g_q|\, \chi_r(g_q)\, \overline{\chi_s(g_q)} \\ &= n^{-1} \textstyle\sum_{q\in[1,n]} 1\cdot \zeta^{(r-1)(q-1)}\cdot \zeta^{-(s-1)(q-1)} \\ &= n^{-1} \textstyle\sum_{q\in[1,n]} \zeta^{(r-s)(q-1)} \;=\; \partial_{r,s}\;; \end{aligned}$$

cf. Beispiel 86.(2), Lösung zu Aufgabe 17.

(3) Allgemein ist $\sum_{s\in[1,t]} |\chi_s(g)|^2 = |\mathrm{C}_G(g)|$ für $g \in G$. Insbesondere ist

$$\textstyle\sum_{s\in[1,t]} n_s^2 \;=\; \sum_{s\in[1,t]} |\chi_s(1)|^2 \;=\; |\mathrm{C}_G(1)| \;=\; |G|\;.$$

Cf. Satz 90.(2). Dies folgt auch durch Dimensionsvergleich aus dem Wedderburnisomorphismus.

Bemerkung 94 *Sei* $\varphi \in \mathrm{Kf}(G)$.

(1) *Es ist* $\varphi = \sum_{s\in[1,t]} {}_G(\varphi,\chi_s)\chi_s$.

Es ist φ *genau dann ein Charakter, wenn* ${}_G(\varphi,\chi_s) \in \mathbf{Z}_{\geqslant 0}$ *ist für alle* $s \in [1,t]$.

(2) *Ist* φ *ein Charakter, so ist* φ *genau dann irreduzibel, wenn* ${}_G(\varphi,\varphi) = 1$, *i.e. wenn* $\sum_{g\in G} |\varphi(g)|^2 = |G|$.

Beweis.

Zu (1). Schreibe $\varphi = \sum_{s\in[1,t]} z_s\,\chi_s$ mit $z_s \in \mathbf{C}$. Für $r \in [1,t]$ wird

$${}_G(\varphi,\chi_r) \;=\; {}_G(\textstyle\sum_s z_s\,\chi_s\,,\chi_r) = \sum_s z_s\, {}_G(\chi_s\,,\chi_r) \;=\; \sum_s z_s\,\partial_{s,r} \;=\; z_r\;.$$

Die zweite Aussage folgt nun aus Bemerkung 75, Bemerkung 77, Korollar 82 und Bemerkung 92.(1).

Zu (2). Schreibe $\varphi = \sum_{s\in[1,t]} z_s\,\chi_s$ mit $z_s \in \mathbf{Z}_{\geqslant 0}$; cf. (1). Es ist φ genau dann irreduzibel, wenn $\varphi \in \{\,\chi_s \,:\, s\in[1,t]\,\}$. Wegen

$${}_G(\varphi,\varphi) = {}_G(\textstyle\sum_s z_s\,\chi_s\,,\sum_r z_r\,\chi_r) = \sum_{s,r} z_s\,z_r\cdot {}_G(\chi_s\,,\chi_r) \;=\; \sum_{s,r} z_s\,z_r\,\partial_{s,r} \;=\; \sum_s z_s^2$$

ist dies genau dann der Fall, wenn ${}_G(\varphi,\varphi) = 1$ ist. ▫

Bemerkung 95 *Seien V und W endlichdimensionale $\mathbf{C}G$-Moduln.*

(1) *Es ist* ${}_G(\chi_V, \chi_W) = \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}G}(V, W) \in \mathbf{Z}_{\geqslant 0}$.
Insbesondere ist ${}_G(\varphi, \psi) = {}_G(\psi, \varphi)$ *für Charaktere* φ *und* ψ *von* G*; cf. Bemerkung* 92.(3).

(2) *Es ist* $V \simeq W$ *genau dann, wenn* $\chi_V = \chi_W$.

Cf. Bemerkung 74.

Beweis.

Zu (1). Da für endlichdimensionale $\mathbf{C}G$-Moduln W' und W'' zum einen ${}_G(\chi_V, \chi_{W' \oplus W''}) = {}_G(\chi_V, \chi_{W'} + \chi_{W''}) = {}_G(\chi_V, \chi_{W'}) + {}_G(\chi_V, \chi_{W''})$, zum anderen $\dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}G}(V, W' \oplus W'') = \dim_{\mathbf{C}}(\mathrm{Hom}_{\mathbf{C}G}(V, W') \oplus \mathrm{Hom}_{\mathbf{C}G}(V, W'')) = \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}G}(V, W') + \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}G}(V, W'')$ ist, können wir annehmen, daß W einfach ist; cf. Bemerkungen 75 und 77.

Genauso können wir annehmen, daß V einfach ist.

Wir finden $r, s \in [1, t]$ mit $V \simeq B\mathrm{e}^r_{1,1}$ und $W \simeq B\mathrm{e}^s_{1,1}$; cf. Lemma 81.

Wir erhalten

$$\begin{array}{rcl} {}_G(\chi_V, \chi_W) & \overset{\text{B. 74}}{=} & {}_G(\chi_{B\mathrm{e}^r_{1,1}}, \chi_{B\mathrm{e}^s_{1,1}}) \\ & \overset{\text{B. 80}}{=} & {}_G(\chi_r, \chi_s) \\ & \overset{\text{B. 92.(1)}}{=} & \partial_{r,s} \\ & \overset{\text{L. 66.(2,4), A. 28}}{=} & \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}G}(B\mathrm{e}^r_{1,1}, B\mathrm{e}^s_{1,1}) \\ & \overset{\text{Komp. m. Isom.}}{=} & \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}G}(V, W)\ . \end{array}$$

Zu (2). Sind V und W isomorph, so ist $\chi_V = \chi_W$; cf. Bemerkung 74.

Sei umgekehrt $\chi_V = \chi_W$. Für $s \in [1, t]$ finden wir $x_s, y_s \in \mathbf{Z}_{\geqslant 0}$ mit $V \simeq \bigoplus_s (B\mathrm{e}^s_{1,1})^{\oplus x_s}$ und $W \simeq \bigoplus_s (B\mathrm{e}^s_{1,1})^{\oplus y_s}$; cf. Bemerkung 77, Lemma 81. Wir haben zu zeigen, daß $x_s \overset{!}{=} y_s$ für $s \in [1, t]$. Aber es wird

$$\begin{array}{rcl} \sum_s x_s \chi_s & \overset{\text{B. 80}}{=} & \sum_s x_s \chi_{B\mathrm{e}^s_{1,1}} \\ & \overset{\text{B. 75}}{=} & \chi_{\bigoplus_s (B\mathrm{e}^s_{1,1})^{\oplus x_s}} \\ & \overset{\text{B. 74}}{=} & \chi_V \\ & = & \chi_W \\ & \overset{\text{B. 74}}{=} & \chi_{\bigoplus_s (B\mathrm{e}^s_{1,1})^{\oplus y_s}} \\ & \overset{\text{B. 75}}{=} & \sum_s y_s \chi_{B\mathrm{e}^s_{1,1}} \\ & \overset{\text{B. 80}}{=} & \sum_s y_s \chi_s\ . \end{array}$$

Das Resultat folgt nun aus der Regularität der Charaktertafel; cf. Bemerkung 92.(1). ▫

4.4 Der Grad eines irreduziblen Charakters teilt die Gruppenordnung

Sei G eine endliche Gruppe.

Wir verwenden Notation 78.

Da ω ein Ringisomorphismus ist, ist

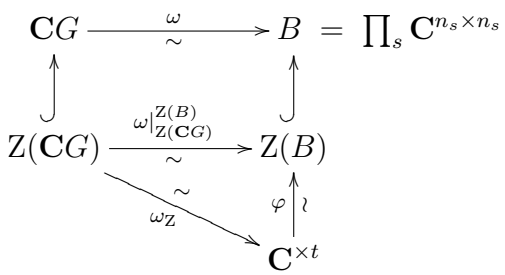
$$\omega(\mathrm{Z}(\mathbf{C}G)) \;=\; \mathrm{Z}(B) \;\overset{\text{A.27}}{=}\; \prod_s \mathrm{Z}(\mathbf{C}^{n_s\times n_s}) \;\overset{\text{A.16}}{=}\; \prod_s \mathbf{C}\langle \mathrm{E}_{n_s}\rangle \;.$$

Es ist

$$\begin{array}{ccc} \mathbf{C}^{\times t} & \xrightarrow[\sim]{\varphi} & \mathrm{Z}(B) \\ (z_s)_s & \longmapsto & (z_s \mathrm{E}_{n_s})_s \end{array}$$

ein Isomorphismus von $\mathbf{C}$-Algebren; cf. Aufgaben 27 und 16.

Setzen wir noch $\omega_{\mathrm{Z}} := \varphi^- \circ \omega|^{\mathrm{Z}(B)}_{\mathrm{Z}(\mathbf{C}G)}$, so sind wir folgender Situation.



Es ist ω_{Z} ein Isomorphismus von $\mathbf{C}$-Algebren.

Schreibe $\omega_{\mathrm{Z}}(\xi) =: (\omega^s_{\mathrm{Z}}(\xi))_s \in \mathbf{C}^{\times t}$ für $\xi \in \mathrm{Z}(\mathbf{C}G)$. Also wird

$$(\omega^s(\xi))_s \;=\; \omega(\xi) \;=\; \varphi\big(\omega_{\mathrm{Z}}(\xi)\big) \;=\; \varphi\big((\omega^s_{\mathrm{Z}}(\xi))_s\big) \;=\; (\omega^s_{\mathrm{Z}}(\xi)\mathrm{E}_{n_s})_s \;,$$

i.e. $\omega^s(\xi) = \omega^s_{\mathrm{Z}}(\xi)\mathrm{E}_{n_s}$ für $\xi \in \mathrm{Z}(\mathbf{C}G)$ und $s \in [1,t]$.

Bemerkung 96 (und Definition) *Es ist*

$$\beta_{r,s} \;:=\; \omega^r_{\mathrm{Z}}(\bar{g}_s) \;=\; \chi_r(g_s)\cdot\frac{|^G g_s|}{n_r}$$

für r, $s \in [1,t]$; cf. Definition 85.

Insbesondere ist $\beta_{r,1} = 1$ für $r \in [1,t]$, sowie $\beta_{1,s} = |^G g_s|$ für $s \in [1,t]$.

Beweis. Es ist

$$\begin{array}{rcl} \chi_r(g_s)\cdot|^G g_s| & = & \sum_{x\in {}^G g_s}\chi_r(x) \\ & = & \sum_{x\in {}^G g_s}\operatorname{tr}\omega^r(x) \\ & = & \operatorname{tr}\omega^r(\bar{g}_s) \\ & = & \operatorname{tr}(\omega^r_{\mathrm{Z}}(\bar{g}_s)\mathrm{E}_{n_r}) \\ & = & n_r\,\omega^r_{\mathrm{Z}}(\bar{g}_s)\;. \end{array}$$

□

Definition 97 Seien $r,\, s \in [1,t]$. Da $\bar{g}_r\,,\, \bar{g}_s \in \mathrm{Z}(\mathbf{C}G)$ ist, ist auch $\bar{g}_r \cdot \bar{g}_s \in \mathrm{Z}(\mathbf{C}G)$. Da $(\bar{g}_a)_a$ eine Basis von $\mathrm{Z}(\mathbf{C}G)$ ist, können wir

$$\bar{g}_r \cdot \bar{g}_s \;=:\; \sum_{a\in[1,t]} \gamma_{r,s,a}\, \bar{g}_a$$

setzen, mit eindeutig bestimmten $\gamma_{r,s,a} \in \mathbf{C}$; cf. Lemma 84.

Bemerkung 98 *Seien $r,\, s,\, a \in [1,t]$. Es ist*

$$\gamma_{r,s,a} \;=\; |\{\, (x,y) \in {}^{G}g_r \times {}^{G}g_s \,:\, xy = g_a \,\}| \;\in\; \mathbf{Z}_{\geqslant 0}\;.$$

Beweis. Es wird

$$\begin{array}{rcl} \bar{g}_r \cdot \bar{g}_s & = & (\sum_{x\,\in\, {}^{G}g_r} x)(\sum_{y\,\in\, {}^{G}g_s} y) \\ & = & \sum_{(x,y)\,\in\, {}^{G}g_r \times {}^{G}g_s} xy \\ & = & \sum_{h\in G} |\{\, (x,y) \,\in\, {}^{G}g_r \times {}^{G}g_s \,:\, xy = h \,\}|\; h\;. \end{array}$$

Also ist der Koeffizient von g_a in $\bar{g}_r \cdot \bar{g}_s$ gleich $|\{\, (x,y) \,\in\, {}^{G}g_r \times {}^{G}g_s \,:\, xy = g_a \,\}|$.

Dies ist auch der Koeffizient $\gamma_{r,s,a}$ von $\bar{g}_a$ in $\bar{g}_r \cdot \bar{g}_s$, da in der Basis $(\,\bar{g}_a \,:\, a \in [1,t]\,)$ von $\mathrm{Z}(\mathbf{C}G)$ das Element g_a nur in $\bar{g}_a$ auftritt, und dort mit Koeffizient 1. ▫

Bemerkung 99 *Seien $q, r \in [1,t]$.*

Für $s \in [1,t]$ wird

$$\beta_{q,r}\, \beta_{q,s} \;=\; \sum_{a\in[1,t]} \gamma_{r,s,a}\, \beta_{q,a}\;.$$

Als Matrixgleichung geschrieben besagt dies

$$\beta_{q,r}\, (\beta_{q,s})_s \;=\; (\gamma_{r,s,a})_{s,a}\, (\beta_{q,a})_a\;.$$

Da $\beta_{q,1} \overset{\text{B. 96}}{=} 1 \neq 0$ ist, hat also $(\gamma_{r,s,a})_{s,a} \in \mathbf{C}^{t\times t}$ den Eigenvektor $(\beta_{q,a})_a \in \mathbf{C}^{t\times 1}$ zum Eigenwert $\beta_{q,r} \in \mathbf{C}$.

Beweis. Es wird

$$\begin{array}{rcl} \beta_{q,r}\, \beta_{q,s} & = & \omega^q_{\mathrm{Z}}(\bar{g}_r)\, \omega^q_{\mathrm{Z}}(\bar{g}_s) \\ & = & \omega^q_{\mathrm{Z}}(\bar{g}_r\, \bar{g}_s) \\ & \overset{\text{D. 97}}{=} & \omega^q_{\mathrm{Z}}\big(\sum_{a\in[1,t]} \gamma_{r,s,a}\, \bar{g}_a\big) \\ & = & \sum_{a\in[1,t]} \gamma_{r,s,a}\, \omega^q_{\mathrm{Z}}(\bar{g}_a) \\ & = & \sum_{a\in[1,t]} \gamma_{r,s,a}\, \beta_{q,a}\;. \end{array}$$

▫

Definition 100 Sei $\mathcal{O} := \{ z \in \mathbf{C} : \text{es gibt } f(X) \in \mathbf{Z}[X] \text{ normiert mit } f(z) = 0 \} \subseteq \mathbf{C}$.

Es ist $\mathcal{O} \subseteq \mathbf{C}$ ein Teilring; cf. Aufgabe 29.(2).

Es heißt $\mathcal{O}$ der *Ring der algebraisch ganzen Zahlen in* $\mathbf{C}$.

Es ist $\mathcal{O} \cap \mathbf{Q} = \mathbf{Z}$; cf. Aufgabe 29.(3).

Es ist e.g. für $k \in \mathbf{Z}_{\geqslant 1}$ und $i \in [0, k-1]$ das Element ζ_k^i in $\mathcal{O}$, als Nullstelle des normierten Polynoms $X^k - 1 \in \mathbf{Z}[X]$.

Bemerkung 101 *Es ist* $\beta_{q,r} \in \mathcal{O}$ *für* $q, r \in [1, t]$.

Beweis. Es ist $\beta_{q,r} \in \mathbf{C}$ der Eigenwert einer Matrix mit ganzzahligen Einträgen, also die Nullstelle eines charakteristischen Polynoms mit ganzzahligen Koeffizienten; cf. Bemerkungen 99 und 98. □

Satz 102 (Grad eines irreduziblen Charakters teilt Gruppenordnung)
Sei χ *ein irreduzibler Charakter der endlichen Gruppe* G.

Es ist der Charaktergrad $\chi(1)$ *ein Teiler der Gruppenordnung* $|G|$.

Beweis. Es gibt ein $s \in [1, t]$ mit $\chi = \chi_s$; cf. Korollar 82.

Wir haben zu zeigen, daß n_s ein Teiler von $|G|$ ist.

Es ist $|G| n_s^{-1} \in \mathbf{Q}$.

Da $\mathbf{Z} = \mathcal{O} \cap \mathbf{Q}$ ist, bleibt zu zeigen, daß $|G| n_s^{-1} \overset{!}{\in} \mathcal{O}$ ist; cf. Aufgabe 29.(3).

Aus $\zeta_{|\langle g_r \rangle|} \in \mathcal{O}$ folgt, daß $\overline{\chi_s(g_r)} \in \mathcal{O}$ liegt für $r \in [1, t]$, da $\mathcal{O} \subseteq \mathbf{C}$ ein unter Konjugation abgeschlossener Teilring ist; cf. Aufgaben 25.(1, 2) und 29.(2); beachte, daß aus $f(z) = 0$ auch $f(\bar{z}) = \overline{f(z)} = 0$ folgt für $z \in \mathbf{C}$ und $f(X) \in \mathbf{Z}[X]$ normiert.

Es ist

$$\begin{aligned} |G| n_s^{-1} &\overset{\text{S. 90.(1)}}{=} n_s^{-1} \textstyle\sum_g \chi_s(g) \, \overline{\chi_s(g)} \\ &= n_s^{-1} \textstyle\sum_r |{}^G g_r| \, \chi_s(g_r) \, \overline{\chi_s(g_r)} \\ &\overset{\text{B. 96}}{=} \textstyle\sum_r \beta_{s,r} \, \overline{\chi_s(g_r)} \\ &\overset{\text{B. 101}}{\in} \mathcal{O} \, . \end{aligned}$$

□

Korollar 103 *Sei* M *ein einfacher* $\mathbf{C}G$*-Modul.*

Es teilt $\dim_{\mathbf{C}} M$ *die Gruppenordnung* $|G|$.

Beweis. Es ist $\dim_{\mathbf{C}} M = \chi_M(1)$; cf. Bemerkung 72. Da M einfach ist, ist χ_M irreduzibel; cf. Definition 76. Also ist $\chi_M(1)$ ein Teiler von $|G|$; cf. Satz 102. □

Beispiel 104 Sei p eine Primzahl. Sei G eine Gruppe von Ordnung $|G| = p^2$. Wir können nun nochmals die bereits in der Lösung zu Aufgabe 13 angemerkte Tatsache zeigen, daß G abelsch ist. Wir verwenden Notation 78 sinngemäß.

Annahme, es ist G nichtabelsch. Es ist also $n_r \geqslant 2$ für ein $r \in [1,t]$, und somit $n_r \in \{p, p^2\}$ nach Satz 102. Da $\sum_{s\in[1,t]} n_s^2 = |G| = p^2$ und da $n_1 = 1$, ist $n_r^2 < p^2$. Dies ist aber für keinen der beiden Kandidaten erfüllt. Wir haben einen *Widerspruch.*

4.5 Konjugation und Produkte

Sei G eine endliche Gruppe.

4.5.1 Konjugation

Definition 105 Ist $\varphi \in \mathrm{Kf}(G)$, so definieren wir die *(komplex) konjugierte Klassenfunktion* $\bar\varphi \in \mathrm{Kf}(G)$ durch

$$\bar\varphi(g) \;:=\; \overline{\varphi(g)}$$

für $g \in G$.

Lemma 106 *Sei M ein endlichdimensionaler $\mathbf{C}G$-Modul.*

Es trägt $M^* := \mathrm{Hom}_{\mathbf{C}}(M, \mathbf{C})$ eine $\mathbf{C}G$-Modulstruktur via

$$(g \cdot f)(m) \;:=\; f(g^- m)$$

für $g \in G$, $f \in M^*$ und $m \in M$.

Ist M einfach, dann auch M^*.

Es ist $\chi_{M^*}(g) = \overline{\chi_M(g)}$ für $g \in G$. I.e. es ist $\chi_{M^*} = \overline{\chi_M}$.

Ist χ ein Charakter von G, dann ist auch $\bar\chi$ ein Charakter von G.

Ist χ ein irreduzibler Charakter von G, dann ist auch $\bar\chi$ ein irreduzibler Charakter von G.

Beweis. Siehe Aufgabe 25.(3) und Lösung.

Alternativ folgt aus der Irreduzibilität von χ, daß

$$1 \;=\; {}_G(\chi\,,\chi) \;=\; \frac{1}{|G|}\sum_g \chi(g)\,\bar\chi(g) \;=\; \frac{1}{|G|}\sum_g \bar\chi(g)\,\chi(g) \;=\; {}_G(\bar\chi\,,\bar\chi)$$

i.e. die Irreduzibilität von $\bar\chi$; cf. Bemerkung 94.(2). □

Beispiel 107 Für $G = \mathrm{C}_n$ operiert die komplexe Konjugation auf der Charaktertafel $\mathrm{X}(\mathrm{C}_n)$ in der Anordnung von Beispiel 86.(2) via

$$\begin{array}{rcl} \bar\chi_1 & = & \chi_1 \\ \bar\chi_i & = & \chi_{n+2-i} \quad \text{für } i \in [2,n] \end{array}$$

4.5.2 Produkte

Definition 108 Sind $\varphi, \varphi' \in \mathrm{Kf}(G)$, so definieren wir ihr *Produkt* $\varphi \cdot \varphi' \in \mathrm{Kf}(G)$ durch

$$(\varphi \cdot \varphi')(g) \ := \ \varphi(g) \cdot \varphi'(g)$$

für $g \in G$.

Notation 109 Seien V und W zwei $\mathbf{C}$-Moduln, i.e. $\mathbf{C}$-Vektorräume.

Via $v \cdot z := zv$ für $z \in \mathbf{C}$ und $v \in V$ wird V zu einem $\mathbf{C}$-Rechtsmodul.

Insgesamt können und werden wir V bei Bedarf kommentarlos als $\mathbf{C}$-$\mathbf{C}$-Bimodul verwenden.

Wir schreiben

$$V \otimes W \ := \ V \underset{\mathbf{C}}{\otimes} W \ ,$$

und dies ist wieder ein $\mathbf{C}$-Vektorraum; cf. Aufgabe 26.(2).

Ist e.g. M ein $\mathbf{C}G$-Modul, so wird aus diesem durch Einschränkung ein $\mathbf{C}$-Vektorraum und dann mittels unserer Konvention ein $\mathbf{C}$-$\mathbf{C}$-Bimodul.

Lemma 110 *Seien M und N endlichdimensionale $\mathbf{C}G$-Moduln.*

Es trägt $M \otimes N$ eine $\mathbf{C}G$-Modulstruktur via

$$g \cdot (m \otimes n) \ := \ (gm) \otimes (gn)$$

für $g \in G$, $m \in M$ und $n \in N$.

Es ist $\chi_{M\otimes N}(g) = \chi_M(g) \cdot \chi_N(g)$ für $g \in G$. I.e. es ist $\chi_{M\otimes N} = \chi_M \cdot \chi_N$.

Sind χ und ψ Charaktere von G, dann ist auch $\chi \cdot \psi$ ein Charakter von G.

Beweis. Sei $g \in G$. Wir haben auf dem $\mathbf{C}$-Vektorraum $M \otimes N$ die Abbildung

$$\begin{array}{ccccc} M & \otimes & N & \xrightarrow{g\cdot(-)} & M & \otimes & N \\ m & \otimes & n & \longmapsto & (gm) & \otimes & (gn) \ , \end{array}$$

da $(gm) \otimes (gn)$ additiv in m und n ist und da

$$(g(mz)) \otimes (gn) \ = \ (gm)z \otimes (gn) \ = \ (gm) \otimes z(gn) \ = \ (gm) \otimes g(zn) \ ,$$

wobei $g \in G$, $m \in M$, $n \in N$ und $z \in \mathbf{C}$.

Dies liefert eine Darstellung $G \longrightarrow \mathrm{GL}(M \otimes N)$, $g \longmapsto g \cdot (-)$, da sich für $g, \tilde{g} \in G$

$$\begin{array}{rcl} (g\tilde{g}) \cdot (\sum_{(m,n)} z_{(m,n)}\, m \otimes n) & = & \sum_{(m,n)} z_{(m,n)}\, ((g\tilde{g})m) \otimes ((g\tilde{g})n) \\ & = & \sum_{(m,n)} z_{(m,n)}\, (g(\tilde{g}m)) \otimes (g(\tilde{g}n)) \\ & = & g \cdot (\sum_{(m,n)} z_{(m,n)}\, (\tilde{g}m) \otimes (\tilde{g}n)) \\ & = & g \cdot (\tilde{g} \cdot (\sum_{(m,n)} z_{(m,n)}\, m \otimes n)) \end{array}$$

ergibt, wobei $z_{(m,n)} \in \mathbf{Z}$ für $(m,n) \in M \times N$.

Somit verfügen wir auch über den zugehörigen $\mathbf{C}G$-Modul $M \otimes N$; cf. Lemma 44.

Sei $(m_1, \ldots, m_k)$ eine $\mathbf{C}$-lineare Basis von M. Sei $(n_1, \ldots, n_\ell)$ eine $\mathbf{C}$-lineare Basis von N.

Als $\mathbf{C}$-Vektorräume ist

$$\begin{array}{rccccccc} M \otimes N & \xleftarrow{\sim} & \mathbf{C}^{\oplus k} & \otimes & \mathbf{C}^{\oplus \ell} & \xrightarrow{\sim} & ((\mathbf{C} \otimes \mathbf{C})^{\oplus k})^{\oplus \ell} & \xrightarrow{\sim} & \mathbf{C}^{k \times \ell} \\ \sum_{i,j} z_i\, w_j\, m_i \otimes n_j & \longmapsfrom & (z_i)_i & \otimes & (w_j)_j & \longmapsto & ((z_i \otimes w_j)_i)_j & \longmapsto & (z_i w_j)_{i,j}\ , \end{array}$$

wobei der erste Isomorphismus mit der Lösung zu Aufgabe 26.(5) aus den Isomorphismen $M \xleftarrow{\sim} \mathbf{C}^{\oplus k}$, $\sum_i z_i\, m_i \longmapsfrom (z_i)_i$ und $N \xleftarrow{\sim} \mathbf{C}^{\oplus \ell}$, $\sum_j w_j\, n_j \longmapsfrom (w_j)_j$ konstruiert werden kann; der zweite folgt aus Aufgabe 26.(5), der dritte aus Aufgabe 26.(3).

Insgesamt korrespondiert $m_i \otimes n_j$ zu $\mathrm{e}_{i,j}$ für $i \in [1,k]$ und $j \in [1,\ell]$, sodaß $(m_i \otimes n_j)_{i,j}$ eine $\mathbf{C}$-lineare Basis von $M \otimes N$ ist.

Sei $g \in G$.

Sei $gm_i = \sum_a z_{a,i}\, m_a$ für $i \in [1,k]$, wobei $z_{a,i} \in \mathbf{C}$ stets.

Sei $gn_j = \sum_b w_{b,j}\, n_b$ für $j \in [1,\ell]$, wobei $w_{b,j} \in \mathbf{C}$ stets.

Es wird

$$g(m_i \otimes n_j) \;=\; (gm_i) \otimes (gn_j) \;=\; \textstyle\sum_{a,b} z_{a,i}\, w_{b,j}\, m_a \otimes n_b\ ,$$

und der Koeffizient von $m_i \otimes n_j$ darin gleich $z_{i,i}\, w_{j,j}$, wobei $i \in [1,k]$ und $j \in [1,\ell]$.

Folglich wird die Spur der Multiplikationsabbildung $g \cdot (-) : M \otimes N \longrightarrow M \otimes N$ gleich

$$\chi_{M \otimes N}(g) \;=\; \textstyle\sum_{i,j} z_{i,i}\, w_{j,j} \;=\; (\sum_i z_{i,i}) \cdot (\sum_j w_{j,j}) \;=\; \chi_M(g) \cdot \chi_N(g)\ .$$

□

Beispiel 111 Sei $G = \mathrm{S}_3$. Wir verwenden die Notation von Beispiel 93.(1).

Es ist $\chi_3 = (2\ 0\ {-1})$.

Es wird $\chi_3 \cdot \chi_3 = (2\ 0\ {-1}) \cdot (2\ 0\ {-1}) = (4\ 0\ 1) = (1\ 1\ 1) + (1\ {-1}\ 1) + (2\ 0\ {-1}) = \chi_1 + \chi_2 + \chi_3$.

Insbesondere ist das Produkt zweier irreduzibler Charaktere i.a. nicht irreduzibel.

Zusammenfassung 112 Sind χ und ψ Charaktere von G, so sind auch $\bar{\chi}$, $\chi + \psi$ und $\chi \cdot \psi$ Charaktere von G. Cf. Bemerkung 75, Lemma 106, Lemma 110.

4.6 Restriktion und Induktion

4.6.1 Restriktion

Seien H und G endliche Gruppen. Sei $f : H \longrightarrow G$ ein Gruppenmorphismus.

Sei $\chi : G \longrightarrow \mathbf{C}$ ein Charakter von G.

Sei $\rho : G \longrightarrow \mathrm{GL}(V)$ eine zu χ gehörige Darstellung von G auf einem endlichdimensionalen $\mathbf{C}$-Vektorraum V.

Bemerkung 113
Es ist $\chi \circ f : H \longrightarrow \mathbf{C}$ *ein Charakter von* H*, der* entlang f eingeschränkte Charakter.

Es ist $\rho \circ f$ *eine zu* $\chi \circ f$ *gehörige Darstellung.*

Beweis. Es ist $\rho \circ f : H \longrightarrow \mathrm{GL}(V)$ eine Darstellung von H auf V. Es ist

$$\chi_{\rho \circ f} \;=\; \mathrm{tr} \circ \rho \circ f \;=\; \chi \circ f \;.$$

□

Definition 114 Ist $H \leqslant G$ und ist $f : H \longrightarrow G,\ h \longmapsto h$ die Inklusionsabbildung, so schreiben wir

$$\chi\big\rfloor_H^G \;:=\; \chi \circ f$$

für den *von* G *nach* H *eingeschränkten* Charakter von χ.

I.e. $\chi\big\rfloor_H^G(h) = \chi(h)$ für $h \in H$.

Für den Charaktergrad gilt $\chi\big\rfloor_H^G(1) = \chi(1)$.

Beispiel 115 Es ist $\mathrm{C}_4 = \langle a \rangle \leqslant \langle\, a, b \,:\, a^4,\ b^2,\ (ba)^2 \,\rangle = \mathrm{D}_8$.

Was die Charaktere von D_8 angeht, verwenden wir die Notation aus der Lösung zu Aufgabe 24.(1). Was die Charaktere von C_4 angeht, verwenden wir die Notation von Beispiel 93.(2).

Es ist $\chi := \chi_1 + \chi_2 + \chi_5 = \left(\begin{smallmatrix} 4 & 0 & 2 & 0 & 0 \end{smallmatrix}\right)$ ein Charakter von D_8, wobei die Konjugationsklassen in der Reihenfolge $\{1\}$, $\{a^2\}$, $\{a, a^3\}$, ... aufgelistet sind.

Es ist $\chi\big\rfloor_{\mathrm{C}_4}^{\mathrm{D}_8} = \left(\begin{smallmatrix} \chi(1) & \chi(a) & \chi(a^2) & \chi(a^3) \end{smallmatrix}\right) = \left(\begin{smallmatrix} 4 & 2 & 0 & 2 \end{smallmatrix}\right) = 2\left(\begin{smallmatrix} 1 & 1 & 1 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & \mathrm{i} & -1 & -\mathrm{i} \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & -\mathrm{i} & -1 & \mathrm{i} \end{smallmatrix}\right)$, wobei die Konjugationsklassen in der Reihenfolge $\{1\}$, $\{a\}$, $\{a^2\}$, $\{a^3\}$ aufgelistet sind.

Wenn also für $H \leqslant G$ und $g \in G$ der Schnitt ${}^G g \cap H$ aus mehreren Konjugationsklassen von H besteht, dann wird beim Einschränken der Charakterwert bei g auf mehrere Konjugationsklassen von H "verteilt".

4.6.2 Induktion

Sei G eine endliche Gruppe. Sei $H \leqslant G$. Sei ψ ein Charakter von H. Sei M ein zu ψ gehöriger $\mathbf{C}H$-Modul, i.e. $\psi = \chi_M$.

Es ist $\mathbf{C}G$ ein $\mathbf{C}G$-$\mathbf{C}G$-Bimodul. Durch Restriktion auf der rechten Seite wird daraus ein $\mathbf{C}G$-$\mathbf{C}H$-Bimodul. I.e. es sei schlicht $g \cdot \xi \cdot h := g\xi h$ für $g \in G$, $\xi \in \mathbf{C}G$ und $h \in H$, letzteres Produkt gebildet im Ring $\mathbf{C}G$.

Sei $\ell := |G|/|H|$. Sei $G = \bigsqcup_{j\in[1,\ell]} Hx_j$, i.e. sei $\{ x_j \,:\, j \in [1,\ell] \}$ ein Repräsentantensystem der Rechtsnebenklassen von H in G. Beachte, daß $G = G^- = \bigsqcup_{i\in[1,\ell]} (Hx_j)^- = \bigsqcup_{i\in[1,\ell]} x_j^- H$.

Findet man e.g. $U \leqslant G$ mit $|U||H| = |G|$ und $U \cap H = 1$, so ist U ein Repräsentantensystem der Rechtsnebenklassen von H in G (und der Linksnebenklassen). Denn $Hu = Hv$ mit $u, v \in U$ impliziert $uv^- \in H \cap U = 1$, sodaß wegen Kardinalität insgesamt $G = \bigsqcup_{u\in U} Hu$ gilt.

Definition 116 Sei

$$\psi\!\uparrow_H^G \;:=\; \chi_{\mathbf{C}G \underset{\mathbf{C}H}{\otimes} M}$$

der *von H nach G induzierte* Charakter von $\psi = \chi_M$; cf. Aufgabe 26.(2).

Lemma 117 *Für $g \in G$ ist*

$$\psi\!\uparrow_H^G(g) \;=\; \sum_{j\,\in\,[1,\ell],\;\; {}^{x_j}g \,\in\, H} \psi({}^{x_j}g) \;=\; \frac{1}{|H|} \sum_{x\,\in\, G,\;\; {}^{x}g \,\in\, H} \psi({}^{x}g)\;.$$

Für den Charaktergrad gilt $\psi\!\uparrow_H^G(1) = \frac{|G|}{|H|}\,\psi(1)$.

Beweis. Sei $(m_1, \ldots, m_k)$ eine $\mathbf{C}$-lineare Basis von M.

Es ist $\mathbf{C}G = \bigoplus_{i\in[1,\ell]} x_j^- \mathbf{C}H$ eine Zerlegung in $\mathbf{C}H$-Rechtsmoduln.

Also ist

$$\mathbf{C}G \underset{\mathbf{C}H}{\otimes} M \;=\; \bigoplus\nolimits_{i\in[1,\ell]}\; x_j^- \mathbf{C}H \underset{\mathbf{C}H}{\otimes} M$$

als $\mathbf{C}$-Vektorräume; cf. Aufgabe 26.(5).

Es ist $\mathbf{C}H \xrightarrow{\sim} x_j^- \mathbf{C}H$, $\xi \longmapsto x_j^- \xi$ als $\mathbf{C}H$-Rechtsmoduln, und daher, als $\mathbf{C}$-Vektorräume,

$$\begin{array}{ccccccccc} x_j^-\mathbf{C}H & \underset{\mathbf{C}H}{\otimes} & M & \xrightarrow{\sim} & \mathbf{C}H & \underset{\mathbf{C}H}{\otimes} & M & \xrightarrow{\sim} & M \\ x_j^- h & \otimes & m & \longmapsto & h & \otimes & m & \longmapsto & hm\,, \end{array}$$

wobei $h \in H$ und $m \in M$; cf. Aufgabe 26.(3) und Lösung zu Aufgabe 26.(5).

Daher ist $(\, x_j^- \otimes m_i \,:\, i \in [1,k]\,)$ eine $\mathbf{C}$-lineare Basis von $x_j^-\mathbf{C}H \underset{\mathbf{C}H}{\otimes} M$. Folglich ist

$$(\, x_j^- \otimes m_i \,:\, i \in [1,k],\; j \in [1,\ell]\,)$$

eine $\mathbf{C}$-lineare Basis von $\mathbf{C}G \underset{\mathbf{C}H}{\otimes} M$.

Damit ist schonmal

$$\psi\uparrow_H^G(1) \;=\; \dim_{\mathbf{C}}(\mathbf{C}G \underset{\mathbf{C}H}{\otimes} M) \;=\; \ell \cdot k \;=\; \tfrac{|G|}{|H|}\,\dim_{\mathbf{C}} M \;=\; \tfrac{|G|}{|H|}\,\psi(1)\;;$$

cf. Bemerkung 72.

Sei $g \in G$ gegeben. Wir wollen die Spur der Multiplikationsabbildung mit g auf $\mathbf{C}G \underset{\mathbf{C}H}{\otimes} M$ bezüglich der eben gefundenen Basis berechnen.

Für $j \in [1,\ell]$ schreiben wir

$$g x_j^- \;=:\; x_{\sigma(j)}^- \, h_j$$

mit $\sigma(j) \in [1,\ell]$ und $h_j \in H$.

Es ist $\sigma(j) = j$ genau dann, wenn $g x_j^- \in x_j^- H$, i.e. wenn $x_j \, g \, x_j^- \in H$.

Für $i \in [1,k]$ wird

$$g(x_j^- \otimes m_i) \;=\; x_{\sigma(j)}^- \, h_j \otimes m_i \;=\; x_{\sigma(j)}^- \otimes h_j \, m_i \;.$$

Wir wollen den Beitrag der Basiselemente $x_j^- \otimes m_i$ mit $i \in [1,k]$ zu unserer Spur berechnen.

Falls $\sigma(j) \neq j$ ist, dann ist dieser Beitrag gleich 0, da $x_{\sigma(j)}^- \otimes h_j \, m_i$ eine $\mathbf{C}$-Linearkombination in $(x_{\sigma(j)}^- \otimes m_a \;:\; a \in [1,k])$ ist, in welcher das Basiselement $x_j^- \otimes m_i$ nicht auftritt.

Falls $\sigma(j) = j$ ist, dann ist $h_j = x_{\sigma(j)} g x_j^- = {}^{x_j}g$. Es ist also, so wir

$${}^{x_j}g \, m_i = \textstyle\sum_{a \in [1,k]} z_{a,i} \, m_a$$

schreiben mit $z_{a,i} \in \mathbf{C}$ für $a,\, i \,\in\, [1,k]$, auch

$$g(x_j^- \otimes m_i) \;=\; x_j^- \otimes {}^{x_j}g \, m_i \;=\; x_j^- \otimes \textstyle\sum_{a \in [1,k]} z_{a,i} \, m_a \;,$$

und es ergibt sich dieser Beitrag zu

$$\textstyle\sum_{i \in [1,k]} z_{i,i} \;=\; \psi({}^{x_j}g) \;.$$

Halten wir schließlich noch fest, daß diesenfalls $\psi({}^{x_j}g) = \psi({}^{hx_j}g)$ ist für $h \in H$, daß also eine andere Wahl des Repräsentanten dieser Rechtsnebenklasse denselben Beitrag zutage fördert; cf. Bemerkung 71.

Insgesamt wird also in der Tat

$$\psi\uparrow_H^G(g) \;=\; \sum_{j \in [1,\ell],\; {}^{x_j}g \in H} \psi({}^{x_j}g) \;=\; \frac{1}{|H|} \sum_{h \in H} \sum_{j \in [1,\ell],\; {}^{hx_j}g \in H} \psi({}^{hx_j}g) \;=\; \frac{1}{|H|} \sum_{x \in G,\; {}^{x}g \in H} \psi({}^{x}g) \;.$$

□

Korollar 118 *Sei $H = \sqcup_{s \in [1,t]}\, {}^{H}h_s$.*

Für $g \in G$ ist

$$\psi\uparrow_H^G(g) \;=\; |\mathrm{C}_G(g)| \sum_{s \in [1,t]} \frac{1}{|\mathrm{C}_H(h_s)|} \cdot \partial_{G_{h_s},\, G_g} \cdot \psi(h_s) \;=\; \sum_{s \in [1,t]} \frac{|\mathrm{C}_G(h_s)|}{|\mathrm{C}_H(h_s)|} \cdot \partial_{G_{h_s},\, G_g} \cdot \psi(h_s) \;.$$

Korollar 118 ist insbesondere dann von Nutzen, wenn die Bestimmung einer Menge von Rechtsnebenklassenvertretern für G/H aufwendig wäre.

Beweis. Die zweite Gleichheit resultiert aus $|\mathrm{C}_G(h_s)| = |\mathrm{C}_G(g)|$, falls ${}^G h_s = {}^G g$; cf. Aufgabe 3.(2).

Zur ersten Gleichheit. Sei $g \in G$. Ist $u \in {}^G g$, so ist, schreiben wir $u = {}^y g$ für ein $y \in G$,

$$\begin{aligned} \{\, x \in G \,:\, {}^x g = u \,\} &= \{\, x \in G \,:\, {}^x g = {}^y g \,\} \\ &= \{\, x \in G \,:\, {}^{y^- x} g = g \,\} \\ &= \{\, x \in G \,:\, y^- x \in \mathrm{C}_G(g) \,\} \;=\; y\,\mathrm{C}_G(g)\;. \end{aligned}$$

Somit wird

$$\begin{aligned} \psi\!\downarrow_H^G(g) &\overset{\text{L. }117}{=} \frac{1}{|H|} \sum_{x \in G,\ {}^x g \in H} \psi({}^x g) \\ &= \frac{1}{|H|} \sum_{h \in H} |\{\, x \in G \,:\, {}^x g = h \,\}| \cdot \psi(h) \\ &= \frac{|\mathrm{C}_G(g)|}{|H|} \sum_{h \in H} \partial_{{}^G h,\, {}^G g} \cdot \psi(h) \\ &= \frac{|\mathrm{C}_G(g)|}{|H|} \sum_{s \in [1,t]} |\,{}^H h_s| \cdot \partial_{{}^G h_s,\, {}^G g} \cdot \psi({}^x g) \\ &\overset{\text{L. }5}{=} |\mathrm{C}_G(g)| \sum_{s \in [1,t]} \frac{1}{|\mathrm{C}_H(h_s)|} \cdot \partial_{{}^G h_s,\, {}^G g} \cdot \psi({}^x g)\;. \end{aligned}$$

□

Beispiel 119 Sei $G = \mathrm{S}_3$. Wir verwenden die Notation von Beispiel 86.(1), was ihre Konjugationsklassenrepräsentanten $g_1 = \mathrm{id}$, $g_2 = (1,2)$ und $g_3 = (1,2,3)$ und ihre irreduziblen Charaktere angeht.

Schreibe $\zeta := \zeta_3$.

Sei $H = \langle (1,2,3) \rangle \leqslant \mathrm{S}_3 = G$.

Die (einelementigen) Konjugationsklassen von H seien von

$$h_1 \;:=\; \mathrm{id}\;, \qquad h_2 \;:=\; (1,2,3)\;, \qquad h_3 \;:=\; (1,3,2)$$

repräsentiert.

Es ist $\psi := (1 \;\; \zeta \;\; \zeta^2)$ ein Charakter von H ; cf. Beispiel 86.(2).

Es wird $\psi\!\downarrow_H^G(\mathrm{id}) = \frac{|G|}{|H|}\,\psi(\mathrm{id}) \;=\; 2$.

Alternativ wird $\psi\!\downarrow_H^G(\mathrm{id}) = \sum_{s \in [1,3]} \frac{|\mathrm{C}_G(h_s)|}{|\mathrm{C}_H(h_s)|} \cdot \partial_{{}^G h_s,\, {}^G \mathrm{id}} \cdot \psi(h_s) = 2 \cdot 1 + 0 + 0 = 0$.

Es wird $\psi\!\downarrow_H^G((1,2)) = \sum_{s \in [1,3]} \frac{|\mathrm{C}_G(h_s)|}{|\mathrm{C}_H(h_s)|} \cdot \partial_{{}^G h_s,\, {}^G (1,2)} \cdot \psi(h_s) = 0 + 0 + 0 = 0$.

Es wird $\psi\uparrow_H^G((1,2,3)) = \sum_{s\in[1,3]} \frac{|\mathrm{C}_G(h_s)|}{|\mathrm{C}_H(h_s)|} \cdot \partial_{G h_s, G(1,2,3)} \cdot \psi(h_s) = 0 + 1\cdot\zeta + 1\cdot\zeta^2 = -1$.

Alternativ wird $G = Hx_1 \sqcup Hx_2$ mit $x_1 := \mathrm{id}$ und $x_2 := (1,2)$, und somit $\psi\uparrow_H^G((1,2,3)) = \sum_{j\in[1,2],\ {}^{x_j}(1,2,3)\in H} \psi({}^{x_j}(1,2,3)) = \zeta + \zeta^2 = -1$.

Insgesamt ist also $\psi\uparrow_H^G = (\begin{smallmatrix}2 & 0 & -1\end{smallmatrix}) = \chi_3$; cf. Beispiel 126.

4.6.3 Frobenius-Reziprozität

Sei G eine endliche Gruppe. Sei $H \leqslant G$.

Sei ψ ein Charakter von H. Sei M ein zu ψ gehöriger $\mathbf{C}H$-Modul, i.e. $\psi = \chi_M$.

Sei χ ein Charakter von G. Sei N ein zu χ gehöriger $\mathbf{C}G$-Modul, i.e. $\chi = \chi_N$.

Der von $\mathbf{C}G$ nach $\mathbf{C}H$ eingeschränkte Modul $N|_{\mathbf{C}H}$, der von der eingeschränkten Darstellung $H \hookrightarrow G \xrightarrow{\rho_N} \mathrm{GL}(N)$ kommt, gehört zum von G nach H eingeschränkten Charakter $\chi\downarrow_H^G$; cf. Bemerkung 113, Aufgabe 31.(3).

Lemma 120 (Frobenius-Reziprozität) *Es ist*

$$ {}_G(\psi\uparrow_H^G, \chi) \;=\; {}_H(\psi, \chi\downarrow_H^G) ; $$

cf. Definition 91, *Bemerkung* 95.(1).

Beweis. Es ist

$$\begin{aligned}
{}_G(\psi\uparrow_H^G, \chi) &\overset{\text{B. 95.(1)}}{=} \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}G}(\mathbf{C}G \underset{\mathbf{C}H}{\otimes} M,\, N) \\
&\overset{\text{A. 31.(2)}}{=} \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}H}(M,\, \mathrm{Hom}_{\mathbf{C}G}(\mathbf{C}G,\, N)) \\
&\overset{\text{A. 31.(3)}}{=} \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}H}(M,\, N|_{\mathbf{C}H}) \\
&\overset{\text{B. 95.(1)}}{=} {}_H(\psi, \chi\downarrow_H^G) .
\end{aligned}$$

□

4.6.4 Mackey

Sei G eine endliche Gruppe. Seien $H,\, K \leqslant G$.

Bemerkung 121 *Sei zudem $K \leqslant H$.*

(1) *Sei χ ein Charakter von G. Es ist $\chi\downarrow_H^G\downarrow_K^H = \chi\downarrow_K^G$. Es ist $\chi\downarrow_G^G = \chi$.*

(2) *Sei κ ein Charakter von K. Es ist $\kappa\uparrow_K^H\uparrow_H^G = \kappa\uparrow_K^G$. Es ist $\kappa\uparrow_K^K = \kappa$.*

Beweis. Zu (2).

Über Charaktere.

Zur ersten Aussage. Es genügt zu zeigen, daß ${}_G(\kappa\restriction_K^H\restriction_H^G, \tau) = {}_G(\kappa\restriction_K^G, \tau)$ ist für jeden irreduziblen Charakter τ von G; cf. Bemerkung 94.(1). In der Tat wird

$$ {}_G(\kappa\restriction_K^H\restriction_H^G, \tau) \overset{\text{L. 120}}{=} {}_H(\kappa\restriction_K^H, \tau\downarrow_H^G) \overset{\text{L. 120}}{=} {}_K(\kappa, \tau\downarrow_H^G\downarrow_K^H) \overset{(1)}{=} {}_K(\kappa, \tau\downarrow_K^G) \overset{\text{L. 120}}{=} {}_G(\kappa\restriction_K^G, \tau) \, . $$

Zur zweiten Aussage. Es genügt zu zeigen, daß ${}_K(\kappa\restriction_K^K, \tau) = {}_K(\kappa, \tau)$ für jeden irreduziblen Charakter τ von K. In der Tat wird

$$ {}_K(\kappa\restriction_K^K, \tau) \overset{\text{L. 120}}{=} {}_K(\kappa, \tau\downarrow_K^K) \overset{(1)}{=} {}_K(\kappa, \tau) \, . $$

Alternativ hierzu, *über Moduln.*

Zur ersten Aussage. Sei M ein zu κ gehöriger $\mathbf{C}K$-Modul, i.e. $\kappa = \chi_M$. Wir haben $\mathbf{C}G$-lineare Isomorphismen

$$ \begin{array}{ccccccccccc} \mathbf{C}G & \underset{\mathbf{C}H}{\otimes} & (\mathbf{C}H & \underset{\mathbf{C}K}{\otimes} & M) & \overset{\text{A. 26.(4)}}{\longrightarrow} & (\mathbf{C}G & \underset{\mathbf{C}H}{\otimes} & \mathbf{C}H) & \underset{\mathbf{C}K}{\otimes} & M \\ g & \otimes & (h & \otimes & m) & \longmapsto & (g & \otimes & h) & \otimes & m \end{array} \overset{\text{A. 26.(3, L.z. 5)}}{\longrightarrow} \begin{array}{ccc} \mathbf{C}G & \underset{\mathbf{C}K}{\otimes} & M \\ gh & \otimes & m \end{array} , $$

wobei die $\mathbf{C}G$-Linearität wie folgt einzusehen ist. Jedes Element von $(\mathbf{C}G \underset{\mathbf{C}H}{\otimes} \mathbf{C}H) \underset{\mathbf{C}K}{\otimes} M)$ ist von der Form $\sum_g (g \otimes 1) \otimes m_g$ mit $m_g \in M$ für $g \in G$. Es ergibt sich

$$ \begin{array}{rcl} (\sum_x z_x \, x)(\sum_g (g \otimes 1) \otimes m_g) & = & \sum_g (\sum_x z_x \, xg \otimes 1) \otimes m_g \\ & \longmapsto & \sum_g (\sum_x z_x \, xg) \otimes m_g \\ & = & (\sum_x z_x \, x)(\sum_g g \otimes m_g) \, , \end{array} $$

wobei $z_x \in \mathbf{C}$ für $x \in G$. Also wird

$$ \kappa\restriction_K^H\restriction_H^G = \chi_{\mathbf{C}G \underset{\mathbf{C}H}{\otimes} (\mathbf{C}H \underset{\mathbf{C}K}{\otimes} M)} \overset{\text{B. 74}}{=} \chi_{\mathbf{C}G \underset{\mathbf{C}K}{\otimes} M} = \kappa\restriction_K^G \, . $$

Die zweite Aussage folgt mit Aufgabe 26.(3).

□

Lemma 122 (Mackeyformel) *Sei κ ein Charakter von K.*

Wähle $D \subseteq G$ mit $G = \bigsqcup_{d\in D} HdK$.

Betrachte den Gruppenisomorphismus $c_d := {}^dK \xrightarrow{\sim} K,\ {}^dk \longmapsto k = {}^{d^-}({}^dk)$ für $d \in D$.

Es ist

$$\kappa\big\uparrow_K^G\big\downarrow_H^G \;=\; \sum_{d\in D}(\kappa\circ c_d)\big\downarrow_{{}^dK\cap H}^{{}^dK}\big\uparrow_{{}^dK\cap H}^{H} .$$

Beweis. Sei V ein $\mathbf{C}K$-Modul mit $\kappa = \chi_V$.

Für $d \in D$ schreiben wir ${}_dV$ für den $\mathbf{C}({}^dK)$-Modul, der zur Darstellung $\rho_V \circ c_d$ von ${}^dK$ auf V gehört. Somit wird ${}^dk \cdot v = kv$ für $k \in K$ und $v \in V$, wobei links auf ${}_dV$ multipliziert wird und rechts auf V.

Schreibe $\mathbf{C}HdK := {}_{\mathbf{C}}\langle\, hdk \,:\, h \in H,\, k \in K \,\rangle$. Es ist $\mathbf{C}G = \bigoplus_{d\in D} \mathbf{C}HdK$ eine Zerlegung in $\mathbf{C}H$-$\mathbf{C}K$-Teilbimoduln. Also wird

$$\mathbf{C}G \underset{\mathbf{C}K}{\otimes} V \;=\; (\textstyle\bigoplus_{d\in D} \mathbf{C}HdK) \underset{\mathbf{C}K}{\otimes} V \;\overset{\text{cf. A. 26.(5)}}{\simeq}\; \bigoplus_{d\in D}(\mathbf{C}HdK \underset{\mathbf{C}K}{\otimes} V) .$$

Sei $d \in D$. Es bleibt zu zeigen, daß

$$\begin{array}{rcccc} \mathbf{C}HdK & \underset{\mathbf{C}K}{\otimes} & V & \longrightarrow & \mathbf{C}H \underset{\mathbf{C}({}^dK\cap H)}{\otimes} {}_dV \\ hdk & \otimes & v & \longmapsto & h \otimes kv \\ hd & \otimes & v & \longleftarrow & h \otimes v \end{array}$$

sich gegenseitig invertierende $\mathbf{C}H$-lineare Abbildungen sind, wobei $h \in H$, $k \in K$ und $v \in V$. Denn zur rechten Seite gehört der Charakter $(\kappa\circ c_d)\big\downarrow_{{}^dK\cap H}^{{}^dK}\big\uparrow_{{}^dK\cap H}^{H}$.

Wohldefiniertheit und $\mathbf{Z}$-Linearität von $\longmapsto$. Ist $hdk = \tilde h d\tilde k$ für $h, \tilde h \in H$ und $k, \tilde k \in K$, dann wird $\tilde h^- h = {}^d(\tilde k k^-) \in {}^dK \cap H$ und folglich auf der rechten Seite

$$h \otimes kv \;=\; \tilde h(\tilde h^- h) \otimes kv \;=\; \tilde h \otimes {}^d(\tilde k k^-) \cdot kv \;=\; \tilde h \otimes \tilde k k^- kv \;=\; \tilde h \otimes \tilde k v .$$

Ferner wird für $h \in H$, $k \in K$, $v \in V$ und $k' \in K$ auch $h \otimes (kk')v = h \otimes k(k'v)$.

Entsprechend für $\mathbf{C}$-Linearkombinationen. Additivität in beiden Faktoren ist ersichtlich.

Wohldefiniertheit und $\mathbf{Z}$-Linearität von $\longleftarrow$. Seien $h \in H$ und $v \in V$ gegeben. Sei ferner $h' = {}^dk' \in {}^dK \cap H$ gegeben. Es wird auf der linken Seite

$$hh'd \otimes v \;=\; h\,{}^dk'd \otimes v \;=\; hdk' \otimes v \;=\; hd \otimes k'v \;=\; hd \otimes {}^dk' \cdot v .$$

Entsprechend für $\mathbf{C}$-Linearkombinationen. Additivität in beiden Faktoren ist ersichtlich.

Sowohl $\mathbf{C}H$*-Linearität* von $\longmapsto$ und $\longleftarrow$ als auch ihre *gegenseitige Inversion* sind ersichtlich.

Satz 123 (Mackeykriterium) *Weiterhin sei G eine endliche Gruppe und $H \leqslant G$.*
Sei ψ ein Charakter von H.
Betrachte den Gruppenisomorphismus $c_g : {}^gH \xrightarrow{\sim} H,\ {}^gh \longmapsto h = {}^{g^-}({}^gh)$ für $g \in G$.
Wähle $D \subseteq G$ so, daß $G = \bigsqcup_{d\in D} HdH$ und daß $1 \in D$.
Es ist $\psi\uparrow_H^G$ genau dann irreduzibel, wenn folgende Aussagen (1) und (2) gelten.

(1) *Es ist ψ irreduzibel.*

(2) *Für $d \in D \smallsetminus \{1\}$ ist ${}_{{}^dH\cap H}(\psi\downarrow^H_{{}^dH\cap H}, (\psi \circ c_d)\downarrow^{{}^dH}_{{}^dH\cap H}) = 0$.*

Beweis. O.E. ist $\psi \neq 0$.

Es ist

$$\begin{aligned}
{}_G(\psi\uparrow_H^G, \psi\uparrow_H^G) &\overset{\text{L. }120}{=} {}_H(\psi, \psi\uparrow_H^G\downarrow_H^G) \\
&\overset{\text{L. }122}{=} {}_H(\psi, \textstyle\sum_{d\in D}(\psi \circ c_d)\downarrow^{{}^dH}_{{}^dH\cap H}\uparrow^H_{{}^dH\cap H}) \\
&= {}_H(\psi,\psi) + \textstyle\sum_{d\in D\smallsetminus\{1\}} {}_H(\psi, (\psi \circ c_d)\downarrow^{{}^dH}_{{}^dH\cap H}\uparrow^H_{{}^dH\cap H}) \\
&\overset{\text{B. }95}{=} {}_H(\psi,\psi) + \textstyle\sum_{d\in D\smallsetminus\{1\}} {}_H((\psi \circ c_d)\downarrow^{{}^dH}_{{}^dH\cap H}\uparrow^H_{{}^dH\cap H}, \psi) \\
&\overset{\text{L. }120}{=} {}_H(\psi,\psi) + \textstyle\sum_{d\in D\smallsetminus\{1\}} {}_{{}^dH\cap H}((\psi \circ c_d)\downarrow^{{}^dH}_{{}^dH\cap H}, \psi\downarrow^H_{{}^dH\cap H}) \\
&\overset{\text{B. }95}{=} {}_H(\psi,\psi) + \textstyle\sum_{d\in D\smallsetminus\{1\}} {}_{{}^dH\cap H}(\psi\downarrow^H_{{}^dH\cap H}, (\psi \circ c_d)\downarrow^{{}^dH}_{{}^dH\cap H}) \,.
\end{aligned}$$

Es liegt das Skalarprodukt zweier Charaktere in $\mathbf{Z}_{\geqslant 0}$; cf. Bemerkung 95.(1). Speziell ist ${}_H(\psi,\psi) \in \mathbf{Z}_{\geqslant 1}$; cf. Definition 91.(2).

Nun ist $\psi\uparrow_H^G$ genau dann irreduzibel, wenn ${}_G(\psi\uparrow_H^G, \psi\uparrow_H^G) = 1$; cf. Bemerkung 94.(2). Nach vorstehendem ist dies aber genau dann der Fall, wenn ${}_H(\psi,\psi) = 1$ und ${}_H(\psi, (\psi \circ c_d)\downarrow^{{}^dH}_{{}^dH\cap H}\uparrow^H_{{}^dH\cap H}) = 0$ ist für $d \in D \smallsetminus \{1\}$.

Ersteres ist schließlich äquivalent dazu, daß ψ irreduzibel ist; cf. Bemerkung 94.(2). ▫

Bemerkung 124 Für einen Charakter ψ von H und $g \in G$ ist explizit

$${}_{{}^gH\cap H}(\psi\downarrow^H_{{}^gH\cap H}, (\psi \circ c_g)\downarrow^{{}^gH}_{{}^gH\cap H}) \;=\; \tfrac{1}{|{}^gH\cap H|}\textstyle\sum_{x\in {}^gH\cap H} \psi(x)\,\overline{\psi(g^-xg)}\,.$$

Da $D \smallsetminus \{1\}$ in Satz 123 ein beliebig gewähltes Doppelnebenklassenrepräsentantensystem ist, folgt aus $\psi\uparrow_H^G$ irreduzibel auch noch, daß ${}_{{}^gH\cap H}(\psi\downarrow^H_{{}^gH\cap H}, (\psi \circ c_g)\downarrow^{{}^gH}_{{}^gH\cap H}) = 0$ für $g \in G \smallsetminus H$.

Beispiel 125 Sei $n \in \mathbf{Z}_{\geqslant 2}$. Betrachte $\mathrm{S}_{n-1} \leqslant \mathrm{S}_n$. Sei ψ ein irreduzibler Charakter von S_{n-1}. Sei $\sigma \in \mathrm{S}_n \smallsetminus \mathrm{S}_{n-1}$. Es wird

$$\frac{1}{|{}^\sigma\mathrm{S}_{n-1} \cap \mathrm{S}_{n-1}|}\sum_{\tau\in {}^\sigma\mathrm{S}_{n-1}\cap \mathrm{S}_{n-1}} \psi(\tau)\,\overline{\psi(\sigma^-\tau\sigma)} \;=\; \frac{1}{|{}^\sigma\mathrm{S}_{n-1} \cap \mathrm{S}_{n-1}|}\sum_{\tau\in {}^\sigma\mathrm{S}_{n-1}\cap \mathrm{S}_{n-1}} \psi(\tau)\,\overline{\psi(\tau)} \;> 0\,.$$

da zwei Elemente aus S_{n-1}, die in S_n konjugiert sind, denselben Zykeltyp aufweisen und damit auch in S_{n-1} konjugiert sind, und da $\psi(1) \neq 0$ ist. Gemäß Mackeykriterium ist also $\psi\downarrow^{\mathrm{S}_n}_{\mathrm{S}_{n-1}}$ nicht irreduzibel; cf. Satz 123, Bemerkung 124. Cf. auch Lösung zu Aufgabe 42.(2).

Beispiel 126 Sei $N \trianglelefteq G$. Sei ψ ein irreduzibler Charakter von N. Sei $G = \bigsqcup_{d\in D} NdN = \bigsqcup_{d\in D} dN$ und $1 \in D$. Es ist $\psi\uparrow^G_N$ irreduzibel genau dann, wenn ${}_N(\psi, \psi \circ c_d) = 0$ ist für $d \in D \smallsetminus \{1\}$; cf. Satz 123. I.e. es ist $\psi\uparrow^G_N$ irreduzibel genau dann, wenn $\psi \circ c_d \neq \psi$ für $d \in D \smallsetminus \{1\}$; cf. Aufgabe 33.(4), Satz 90.(1).

In der Situation von Beispiel 119 ist $G = \mathrm{S}_3$, $N = \langle(1,2,3)\rangle$ und $D = \{\mathrm{id}, (1,2)\}$. Wir schreiben $\zeta := \zeta_3$. Es ist $\psi = (1\ \zeta\ \zeta^2)$ und $\psi \circ c_{(1,2)} = (1\ \zeta^2\ \zeta) \neq \psi$. Also ist $\psi\uparrow^G_N$ irreduzibel, wie in loc. cit. ja auch schon festgestellt.

Cf. auch Nebenbemerkung in Lösung zu Aufgabe 52.

Kapitel 5

Burnside, Artin und Brauer

5.1 Burnside

Sei G eine endliche Gruppe.

5.1.1 Ein Lemma über Gruppen mittels Charakteren

Lemma 127 *Sei $k \in \mathbf{Z}_{\geqslant 1}$. Schreibe $\zeta := \zeta_k$.*

Sei $n \in \mathbf{Z}_{\geqslant 1}$. Seien $x_i \in \mathbf{Z}_{\geqslant 0}$ für $i \in [0, k-1]$ mit $\sum_{i \in [0,k-1]} x_i = n$ gegeben.

Es liege $\alpha := \frac{1}{n} \sum_{i \in [0,k-1]} x_i \, \zeta^i$ in $\mathcal{O} \setminus \{0\}$; cf. Definition 100, Aufgabe 29.(2, 3).

Dann gibt es ein $j \in [1, n]$ mit $x_i = n \, \partial_{j,i}$ für $i \in [0, k-1]$, und mit $\alpha = \zeta^j$.

Beweis. Schreibe $\mathbf{Q}(\zeta) := {}_{\mathbf{Q}}\langle \, \zeta^i \, : \, i \in [0, k-1] \, \rangle \subseteq \mathbf{C}$. Da das angegebene $\mathbf{Q}$-lineare Erzeugendensystem unter Multiplikation abgeschlossen ist, ist $\mathbf{Q}(\zeta) \subseteq \mathbf{C}$ eine endlichdimensionale $\mathbf{Q}$-Teilalgebra.

Da $\mathbf{Q}(\zeta)$ als Teilring von $\mathbf{C}$ auch ein Integritätsbereich ist, ist es ein Körper, da aus der Injektivität der $\mathbf{Q}$-linearen Multiplikationsabbildung auf $\mathbf{Q}(\zeta)$ mit einem Element ξ aus $\mathbf{Q}(\zeta) \setminus \{0\}$ auch ihre Surjektivität und damit die Invertierbarkeit von ξ in $\mathbf{Q}(\zeta)$ folgt.

Sei $\Gamma := \{ \, \mathbf{Q}(\zeta) \xrightarrow{\sigma} \mathbf{Q}(\zeta) \, : \, \sigma \text{ ist ein } \mathbf{Q}\text{-Algebrenisomorphismus} \, \}$. Mit der Komposition als Multiplikation ist Γ eine Gruppe.

Wir brauchen folgende Aussagen aus der Galoistheorie; cf. Aufgabe 40.

(i) Es ist Γ endlich.

(ii) Es ist $\{ \, \xi \in \mathbf{Q}(\zeta) \, : \, \text{es ist } \tau(\xi) = \xi \text{ für } \tau \in \Gamma \, \} = \mathbf{Q}$.

Sei $A := \prod_{\sigma\in\Gamma} \sigma(\alpha)$, was dank (i) ein endliches und damit bildbares Produkt ist.

Für $\tau \in \Gamma$ ist $\tau(A) = \prod_{\sigma\in\Gamma}(\tau\circ\sigma)(\alpha) \overset{\rho := \tau\circ\sigma}{=} \prod_{\rho\in\Gamma} \rho(\alpha) = A$. Mit (ii) folgt $A \in \mathbf{Q}$.

Sei $\tau \in \Gamma$. Da $\alpha \in \mathcal{O}$ ist, gibt es ein Polynom $f(X) = \sum_{i\in[0,m]} b_i X^i \in \mathbf{Z}[X]$ mit $m \in \mathbf{Z}_{\geqslant 1}$, mit $b_m = 1$ und mit $f(\alpha) = 0$. Es folgt

$$f(\tau(\alpha)) \;=\; \textstyle\sum_{i\in[0,m]} b_i \tau(\alpha)^i \;\overset{\text{A. 19.(2)}}{=}\; \tau(\sum_{i\in[0,m]} b_i \alpha^i) \;=\; \tau(f(\alpha)) \;=\; \tau(0) \;=\; 0\,.$$

Also ist auch $\tau(\alpha) \in \mathcal{O}$.

Insgesamt folgt

$$A \;=\; \textstyle\prod_{\sigma\in\Gamma} \sigma(\alpha) \;\overset{\text{A. 29.(2)}}{\in}\; \mathcal{O}\cap\mathbf{Q} \;\overset{\text{A. 29.(3)}}{=}\; \mathbf{Z}\,.$$

Sei $\tau \in \Gamma$. Für $i \in [0, k-1]$ ist $|\tau(\zeta^i)|^k = |\tau(\zeta^{ik})| = 1$ und also $|\tau(\zeta^i)| = 1$. Mit der Dreiecksungleichung wird

$$|\tau(\alpha)| \;=\; |\tau(\tfrac{1}{n}\textstyle\sum_{i\in[0,k-1]} x_i\,\zeta^i)| \;=\; |\tfrac{1}{n}\textstyle\sum_{i\in[0,k-1]} x_i\,\tau(\zeta^i)| \;\leqslant\; \tfrac{1}{n}\textstyle\sum_{i\in[0,k-1]} x_i\,|\tau(\zeta^i)| \;=\; 1\,.$$

Hieraus ergibt sich

$$|A| \;=\; |\textstyle\prod_{\sigma\in\Gamma} \sigma(\alpha)| \;=\; \prod_{\sigma\in\Gamma} |\sigma(\alpha)| \;\leqslant\; 1\,.$$

Da $A \in \mathbf{Z}$ ist, folgt $|A| = 0$ oder $|A| = 1$.

Fall $|A| = 0$. Es ist $A = 0$. Da $\operatorname{Kern}\sigma = 0$ für $\sigma \in \Gamma$, folgt $\alpha = 0$. Nach Voraussetzung tritt dies nicht ein.

Fall $|A| = 1$. Es folgt $|\sigma(\alpha)| = 1$ für alle $\sigma \in \Gamma$, insbesondere also $|\alpha| = 1$, i.e. $|\sum_{i\in[0,k-1]} x_i\,\zeta^i| = n$.

Angenommen, es gibt $j, j' \in [0, k-1]$ mit $j \neq j'$, $x_j \geqslant 1$ und $x_{j'} \geqslant 1$. Vermittels Multiplikation mit $\zeta^{-j'}$ dürfen wir $j' = 0$ annehmen.

Aus

$$n \;=\; |\textstyle\sum_{i\in[0,k-1]} x_i\,\zeta^i| \;\overset{\text{D.U.}}{\leqslant}\; \underbrace{|\textstyle\sum_{i\in[1,k-1]\smallsetminus\{j\}} x_i\,\zeta^i|}_{\overset{\text{D.U.}}{\leqslant}\, n-x_0-x_j} + \underbrace{|x_0 + x_j\,\zeta^j|}_{\overset{\text{D.U.}}{\leqslant}\, x_0+x_j}$$

folgt $|x_0 + x_j\,\zeta^j| = x_0 + x_j$, mit Aufgabe 39 also $x_j\,\zeta^j \in \mathbf{R}_{\geqslant 0}$, *Widerspruch.*

Also gibt es ein $j \in [0, k-1]$ mit $x_i = 0$ für $i \in [0, k-1] \smallsetminus \{j\}$.

Da $\sum_{i\in[0,k-1]} x_i = n$ ist, folgt $\alpha = \zeta^j$. ▫

Lemma 128 *Sei χ ein irreduzibler Charakter von G. Sei $\rho : G \longrightarrow \mathrm{GL}(V)$ eine Darstellung von G auf einem endlichdimensionalen $\mathbf{C}$-Vektorraum V mit $\chi = \chi_\rho$.*

Sei $g \in G$ mit $\chi(g) \neq 0$ gegeben. Sei $k := |\langle g\rangle|$ seine Ordnung. Schreibe $\zeta := \zeta_k$.

Falls $|{}^G g|$ und $\chi(1)$ in $\mathbf{Z}$ teilerfremd sind, dann ist $\rho(g) = \zeta^j \cdot \mathrm{id}_V$ für ein $j \in [0, k-1]$.

Beweis. Es ist $\chi(g) \cdot \frac{|^G g|}{\chi(1)} \in \mathcal{O}$; cf. Bemerkungen 96 und 101.

Es ist $\chi(g) = \sum_{i\in[0,k-1]} x_i\, \zeta^i$ mit $x_i \in \mathbf{Z}_{\geqslant 0}$ für $i \in [0, k-1]$ so, daß $\sum_{i\in[0,k-1]} x_i = \chi(1)$; cf. Aufgabe 25.(1). Ferner ist x_i die Multiplizität des Eigenwerts ζ^i des diagonalisierbaren Endomorphismus $\rho(g)$; cf. Lösung zu loc. cit.

Insbesondere ist $\chi(g) \in \mathcal{O}$; cf. Aufgabe 29.(2).

Wegen Teilerfremdheit gibt es $a,\, b \in \mathbf{Z}$ mit $a|^G g| + b\chi(1) = 1$. Somit ist

$$\frac{\chi(g)}{\chi(1)} \;=\; \chi(g) \cdot \frac{a|^G g| + b\chi(1)}{\chi(1)} \;=\; a \cdot \underbrace{\chi(g) \cdot \frac{|^G g|}{\chi(1)}}_{\in \mathcal{O}} + b \cdot \underbrace{\chi(g)}_{\in \mathcal{O}} \;\in\; \mathcal{O}\,;$$

cf. Aufgabe 29.(2). Insgesamt ist also $\dfrac{\chi(g)}{\chi(1)} \in \mathcal{O} \smallsetminus \{0\}$.

Somit sind die Voraussetzungen von Lemma 127 erfüllt. Es gibt also ein $j \in [0, k-1]$ so, daß $x_i = \chi(1)\partial_{j,i}$ ist für $i \in [0, k-1]$.

Somit ist ζ^j der einzige Eigenwert des diagonalisierbaren Endomorphismus $\rho(g)$. Folglich ist $\rho(g) = \zeta^j \cdot \mathrm{id}_V$. ▫

> Die Aussage des folgenden Lemmas bezieht sich nur auf Gruppen; unser Beweis benötigt aber Charaktere.

Lemma 129 *Sei $p \in \mathbf{Z}_{\geqslant 1}$ prim. Sei $g \in G \smallsetminus \{1\}$.*
Falls $|^G g| = p^\ell$ ist für ein $\ell \in \mathbf{Z}_{\geqslant 0}$, dann gibt es ein $N \lhd G$ mit $gN \in \mathrm{Z}(G/N)$.

Beweis. Seien $\{\chi_1\,,\, \ldots\,,\, \chi_t\}$ die paarweise verschiedenen irreduziblen Charaktere von G, wobei χ_1 der triviale Charakter sei.

Wir *behaupten,* daß es ein $s \in [2, t]$ mit $\chi_s(g) \neq 0$ und mit $\chi_s(1) \not\equiv_p 0$ gibt.

Annahme, für alle $s \in [2, t]$ mit $\chi_s(g) \neq 0$ ist $\chi_s(1) \equiv_p 0$. Dank $g \neq 1$ erhalten wir mit vertikaler Orthogonalität

$$1 + \textstyle\sum_{s\in[2,t],\, \chi_s(g)\neq 0} \chi_s(1)\, \chi_s(g) \;=\; \sum_{s\in[1,t]} \chi_s(1)\, \chi_s(g) \;\overset{\text{S. 90.(2)}}{=}\; 0\,.$$

Es ist $\chi_s(g) \in \mathcal{O}$ für $s \in [2, t]$; cf. Aufgaben 25.(1) und 29.(2). Somit folgt

$$\tfrac{1}{p} \;=\; -\tfrac{1}{p} \textstyle\sum_{s\in[2,t]} \chi_s(1)\chi_s(g) \;=\; -\sum_{s\in[2,t],\, \chi_s(g)\neq 0} \underbrace{\tfrac{1}{p}\, \chi_s(1)}_{\in \mathbf{Z}} \underbrace{\chi_s(g)}_{\in \mathcal{O}} \;\in\; \mathcal{O} \cap \mathbf{Q} \;\overset{\text{A. 29.(3)}}{=}\; \mathbf{Z}\,.$$

Wir haben einen *Widerspruch,* und damit die *Behauptung* gezeigt.

Schreibe $\chi := \chi_s$. Sei $\rho : G \longrightarrow \mathrm{GL}(V)$ eine Darstellung auf einem endlichdimensionalen $\mathbf{C}$-Vektorraum V mit $\chi = \chi_\rho$. Schreibe $k := |\langle g\rangle|$ und $\zeta := \zeta_k$.

Setze $N := \operatorname{Kern}\rho = \operatorname{Kern}\chi = \{\, x \in G \,:\, \chi(x) = \chi(1) \,\}$; cf. Aufgabe 30.

Wäre $\operatorname{Kern}\chi = G$, dann wäre $\chi(x) = \chi(1)$ für alle $x \in G$, i.e. $\chi = \chi(1) \cdot \chi_1$, also wegen Irreduzibilität $\chi(1) = 1$, also $\chi = \chi_1$, was aber nicht der Fall ist. Also ist $N = \operatorname{Kern}\chi \lhd G$.

Es ist $\chi(g) \neq 0$. Da $|{}^G g| = p^\ell$ und $\chi(1) \not\equiv_p 0$ ist, sind $|{}^G g|$ und $\chi(1)$ teilerfremd in $\mathbf{Z}$. Gemäß Lemma 128 ist also $\rho(g) = \zeta^j \cdot \mathrm{id}_V$ für ein $j \in [0, k-1]$, und somit $\rho(g) \in \mathrm{Z}(\mathrm{GL}(V))$.

Sei $x \in G$ gegeben. Es ist $\rho({}^x g \cdot g^-) = {}^{\rho(x)}\rho(g) \cdot \rho(g)^- = \rho(g) \cdot \rho(g)^- = 1$. Daher ist ${}^x g \cdot g^- \in \operatorname{Kern}\rho = N$. Es folgt ${}^{(xN)}(gN) \cdot (gN)^- = {}^x g \cdot g^- N = 1_{G/N}$, i.e. ${}^{(xN)}(gN) = gN$.

Somit ist $gN \in \mathrm{Z}(G/N)$. ▫

5.1.2 Anwendung auf Gruppen der Ordnung $p^a q^b$

Seien $p,\, q \in \mathbf{Z}_{\geqslant 1}$ prim, und sei $p \neq q$.

Sei $|G| = p^a q^b$ für gewisse $a,\, b \in \mathbf{Z}_{\geqslant 0}$.

Wir erinnern daran, daß die Gruppe G einfach genannt wird, falls sie genau zwei Normalteiler enthält, nämlich 1 und G ; cf. Aufgabe 8.

Der Auflösbarkeitsbegriff findet sich in Definition 30.(1).

Lemma 130 *Ist* $\mathrm{Z}(G) = 1$*, so ist* G *nicht einfach.*

Beweis. Da im Falle $a = b = 0$ nichts zu zeigen ist, ist o.E. $b \geqslant 1$.

Schreibe $G = \bigsqcup_{s\in[1,t]} {}^G g_s$, wobei $t \in \mathbf{Z}_{\geqslant 1}$ und $g_s \in G$ für $s \in [1,t]$, mit $g_1 = 1$.

Es ist $|{}^G g_s|$ ein Teiler von $|G|$ für $s \in [1,t]$; cf. Lemma 5.

Wäre $|{}^G g_s| \equiv_q 0$ für alle $s \in [2,t]$, dann wäre

$$0 \;\equiv_q\; |G| \;=\; \textstyle\sum_{s\in[1,t]} |{}^G g_s| \;\equiv_q\; |{}^G g_1| \;=\; 1 \;,$$

was nicht der Fall ist. Also gibt es ein $s \in [2,t]$ mit $|{}^G g_s| \not\equiv_q 0$.

Schreibe $g := g_s \in G \smallsetminus \{1\}$. Es ist $|{}^G g| = p^\ell$ für ein $\ell \in [0,a]$.

Dank Lemma 129 gibt es ein $N \lhd G$ mit $gN \in \mathrm{Z}(G/N)$. Es kann nicht $N = 1$ sein, da $\mathrm{Z}(G) = 1$ ist, aber $g \neq 1$. Also ist G nicht einfach. ▫

Satz 131 (Burnside) *Wir erinnern daran, daß* G *eine Gruppe ist mit* $|G| = p^a q^b$ *für gewisse* $a,\, b \in \mathbf{Z}_{\geqslant 0}$ *, wobei* p *und* q *verschiedene Primzahlen sind.*

Es ist G *auflösbar.*

Beweis. Induktion nach $|G|$. Für $|G| = 1$ ist nichts zu zeigen. Sei $|G| > 1$. Nach Induktionsvoraussetzung sind alle Gruppen H, deren Ordnung $|H|$ ein echter Teiler von $|G|$ ist, auflösbar.

Fall $\mathrm{Z}(G) \neq 1$. Es ist $\mathrm{Z}(G)$ abelsch, also auflösbar. Da $|G/\mathrm{Z}(G)|$ ein echter Teiler von $|G|$ ist, ist auch $G/\mathrm{Z}(G)$ auflösbar. Folglich ist auch G auflösbar; cf. Aufgabe 12.(1).

Fall $\mathrm{Z}(G) = 1$. Es ist G dank Lemma 130 nicht einfach. Somit gibt es ein $1 \neq N \lhd G$. Da $|N|$ und $|G/N|$ echte Teiler von $|G|$ sind, sind N und G/N auflösbar. Folglich ist auch G auflösbar; cf. Aufgabe 12.(1). ▫

Beispiel 132

(1) Da $|\mathrm{S}_4| = 2^3 \cdot 3^1$, ist S_4 auflösbar. Dies wissen wir bereits aus Beispiel 33.(4).

(2) Es ist S_5 nicht auflösbar, da die nichtabelsche einfache, und also nichtauflösbare Gruppe A_5 enthalten ist; cf. Aufgabe 12.(2). Cf. Beispiel 33.(4). Aber auf der anderen Seite ist ja auch $|\mathrm{S}_5| = 2^3 \cdot 3^1 \cdot 5^1$.

(3) Ist $a = 0$ oder $b = 0$, so ist G sogar nilpotent; cf. Definition 30.(3), Beispiel 33.(2).

(4) Im Fall $a, b \in \{1, 2\}$ wurde die Auflösbarkeit von G in Aufgabe 13 mit gruppentheoretischen Methoden gezeigt.

(5) Nach einer von Feit und Thompson bewiesenen Vermutung von Burnside sind Gruppen ungerader Ordnung auflösbar. Äquivalent hierzu, jede nichtabelsche einfache endliche Gruppe hat gerade Ordnung. Das kann ich nicht zeigen.

5.2 Artin und Brauer

5.2.1 Virtuelle Charaktere

Notation 133 Sei G eine endliche Gruppe.

Sei t die Anzahl der irreduziblen Charaktere von G; cf. Lemma 84. Seien $\chi_1, \ldots, \chi_t$ die irreduziblen Charaktere von G, wobei χ_1 den trivialen Charakter bezeichne. Diese bilden eine Orthonormalbasis des Raums der Klassenfunktionen $\mathrm{Kf}(G)$; cf. Bemerkung 92.(1).

Sei $R \subseteq \mathbf{C}$ ein Teilring.

Sei $K \leqslant H \leqslant G$.

Sei u die Anzahl der Konjugationsklassen von H. Seien $\psi_1, \ldots, \psi_u$ die irreduziblen Charaktere von H.

Definition 134 Sei

$$\mathrm{V}_R(G) \;:=\; {}_R\langle\, \chi_s \,:\, s \in [1,t] \,\rangle \;=\; \{\, \textstyle\sum_{s\in[1,t]} r_s\, \chi_s \,:\, r_s \in R \text{ für } s \in [1,t] \,\}$$

die Menge der *virtuellen Charaktere von G mit Koeffizienten in R.*

Wir schreiben auch $\mathrm{V}(G) := \mathrm{V}_{\mathbf{Z}}(G)$. Ein virtueller Charakter mit Koeffizienten in $\mathbf{Z}$ heißt auch kurz *virtueller Charakter von G.*

Es ist $\mathrm{V}_{\mathbf{C}}(G) = \mathrm{Kf}(G)$.

Bemerkung 135 Seien $z_s \in \mathbf{C}$ für $s \in [1,t]$ gegeben. Es ist $\sum_{s\in[1,t]} z_s\,\chi_s$ genau dann ein Charakter, wenn $z_s \in \mathbf{Z}_{\geqslant 0}$ für $s \in [1,t]$; cf. Bemerkung 94.(1).

Ist $\chi = \sum_{s\in[1,t]} z_s\,\chi_s$ ein virtueller Charakter, ist also $z_s \in \mathbf{Z}$ für $s \in [1,t]$, und schreiben wir

$$\begin{aligned} \chi_+ &:= \sum_{s\in[1,t],\ z_s>0} z_s\,\chi_s \\ \chi_- &:= \sum_{s\in[1,t],\ z_s<0} (-z_s)\,\chi_s\ , \end{aligned}$$

so sind χ_+ und χ_- Charaktere und $\chi = \chi_+ - \chi_-$. Virtuelle Charaktere sind also genau die Klassenfunktionen, die sich als Differenz zweier Charaktere schreiben lassen.

Bemerkung 136 *Es ist* $\mathrm{Kf}(G)$ *mit der punktweisen Addition und Multiplikation ein kommutativer Ring, mit* $1_{\mathrm{Kf}(G)} = \chi_1$ *.*

Es ist $\mathrm{V}_R(G) \subseteq \mathrm{Kf}(G)$ *ein Teilring.*

Via $R \longrightarrow \mathrm{V}_R(G)$, $r \longmapsto r\chi_1$ *ist* $\mathrm{V}_R(G)$ *eine R-Algebra, die R-linear isomorph zu $R^{\oplus t}$ ist.*

Beweis. Nach Definition ist $\mathrm{V}_R(G) \subseteq \mathrm{Kf}(G)$ eine additive Untergruppe.

Es ist $1_{\mathrm{Kf}(G)} = \chi_1 \in \mathrm{V}_R(G)$.

Seien $\chi,\ \psi\ \in\ \mathrm{V}_R(G)$. Schreibe $\chi = \sum_s r_s\,\chi_s$ und $\psi = \sum_s r'_s\,\chi_s$ mit $r_s\,, r'_s\ \in\ R$ für $s \in [1,t]$. Es wird

$$\chi\cdot\psi\ =\ \sum_{s,s'} r_s\,r'_{s'}\,\chi_s\cdot\chi_{s'}\ \in\ \mathrm{V}_R(G)\ ,$$

da $\chi_s\cdot\chi_{s'}$ stets ein Charakter ist; cf. Lemma 110.

Schließlich ist $R \longrightarrow \mathrm{V}_R(G)$, $r \longmapsto r\chi_1$ ein Ringmorphismus, der $\mathrm{V}_R(G)$ zu einer R-Algebra macht. ▫

Beispiel 137 Es ist $\mathrm{X}(\mathrm{S}_3) = \left(\begin{smallmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & 0 & -1 \end{smallmatrix}\right)$; cf. Beispiel 93.(1).

Umformungen mit $\mathrm{GL}_3(\mathbf{Z})$ von links liefern die Zeilen von $\left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{smallmatrix}\right)$ als $\mathbf{Z}$-lineare Erzeuger.

Also ist $\mathrm{V}(\mathrm{S}_3) \simeq \{\,(a,b,c) \in \mathbf{Z}^{\times 3}\ :\ a \equiv_2 b,\ a \equiv_3 c\,\}$.

Definition 138

(1) Sei $\psi = \sum_{s\in[1,u]} r_s\,\psi_s \in \mathrm{V}_R(H)$, wobei $r_s \in R$ für $s \in [1,u]$.
Setze $\psi\uparrow_H^G := \sum_{s\in[1,u]} r_s(\psi_s\uparrow_H^G) \in \mathrm{V}_R(G)$; cf. Definition 116.
Dies liefert eine Abbildung

$$\begin{aligned} \mathrm{V}_R(H) &\xrightarrow{\ \mathrm{ind}\uparrow_H^G\ } \mathrm{V}_R(G) \\ \psi &\longmapsto \psi\uparrow_H^G\ . \end{aligned}$$

(2) Wir haben den Morphismus von R-Algebren

$$\begin{array}{rcl} \mathrm{V}_R(G) & \xrightarrow{\mathrm{res}\downarrow_H^G} & \mathrm{V}_R(H) \\ \chi & \longmapsto & \chi\downarrow_H^G \, , \end{array}$$

wobei $\chi\downarrow_H^G(h) := \chi(h)$ für $h \in H$; cf. Definition 114.

Bemerkung 139

(1) *Für $\psi \in \mathrm{V}_R(H)$ und $g \in G$ ist*

$$\psi\uparrow_H^G(g) \;=\; \frac{1}{|H|} \sum_{x \in G,\ {}^x g \in H} \psi({}^x g) \, .$$

Insbesondere stimmen für einen Charakter ψ die Definitionen 116 *und* 138.(1) *überein.*

(2) *Für $\psi \in \mathrm{V}_R(H)$ und $\chi \in \mathrm{V}_R(G)$ ist*

$$(\psi \cdot (\chi\downarrow_H^G))\uparrow_H^G \;=\; (\psi\uparrow_H^G) \cdot \chi \, .$$

Es ist das Bild $\mathrm{ind}\uparrow_H^G(\mathrm{V}_R(H))$ ein Ideal in $\mathrm{V}_R(G)$.

(3) *Es ist $\mathrm{ind}\uparrow_H^G \circ \mathrm{ind}\uparrow_K^H = \mathrm{ind}\uparrow_K^G$, als Abbildungen von $\mathrm{V}_R(K)$ nach $\mathrm{V}_R(G)$.*
Es ist $\mathrm{ind}\uparrow_K^K = \mathrm{id}_{\mathrm{V}_R(K)}$.

(4) *Für $\psi \in \mathrm{V}_R(H)$ und $\chi \in \mathrm{V}_R(G)$ ist*

$${}_G(\psi\uparrow_H^G, \chi) \;=\; {}_H(\psi, \chi\downarrow_H^G) \, .$$

Beweis.

Zu (1). Schreiben wir $\psi = \sum_s r_s \, \psi_s$ mit $r_s \in R$, so wird

$$\begin{array}{rcl} \psi\uparrow_H^G(g) & = & \sum_s r_s \, \psi_s\uparrow_H^G(g) \\ & \overset{\text{L. } 117}{=} & \sum_s r_s \frac{1}{|H|} \sum_{x \in G,\ {}^x g \in H} \psi_s({}^x g) \\ & = & \frac{1}{|H|} \sum_{x \in G,\ {}^x g \in H} \psi({}^x g) \, . \end{array}$$

Kurz gesagt, die fragliche Gleichheit gilt, da sie für Charaktere gilt und da beide Seiten R-linear in ψ sind.

Zu (2). Es ist

$$(\psi \cdot (\chi\downarrow_H^G))\uparrow_H^G \;=\; (\psi\uparrow_H^G) \cdot \chi$$

da dies für Charaktere zutrifft und da beide Seiten R-linear in ψ und in χ sind; cf. Aufgabe 36.(1).

Nach Konstruktion ist ind_H^G eine R-lineare Abbildung. Also ist ihr Bild eine additive Untergruppe von $\mathrm{V}_R(G)$. Wegen $(\psi\mathrm{res}_H^G) \cdot \chi \in \mathrm{ind}_H^G(\mathrm{V}_R(H))$ ist dieses Bild auch ein Ideal.

Zu (3). Sei $\kappa \in \mathrm{V}_R(K)$. Die Gleichheiten $\kappa\mathrm{res}_K^H\mathrm{res}_H^G = \kappa\mathrm{res}_K^G$ und $\kappa\mathrm{res}_K^K = \kappa$ gelten, da sie für Charaktere gelten und jeweils beide Seiten R-linear in κ sind; cf. Bemerkung 121.(2).

Zu (4). Die Gleichheit gilt für Charaktere, und beide Seiten sind R-linear in ψ und χ; cf. Lemma 120. □

5.2.2 Artin

Sei G eine endliche Gruppe. Sei χ_1 der triviale Charakter von G, mit $\chi_1(g) = 1$ für $g \in G$.

Definition 140

(1) Wir schreiben $\mathrm{Zyk}(G)$ für die Menge der zyklischen Untergruppen der endlichen Gruppe G.

(2) Sei $R \subseteq \mathbf{C}$ ein Teilring. Wir betrachten die R-lineare Abbildung

$$\begin{array}{ccc} \bigoplus_{U \in \mathrm{Zyk}(G)} \mathrm{V}_R(U) & \xrightarrow{\mathrm{ind}_{\mathrm{Zyk}(G)}^G} & \mathrm{V}_R(G) \\ (\psi_U)_{U \in \mathrm{Zyk}(G)} & \longmapsto & \sum_{U \in \mathrm{Zyk}(G)} \psi_U\mathrm{res}_U^G \,. \end{array}$$

Sei $\mathrm{V}_{R,\mathrm{Zyk}}(G) := \sum_{U \in \mathrm{Zyk}(G)} \mathrm{ind}_U^G(\mathrm{V}_R(U)) \subseteq \mathrm{V}_R(G)$ ihr Bild.

Wir schreiben auch $\mathrm{V}_{\mathrm{Zyk}}(G) := \mathrm{V}_{\mathbf{Z},\mathrm{Zyk}}(G)$

Definition 141 Sei U eine endliche zyklische Gruppe.

Wir definieren $\vartheta_U \in \mathrm{Kf}(U) = \mathrm{V}_{\mathbf{C}}(U)$ als

$$\begin{array}{ccc} U & \xrightarrow{\vartheta_U} & \mathbf{C} \\ x & \longmapsto & \vartheta_U(x) := |U|\,\partial_{\langle x\rangle,U} \,. \end{array}$$

Es ist also $\vartheta_U(x)$ gleich $|U|$, falls x ein Erzeuger von U ist, und 0 sonst.

Beispiel 142 Ist $U = \mathrm{C}_4 = \langle\, a \,:\, a^4 \,\rangle$, so ist

$$\vartheta_U(a^0) \;=\; 0\,, \quad \vartheta_U(a^1) \;=\; 4\,, \quad \vartheta_U(a^2) \;=\; 0\,, \quad \vartheta_U(a^3) \;=\; 4\,.$$

Lemma 143 *Es ist*

$$|G|\chi_1 \;=\; \sum_{U \in \mathrm{Zyk}(G)} \vartheta_U\mathrm{res}_U^G \,.$$

Beweis. Für $g \in G$ ist

$$\begin{aligned}
\textstyle\sum_{U \in \mathrm{Zyk}(G)} \vartheta_U 1_U^G(g) &\overset{\text{B. 139.(1)}}{=} \textstyle\sum_{U \in \mathrm{Zyk}(G)} \frac{1}{|U|} \sum_{x \in G,\ {}^x g \in U} \vartheta_U({}^x g) \\
&= \textstyle\sum_{U \in \mathrm{Zyk}(G)} \frac{1}{|U|} \sum_{x \in G,\ {}^x g \in U} |U|\, \partial_{\langle {}^x g \rangle, U} \\
&= \textstyle\sum_{U \in \mathrm{Zyk}(G)} \sum_{x \in G} \partial_{\langle {}^x g \rangle, U} \\
&= \textstyle\sum_{x \in G} \sum_{U \in \mathrm{Zyk}(G)} \partial_{\langle {}^x g \rangle, U} \\
&= \textstyle\sum_{x \in G} 1 \\
&= |G| \\
&= |G| \chi_1(g) \ .
\end{aligned}$$

□

Lemma 144 *Sei U eine endliche zyklische Gruppe. Es ist $\vartheta_U \in \mathrm{V}(U)$.*

Beweis. Induktion über $|U|$. Sei φ_1 der triviale Charakter von U.

Sei die Aussage für alle zyklischen Gruppen kleinerer Ordnung als U bekannt. Es ist

$$|U| \varphi_1 \ = \ \textstyle\sum_{V \leqslant U} \vartheta_V 1_V^U \ = \ \vartheta_U + \sum_{V < U} \vartheta_V 1_V^U \ ;$$

cf. Lemma 143, Lösung zu Aufgabe 5, Bemerkung 139.(3). Für $V < U$ ist nach Induktionsvoraussetzung $\vartheta_V \in \mathrm{V}(V)$, und somit auch auch $\vartheta_V 1_V^U \in \mathrm{V}(U)$. Da auch $|U|\varphi_1 \in \mathrm{V}(U)$ ist, folgt $\vartheta_U \in \mathrm{V}(U)$. □

> Beachte, daß bei einem Induktionsbeweis wie dem zu Lemma 144 kein Induktionsanfang erforderlich ist.

Satz 145 (Artin)

Weiterhin sei G eine endliche Gruppe. Weiterhin bezeichne $\mathrm{Zyk}(G)$ die Menge der zyklischen Untergruppen von G.

Der Ring $\mathrm{V}(G)$ der virtuellen Charaktere von G wurde in Definition 134 und Bemerkung 136 eingeführt.

Die additive Untergruppe $\mathrm{V}_{\mathrm{Zyk}}(G) \subseteq \mathrm{V}(G)$ der Summen aus von zyklischen Untergruppen nach G induzierten virtuellen Charakteren stammt aus Definition 140.

Es ist

$$|G|\mathrm{V}(G) \ \subseteq \ \mathrm{V}_{\mathrm{Zyk}}(G) \ \subseteq \ \mathrm{V}(G) \ .$$

In anderen Worten, für $\chi \in \mathrm{V}(G)$ ist $|G|\chi$ eine $\mathbf{Z}$-Linearkombination aus von zyklischen Untergruppen nach G induzierten Charakteren.

Abermals in anderen Worten, es ist $|G| \cdot \big(\mathrm{V}(G)/\mathrm{V}_{\mathrm{Zyk}}(G) \big) = 0$.

Somit ist $\mathrm{V}(G)/\mathrm{V}_{\mathrm{Zyk}}(G)$ eine endliche abelsche Gruppe, deren Ordnung $|G|^t$ teilt, wobei t die Anzahl der Konjugationsklassen von G ist.

Beweis. Es ist

$$|G|\chi \;=\; |G|\chi_1 \cdot \chi \overset{\text{L. }143}{=} \sum_{U \in \mathrm{Zyk}(G)} (\vartheta_U 1_U^G) \cdot \chi \overset{\text{B. }139.(2)}{=} \sum_{U \in \mathrm{Zyk}(G)} (\vartheta_U \cdot (\chi|_U^G))1_U^G \overset{\text{L. }144}{\in} \mathrm{V}_{\mathrm{Zyk}}(G)\ .$$

□

Korollar 146 *Es ist* $\mathrm{V}_{\mathbf{Q},\mathrm{Zyk}}(G) = \mathrm{V}_{\mathbf{Q}}(G)$.

In anderen Worten, jeder virtuelle Charakter von G mit Koeffizienten in $\mathbf{Q}$, insbesondere also jeder Charakter von G, ist eine $\mathbf{Q}$-Linearkombination aus von zyklischen Untergruppen nach G induzierten Charakteren.

Beweis. Sei χ ein Charakter von G. Schreibe $|G|\chi = \sum_{i\in[1,k]} z_i\, \psi_i 1_{U_i}^G$, wobei $k \in \mathbf{Z}_{\geqslant 0}$, sowie $U_i \in \mathrm{Zyk}(G)$, ψ_i Charakter von U_i und $z_i \in \mathbf{Z}$ für $i \in [1,k]$; cf. Satz 145. Dann ist $\chi = \sum_{i\in[1,k]} \underbrace{z_i\, |G|^{-1}}_{\in \mathbf{Q}}\, \psi_i 1_{U_i}^G$. □

5.2.3 Brauer

5.2.3.1 Irreduzible Charaktere überauflösbarer Gruppen

Sei G eine überauflösbare endliche Gruppe; cf. Definition 30.(2).

Bemerkung 147 *Ist G nichtabelsch, dann gibt es $\mathrm{Z}(G) < N \trianglelefteqslant G$ mit N abelsch.*

Beweis. Es ist $G/\mathrm{Z}(G)$ überauflösbar; cf. Aufgabe 12.(6). Da G nichtabelsch ist, ist $G/\mathrm{Z}(G) \neq 1$. Bestehe

$$\mathrm{Z}(G) \;=\; G_n \;\lhd\; G_{n-1} \;\lhd\; G_{n-2} \;\lhd\; \cdots \;\lhd\; G_1 \;\lhd\; G_0 \;=\; G$$

aus den Urbildern einer (nichtredundanten) überauflösenden Kette von $G/\mathrm{Z}(G)$, wobei $n \in \mathbf{Z}_{\geqslant 1}$.

Wir setzen $N := G_{n-1}$. Es ist $\mathrm{Z}(G) < N \trianglelefteqslant G$. Bleibt zu zeigen, daß N abelsch ist. Nach Definition einer überauflösenden Kette ist $N/\mathrm{Z}(G)$ zyklisch. Sei $x \in N$ mit $\langle x\mathrm{Z}(G)\rangle = N/\mathrm{Z}(G)$ gewählt. Zwei gegebene Elemente von N können wir also in der Form $x^i z$ und $x^j w$ schreiben, wobei $i,\, j \in \mathbf{Z}$ und $z,\, w \in \mathrm{Z}(G)$. Es folgt $(x^i z)(x^j w) = x^{i+j} zw = (x^j w)(x^i z)$. Also ist N abelsch. □

Cf. Kommentar zu Lösung zu Aufgabe 13.(2).

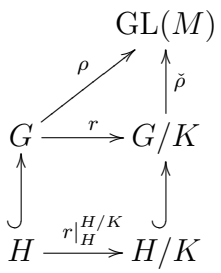
Lemma 148 *Sei χ ein irreduzibler Charakter von G. Dann gibt es eine Untergruppe $H \leqslant G$ und einen Charakter ψ von H mit $\psi(1) = 1$ und $\psi 1_H^G = \chi$.*

Beweis. Induktion nach $|G|$.

Sei M ein einfacher $\mathbf{C}G$-Modul mit $\chi = \chi_M$. Schreibe $k := \dim_{\mathbf{C}} M = \chi(1)$.

Sei $\rho = \rho_M : G \longrightarrow \mathrm{GL}(M)$ die zugehörige Darstellung. Schreibe $K := \operatorname{Kern} \rho$.

Fall $K \neq 1$. Sei $r : G \longrightarrow G/K$, $g \longmapsto gK$ der Restklassenmorphismus. Es gibt eine Darstellung $\check{\rho}$ von G/K mit $\check{\rho} \circ r = \rho$. Also gilt auch für den zugehörigen Charakter $\check{\chi}$ von G/K, daß $\check{\chi} \circ r = \chi$; cf. Bemerkung 113. Da mit G auch G/K überauflösbar ist und da $|G/K| < |G|$, folgt mit Induktion, daß es eine Untergruppe $K \leqslant H \leqslant G$ und einen Charakter $\check{\psi}$ von H/K gibt mit $\check{\psi}(1) = 1$ und $\check{\psi}1_{H/K}^{G/K} = \check{\chi}$; cf. Aufgabe 12.(6).



Es ist $\psi := \check{\psi} \circ r|_H^{H/K}$ ein Charakter von H. Es ist $\psi(1) = (\check{\psi} \circ r)(1) = 1$. Ferner ist

$$\psi 1_H^G \;=\; (\check{\psi} \circ r|_H^{H/K}) 1_H^G \;\overset{\text{A. 45}}{=}\; (\check{\psi} 1_{H/K}^{G/K}) \circ r \;=\; \check{\chi} \circ r \;=\; \chi \,.$$

Fall $K = 1$.

Subfall G abelsch. Es ist $\chi(1) = 1$, da wegen $\mathbf{C}G$ kommutativ alle direkten Faktoren in der Wedderburn-Zerlegung gleich $\mathbf{C}^{1\times 1}$ sind; cf. Satz 67, Korollar 82, Notation 78. Also können (und müssen) wir $H := G$ und $\psi := \chi$ wählen.

Subfall G nichtabelsch. Sei $\mathrm{Z}(G) < N \trianglelefteqslant G$ mit N abelsch; cf. Bemerkung 147. Da ρ injektiv ist, folgt, daß $\mathrm{Z}(\rho(G)) = \rho(\mathrm{Z}(G)) < \rho(N) \trianglelefteqslant \rho(G)$ ist. Folglich gibt es ein $n \in N$ mit $\rho(n) \notin {}_{\mathbf{C}}\langle \mathrm{id}_M \rangle$.

Annahme, es gibt ein primitives Idempotent $\varepsilon \in \mathrm{Z}(\mathbf{C}N) = \mathbf{C}N$ mit $\varepsilon M = M$. Sei $M = \bigoplus_{i\in[1,k]} S_i$ mit S_i einfachem (und eindimensionalem) $\mathbf{C}N$-Modul für $i \in [1,k]$; cf. Bemerkung 77. Da $\varepsilon M = M$ ist, ist $\varepsilon S_i = S_i$ für $i \in [1,k]$. Somit ist $S_i \simeq S_j$ als $\mathbf{C}N$-Moduln für $i, j \in [1,k]$; cf. Lemma 81, Aufgabe 22. Also ist $\rho_{S_i}(n) = \rho_{S_j}(n)$ für $i, j \in [1,k]$. Es folgt

$$\rho(n) \;=\; \rho_M(n) \;=\; \rho_{S_1}(n) \cdot \mathrm{id}_M \;.$$

Aber $\rho(n) \notin {}_{\mathbf{C}}\langle \mathrm{id}_M \rangle$, und wir haben einen *Widerspruch.*

Cf. auch Lösung zu Aufgabe 43.(3).

Daher gibt es eine Untergruppe $N \trianglelefteqslant L < G$ und einen Charakter φ von L mit $\chi = \varphi 1_L^G$; cf. Aufgabe 43.(2). Da mit G auch L überauflösbar ist und da $|L| < |G|$ ist, folgt mit

Induktion, daß es ein $H \leqslant L$ und einen Charakter ψ von H mit $\psi(1) = 1$ und $\psi 1_H^L = \varphi$ gibt. Wir erhalten

$$\psi 1_H^G \overset{\text{B. 121.(2)}}{=} \psi 1_H^L 1_L^G \;=\; \varphi 1_L^G \;=\; \chi \,,$$

cf. Aufgabe 12.(5). ▫

5.2.3.2 Erzeugen und schneiden

Sei G eine endliche Gruppe.

Wir erinnern an den Teilring $\mathcal{O} \subseteq \mathbf{C}$ der algebraisch ganzen Zahlen; cf. Definition 100.

Bemerkung 149 *Sei $a \in \mathbf{Z}$. Es ist $a\mathcal{O} \cap \mathbf{Z} = a\mathbf{Z}$.*

Beweis. O.E. ist $a \neq 0$. Zu zeigen ist nur $a\mathcal{O} \cap \mathbf{Z} \overset{!}{\subseteq} a\mathbf{Z}$. Die Multiplikation mit a gibt eine Bijektion von $\mathbf{C}$ nach $\mathbf{C}$, so daß wir äquivalent $\mathcal{O} \cap a^{-1}\mathbf{Z} \overset{!}{\subseteq} \mathbf{Z}$ zeigen können. Aber es ist $\mathcal{O} \cap a^{-1}\mathbf{Z} \subseteq \mathcal{O} \cap \mathbf{Q} \overset{\text{A. 29.(3)}}{=} \mathbf{Z}$. ▫

Lemma 150 *Sei $A \leqslant \mathrm{V}(G)$ eine additive Untergruppe. Es ist ${}_{\mathcal{O}}\langle A\rangle \cap \mathrm{V}(G) = A$.*

> Ersetzt man in dieser Aussage $\mathcal{O}$ etwa durch $\mathbf{C}$, so wird sie i.a. falsch.

Beweis. Seien $\chi_1\,,\ \ldots\,,\ \chi_t$ die verschiedenen irreduziblen Charaktere von G. Es ist $\mathrm{V}(G) = {}_{\mathbf{Z}}\langle \chi_1\,, \ldots, \chi_t\rangle$; cf. Definition 134. Schreibe $A = {}_{\mathbf{Z}}\langle\, \psi_i \,:\, i \in [1,t]\,\rangle$ mit $\psi_i \in \mathrm{V}(G)$ für $i \in [1,t]$; cf. Aufgabe 29.(1).

Schreibe $\psi_i = \sum_s z_{s,i}\,\chi_s$ für $i \in [1,t]$, wobei $z_{s,i} \in \mathbf{Z}$. Sei $Z = (z_{s,i}) \in \mathbf{Z}^{t\times t}$. Nach Elementarteilersatz gibt es $U = (u_{i,j})_{i,j} \in \mathrm{GL}_t(\mathbf{Z})$ und $V = (v_{i,j})_{i,j} \in \mathrm{GL}_t(\mathbf{Z})$ mit $U^{-1}ZV = \mathrm{diag}(d_1\,, \ldots, d_t) \in \mathbf{Z}^{t\times t}$. Setze $\varphi_i := \sum_s u_{s,i}\,\chi_s$. Da $U \in \mathrm{GL}_t(\mathbf{Z})$ ist, ist

$$\mathrm{V}(G) \;=\; {}_{\mathbf{Z}}\langle\, \varphi_i \,:\, i \in [1,t]\,\rangle\,.$$

Wegen $U\,\mathrm{diag}(d_1\,, \ldots, d_t) = ZV$ ist ferner

$$d_i\,\varphi_i \;=\; \textstyle\sum_s u_{s,i}\,d_i\,\chi_s \;=\; \sum_{s,j} z_{s,j}\,v_{j,i}\,\chi_s \;=\; \sum_j v_{j,i}\,\psi_j$$

für $i \in [1,t]$. Da $V \in \mathrm{GL}_t(\mathbf{Z})$ ist, folgt

$$A \;=\; {}_{\mathbf{Z}}\langle\, d_i\,\varphi_i \,:\, i \in [1,t]\,\rangle\,,$$

und also

$${}_{\mathcal{O}}\langle A\rangle \;=\; {}_{\mathcal{O}}\langle\, d_i\,\varphi_i \,:\, i \in [1,t]\,\rangle\,.$$

Es ist $\mathrm{V}_{\mathbf{C}}(G) = {}_{\mathbf{C}}\langle \mathrm{V}(G)\rangle = {}_{\mathbf{C}}\langle\, \varphi_i \,:\, i \in [1,t]\,\rangle$. Da $\dim_{\mathbf{C}} \mathrm{V}_{\mathbf{C}}(G) = t$ ist, folgt, daß $(\varphi_i)_{i\in[1,t]}$ eine $\mathbf{C}$-lineare Basis von $\mathrm{V}_{\mathbf{C}}(G)$ ist.

Zu zeigen ist nur ${}_{\mathcal{O}}\langle A\rangle \cap \mathrm{V}(G) \overset{!}{\subseteq} A$. Sei $\sum_i \alpha_i \varphi_i \in \mathrm{V}(G)$ gegeben, wobei $\alpha_i \in \mathbf{Z}$ für $i \in [1,t]$. Da $(\varphi_i)_{i\in[1,t]}$ ein $\mathbf{C}$-linear unabhängiges Tupel ist, ist $\sum_i \alpha_i \varphi_i \in {}_{\mathcal{O}}\langle A\rangle$ genau dann, wenn $\alpha_i = \beta_i d_i$ ist für gewisse $\beta_i \in \mathcal{O}$ für $i \in [1,t]$. Dann aber ist $\alpha_i \in \mathbf{Z} \cap d_i\mathcal{O} \overset{\text{B. }149}{=} d_i\mathbf{Z}$, und folglich $\sum_i \alpha_i \varphi_i \in A$. ▫

5.2.3.3 Eine Variante des Satzes von Artin

Schreibe $\zeta := \zeta_{|G|}$.

Sei $\mathbf{Z}[\zeta]$ das Bild des Ringmorphismus $\mathbf{Z}[X] \longrightarrow \mathbf{C}$, $X \longmapsto \zeta$. Da $\zeta \in \mathcal{O}$ ist, ist $\mathbf{Z}[\zeta] \subseteq \mathcal{O}$; cf. Aufgabe 29.(2).

Sei χ_1 der triviale Charakter von G.

Lemma 151 *Sei $\varphi \in \mathrm{V}_{\mathbf{C}}(G)$ mit $\varphi(g) \in \mathbf{Z}[\zeta]$ für $g \in G$.*

Es ist $|G|\varphi \in \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{Zyk}}(G) \subseteq \mathrm{V}_{\mathbf{Z}[\zeta]}(G)$.

I.e. es ist $|G|\varphi$ eine $\mathbf{Z}[\zeta]$-Linearkombination aus von zyklischen Untergruppen induzierten Charakteren.

Beweis. Es ist $|G|\chi_1 = \sum_{U\in \mathrm{Zyk}(G)} \vartheta_U\rfloor_U^G$; cf. Definition 141, Lemma 143. Also ist

$$|G|\varphi \;=\; |G|\chi_1 \cdot \varphi \;=\; \textstyle\sum_{U\in \mathrm{Zyk}(G)} \vartheta_U\rfloor_U^G \cdot \varphi \;\overset{\text{B. }139}{=}\; \sum_{U\in \mathrm{Zyk}(G)} (\vartheta_U \cdot \varphi\rfloor_U^G)\rceil_U^G \,.$$

Es bleibt zu zeigen, daß $\vartheta_U \cdot \varphi\rfloor_U^G \in \mathrm{V}_{\mathbf{Z}[\zeta]}(U)$ für $U \in \mathrm{Zyk}(G)$. Ist ψ ein irreduzibler Charakter von U, so wird in der Tat

$${}_U(\vartheta_U \cdot \varphi\rfloor_U^G, \psi) \;=\; \tfrac{1}{|U|} \textstyle\sum_{u\in U} |U|\, \partial_{\langle u\rangle,U}\, \varphi(u)\, \overline{\psi(u)} \;=\; \sum_{u\in U} \partial_{\langle u\rangle,U}\, \varphi(u)\, \overline{\psi(u)} \;\overset{\text{A. }25.(1)}{\in}\; \mathbf{Z}[\zeta]\,;$$

cf. Bemerkung 94.(1). ▫

> Im Unterschied zum Satz 145 von Artin wird nicht mehr $\varphi \in \mathrm{V}(G)$, sondern nur noch $\varphi \in \mathrm{V}_{\mathbf{C}}(G)$ mit stets $\varphi(g) \in \mathbf{Z}[\zeta]$ vorausgesetzt, aber auch nur noch gefolgert, daß φ eine $\mathbf{Z}[\zeta]$-Linearkombination der von zyklischen Untergruppen induzierten Charakteren ist, nicht mehr notwendig eine $\mathbf{Z}$-Linearkombination.

5.2.3.4 An einer Primzahl

Sei G eine endliche Gruppe. Sei $p \in \mathbf{Z}_{>0}$ prim.

Bemerkung 152 (und Definition)
Sei $g \in G$. Sei $|\langle g\rangle| = p^a\, n$ mit $a \in \mathbf{Z}_{\geqslant 0}$ und $n \in \mathbf{Z}_{\geqslant 1}$ mit $n \not\equiv_p 0$.

Es gibt eindeutig bestimmte Elemente g_{u} und g_{r} in G mit den Eigenschaften (1), (2) *und* (3).

(1) *Es ist* $g = g_{\mathrm{u}}\, g_{\mathrm{r}} = g_{\mathrm{r}}\, g_{\mathrm{u}}$.

(2) *Es ist* $|\langle g_{\mathrm{u}}\rangle|$ *eine Potenz von* p.

(3) *Es ist* $|\langle g_{\mathrm{r}}\rangle| \not\equiv_p 0$.

Es heißt g_{u} *der* p-unipotente *und* g_{r} *der* p-reguläre *Anteil von* g.

Es sind g_{u} *und* g_{r} *in* $\langle g\rangle$ *enthalten.*

Es ist $g_{\mathrm{u}}^i := (g_{\mathrm{u}})^i = (g^i)_{\mathrm{u}}$ *und* $g_{\mathrm{r}}^i := (g_{\mathrm{r}})^i = (g^i)_{\mathrm{r}}$ *für* $i \in \mathbf{Z}$.

Es ist $|\langle g_{\mathrm{u}}\rangle| = p^a$ *und* $|\langle g_{\mathrm{r}}\rangle| = n$. *Folglich ist* $\langle g\rangle = \langle g_{\mathrm{u}}\rangle \times \langle g_{\mathrm{r}}\rangle$.

Es ist $g = g_{\mathrm{r}}$ *genau dann, wenn* $|\langle g\rangle| \not\equiv_p 0$. *Wir nennen* g *diesenfalls* p-regulär.

Beweis. Wähle $z,\, w \in \mathbf{Z}$ mit

$$zp^a + wn \;=\; 1\ .$$

Existenz. Setze $g_{\mathrm{u}} := g^{wn}$ und $g_{\mathrm{r}} := g^{zp^a}$. Es wird

$$g \;=\; g^1 \;=\; g^{wn} g^{zp^a} \;=\; g_{\mathrm{u}}\, g_{\mathrm{r}} = g_{\mathrm{r}}\, g_{\mathrm{u}}\ .$$

Ferner ist $(g_{\mathrm{u}})^{p^a} = g^{wnp^a} = 1^w = 1$ und $(g_{\mathrm{r}})^n = g^{zp^an} = 1^z = 1$.

Eindeutigkeit. Seien $x,\, y \in G$ mit $|\langle x\rangle|$ eine Potenz von p, mit $|\langle y\rangle| \not\equiv_p 0$ und mit $g = xy = yx$. Dann ist $1 = g^{p^an} = x^{p^an} y^{p^an}$, und folglich $x^{p^an} = y^{-p^an}$. Da $|\langle x^{p^an}\rangle|$ eine Potenz von p ist und $|\langle y^{-p^an}\rangle| \not\equiv_p 0$, folgt $x^{p^an} = 1$ und $y^{p^an} = 1$. Da $|\langle x\rangle|$ eine Potenz von p und nun auch ein Teiler von p^an ist, folgt, daß $|\langle x\rangle|$ ein Teiler von p^a ist. Da $|\langle y\rangle| \not\equiv_p 0$ und nun auch ein Teiler von $p^a\, n$ ist, folgt, daß $|\langle y\rangle|$ ein Teiler von n ist. Somit erhalten wir

$$\begin{array}{rcccccl} g_{\mathrm{u}} & = & g^{wn} & = & x^{wn}y^{wn} & = & x^{1-zp^a} \;=\; x \\ g_{\mathrm{r}} & = & g^{zp^a} & = & x^{zp^a}y^{zp^a} & = & y^{1-nw} \;=\; y\ . \end{array}$$

Nach Konstruktion sind $g_{\mathrm{u}}\,,\ g_{\mathrm{r}} \in \langle g\rangle$.

Für $i \in \mathbf{Z}$ ist $g^i = (g_{\mathrm{u}})^i (g_{\mathrm{r}})^i = (g_{\mathrm{r}})^i (g_{\mathrm{u}})^i$, die Ordnung von $(g_{\mathrm{u}})^i$ ist eine p-Potenz, die Ordnung von $(g_{\mathrm{r}})^i$ ist teilerfremd zu p. Also ist $(g^i)_{\mathrm{u}} = (g_{\mathrm{u}})^i$ und $(g^i)_{\mathrm{r}} = (g_{\mathrm{r}})^i$.

Wir haben schon gesehen, daß $|\langle g_{\mathrm{u}}\rangle|$ ein Teiler von p^a ist und daß $|\langle g_{\mathrm{r}}\rangle|$ ein Teiler von n ist. Schreibe $s := |\langle g_{\mathrm{u}}\rangle| \cdot |\langle g_{\mathrm{r}}\rangle|$. Es genügt zu zeigen, daß $p^a\, n$ ein Teiler von s ist. Aber es ist

$$g^s \;=\; (g_{\mathrm{u}})^s \cdot (g_{\mathrm{r}})^s \;=\; 1\ .$$

Ist schließlich $|\langle g\rangle| \not\equiv_p 0$, dann ist $a = 0$, sodaß mit $z = 1$ und $w = 0$ folgt, daß $g_{\mathrm{r}} = g^{zp^a} = g$. ▫

Definition 153

(1) Eine endliche Gruppe heißt *p-fastzyklisch,* falls sie isomorph zu einem direkten Produkt aus einer zyklischen Gruppe von Ordnung teilerfremd zu p und einer p-Gruppe ist.

Die Menge der p-fastzyklischen Untergruppen von G wird $\mathrm{FZyk}_p(G)$ geschrieben.

Es ist $\mathrm{Zyk}(G) \subseteq \mathrm{FZyk}_p(G)$; cf. Definition 140, Bemerkung 152.

Jede p-Untergruppe von G ist p-fastzyklisch.

(2) Sei $R \subseteq \mathbf{C}$ ein Teilring. Betrachte die R-lineare Abbildung

$$\begin{array}{ccc} \displaystyle\bigoplus_{H \in \mathrm{FZyk}_p(G)} \mathrm{V}_R(H) & \xrightarrow{\mathrm{ind}\uparrow^G_{\mathrm{FZyk}_p(G)}} & \mathrm{V}_R(G) \\ (\psi_H)_{H \in \mathrm{FZyk}_p(G)} & \longmapsto & \sum_{H \in \mathrm{FZyk}_p(G)} \psi_H\uparrow^G_H \,. \end{array}$$

Sei $\mathrm{V}_{R,\mathrm{FZyk},p}(G) := \sum_{H \in \mathrm{FZyk}_p(G)} \mathrm{ind}\uparrow^G_H(\mathrm{V}_R(H)) \subseteq \mathrm{V}_R(G)$ ihr Bild.

Wir schreiben auch $\mathrm{V}_{\mathrm{FZyk},p}(G) := \mathrm{V}_{\mathbf{Z},\mathrm{FZyk},p}(G)$.

Cf. Satz 145 von Artin.

Bemerkung 154 *Jede Untergruppe einer p-fastzyklischen Gruppe ist p-fastzyklisch.*

Beweis. Sei $m \in \mathbf{Z}_{\geqslant 1}$ teilerfremd zu p. Sei $\mathrm{C}_m = \langle\, a \,:\, a^m \,\rangle$. Sei P eine p-Gruppe. Sei $U \leqslant \mathrm{C}_m \times P$. Wir haben zu zeigen, daß U eine p-fastzyklische Gruppe ist.

Es genügt zu zeigen, daß

$$U \overset{!}{=} \{\, a^i \,:\, i \in \mathbf{Z},\ (a^i, 1) \in U \,\} \times \{\, x \,:\, x \in P,\ (1, x) \in U \,\}\,;$$

cf. Lösung zu Aufgabe 5.

Zu $\overset{!}{\geqslant}$. Sind $i \in \mathbf{Z}$ mit $(a^i, 1) \in U$ und $x \in P$ mit $(1, x) \in U$ gegeben, dann ist auch $(a^i, x) = (a^i, 1)(1, x) \in U$.

Zu $\overset{!}{\leqslant}$. Sei $(a^i, x) \in U$, wobei $i \in \mathbf{Z}$. Es ist $(a^i, x)_{\mathrm{u}} = (1, x) \in \langle (a^i, x) \rangle \leqslant U$ und $(a^i, x)_{\mathrm{r}} = (a^i, 1) \in \langle (a^i, x) \rangle \leqslant U$, da diese beiden Elemente kommutieren, Ordnung eine p-Potenz resp. Ordnung teilerfremd zu p haben und im Produkt (a^i, x) ergeben. Also ist (a^i, x) in der rechten Seite enthalten. ▫

Bemerkung 155

Sei $g \in G$ ein p-reguläres Element. Sei P eine p-Untergruppe von $\mathrm{C}_G(g)$.

Sei $H := \langle \{g\} \cup P \rangle$. Dann ist H eine p-fastzyklische Gruppe.

Genauer gesagt, wir haben einen Gruppenisomorphismus $\langle g\rangle \times P \xrightarrow{\sim} H$, $(g^i, x) \longmapsto g^i x$, *wobei* $i \in \mathbf{Z}$. *Insbesondere ist* $|H| = |\langle g\rangle| \cdot |P|$.

Umgekehrt ist jede p-fastzyklische Untergruppe von G ist von dieser Form.

Beweis. Die Abbildung

$$\begin{array}{ccccc} \langle g\rangle & \times & P & \xrightarrow{f} & G \\ (g^i & , & x) & \longmapsto & g^i\, x\ , \end{array}$$

wobei $i \in \mathbf{Z}$, ist ein Gruppenmorphismus mit Bild H, da Elemente aus $\langle g\rangle$ mit Elementen aus P kommutieren.

Es ist f injektiv. Denn ist $1 = f((g^i, x)) = g^i\, x$, dann ist $g^{-i} = x \in P \cap \langle g\rangle = 1$, da nur 1 eine Ordnung hat, die zugleich p-Potenz und teilerfremd zu p ist.

Sei umgekehrt $\tilde{H} \leqslant G$ eine p-fastzyklische Untergruppe von G. Dann gibt es ein $\tilde{m} \in \mathbf{Z}_{\geqslant 1}$ teilerfremd zu p, eine p-Gruppe $\tilde{Q}$ und einen injektiven Gruppenmorphismus $\mathrm{C}_{\tilde{m}} \times \tilde{Q} \xrightarrow{f} G$ mit Bild $\tilde{H}$. Schreibe $\mathrm{C}_{\tilde{m}} = \langle\, \tilde{a}\ :\ \tilde{a}^{\tilde{m}}\,\rangle$. Es ist $\tilde{g} := f((\tilde{a}, 1))$ ein p-reguläres Element von G. Es ist $\tilde{P} := f(1 \times \tilde{Q})$ eine p-Untergruppe von $\mathrm{C}_G(\tilde{g})$, da die Elemente von $1 \times \tilde{Q}$ bereits in $\mathrm{C}_{\tilde{m}} \times \tilde{Q}$ mit $(\tilde{a}, 1)$ vertauschen. Schließlich ist $\tilde{H} = \langle \{\tilde{g}\} \cup \tilde{P}\rangle$, da bereits $\mathrm{C}_{\tilde{m}} \times \tilde{Q} = \langle \{(\tilde{a}, 1)\} \cup (1 \times \tilde{Q})\rangle$ ist. ▫

Lemma 156 *Sei* $\varphi \in \mathrm{V}_{\mathcal{O}}(G)$ *mit* $\varphi(g) \in \mathbf{Z}$ *für* $g \in G$.

Für $g \in G$ *ist*

$$\varphi(g)\ \equiv_p\ \varphi(g_{\mathrm{r}})\,;$$

cf. Bemerkung 152.

Beweis. Da g und g_{r} in $\langle g\rangle$ liegen, können wir dank Restriktion o.E. annehmen, daß $G = \langle g\rangle$ ist. Schreibe $\varphi(g) = \sum_s a_s\, \chi_s$, wobei stets $a_s \in \mathcal{O}$ ist und χ_s ein irreduzibler Charakter von G ist. Insbesondere ist stets $\chi_s(1) = 1$; cf. e.g. Beispiel 86. Sei $\rho_s : G \longrightarrow \mathrm{GL}_1(\mathbf{C})$ die zu χ_s gehörige Darstellung. Es ist $\rho_s(g) = \chi_s(g)$ für $g \in G$ und also $\chi_s(g^k) = \chi_s(g)^k$ für $k \in \mathbf{Z}$.

Sei $q := |\langle g_{\mathrm{u}}\rangle|$. Es ist q eine Potenz von p. Es ist $g^q = (g_{\mathrm{r}}\, g_{\mathrm{u}})^q = g_{\mathrm{r}}^q$ und also

$$\chi_s(g)^q\ =\ \chi_s(g^q)\ =\ \chi_s(g_{\mathrm{r}}^q) = \chi_s(g_{\mathrm{r}})^q$$

stets. Damit wird

$$\varphi(g)^q\ =\ (\textstyle\sum_s a_s\, \chi_s(g))^q\ \equiv_{p\mathcal{O}}\ \sum_s a_s^q\, \chi_s(g)^q\ =\ \sum_s a_s^q\, \chi_s(g_{\mathrm{r}})^q\ \equiv_{p\mathcal{O}}\ \varphi(g_{\mathrm{r}})^q\ .$$

Somit ist $\varphi(g)^q - \varphi(g_{\mathrm{r}})^q \in p\,\mathcal{O} \cap \mathbf{Z} \overset{\text{B.149}}{=} p\mathbf{Z}$. Da $a \equiv_p a^q$ ist für $a \in \mathbf{Z}$, folgt

$$\varphi(g)\ \equiv_p\ \varphi(g)^q\ \equiv_p\ \varphi(g_{\mathrm{r}})^q\ \equiv_p\ \varphi(g_{\mathrm{r}})\ .$$

▫

Lemma 157 *Schreibe* $\zeta := \zeta_{|G|}$.

Sei g *ein* p*-reguläres Element von* G*.*

Wir können diesem ein Element $\varphi_g \in \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{FZyk},p}(G)$ *zuordnen mit den folgenden Eigenschaften* (1), (2) *und* (3)*.*

(1) *Es ist* $\varphi_g(x) \in \mathbf{Z}$ *für* $x \in G$*.*

(2) *Es ist* $\varphi_g(g) \not\equiv_p 0$ *in* $\mathbf{Z}$*.*

(3) *Es ist* $\varphi_g(x) = 0$ *für alle* p*-regulären Elemente* $x \in G$*, die nicht zu* g *konjugiert sind.*

Beweis. Schreibe $n := |\langle g\rangle|$. Sei P eine p-Sylowgruppe von $\mathrm{C}_G(g)$; cf. Satz 13.

Es ist $H := \langle \{g\} \cup P\rangle \in \mathrm{FZyk}_p(G)$ und $|H| = n \cdot |P|$; cf. Bemerkung 155.

Sei $\gamma : \langle g\rangle \longrightarrow \mathbf{C}$, $x \longmapsto n\,\partial_{x,g}$. Es ist $\gamma \in \mathrm{V}_{\mathbf{Z}[\zeta_n]}(\langle g\rangle) \subseteq \mathrm{V}_{\mathbf{Z}[\zeta]}(\langle g\rangle)$ nach Lemma 151.

> Das ist allerdings mit Kanonen auf Spatzen geschossen. Unter Verwendung der irreduziblen Charaktere $\chi_i : \langle g\rangle \longrightarrow \mathbf{C}$, $g \mapsto \zeta_n^i$ von $\langle g\rangle$ für $i \in [0, n-1]$ erkennen wir ebenfalls, daß $\gamma = \sum_{i\in[0,n-1]} \zeta_n^{-i}\,\chi_i \in \mathrm{V}_{\mathbf{Z}[\zeta_n]}(\langle g\rangle)$ ist; cf. Lösung zu Aufgabe 17, Beispiel 86.(2).

Wir haben den Gruppenmorphismus $\pi : H \longrightarrow \langle g\rangle$, $g^i\,x \longmapsto g^i$ für $i \in \mathbf{Z}$ und $x \in P$; cf. Bemerkung 155.

Sei $\hat\gamma := \gamma \circ \pi$, i.e. sei $\hat\gamma(g^i\,x) := \gamma(g^i)$ für $i \in \mathbf{Z}$ und $x \in P$.

Da $\gamma \in \mathrm{V}_{\mathbf{Z}[\zeta]}(\langle g\rangle)$ ist, ist $\hat\gamma \in \mathrm{V}_{\mathbf{Z}[\zeta]}(H)$; cf. Bemerkung 113.

Da $H \in \mathrm{FZyk}_p(G)$ ist, folgt

$$\varphi_g \;:=\; \hat\gamma|_H^G \;\in\; \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{FZyk},p}(G)\ .$$

Ferner hat mit γ auch $\hat\gamma$ und also auch φ_g alle Werte in $\mathbf{Z}$, i.e. (1) ist erfüllt; cf. Lemma 117.

Für ein p-reguläres Element $x \in G$ und für $y \in G$ ist ${}^yx \in H$ genau dann, wenn ${}^yx \in \langle g\rangle$; cf. Bemerkung 155; daher wird

$$\begin{aligned}
\varphi_g(x) &\overset{\text{L. }117}{=} \tfrac{1}{|H|}\textstyle\sum_{y\in G,\ {}^yx\in H} \hat\gamma({}^yx)\\
&= \tfrac{1}{n\cdot|P|}\textstyle\sum_{y\in G,\ {}^yx\in\langle g\rangle} \gamma({}^yx)\\
&= \tfrac{1}{n\cdot|P|}\textstyle\sum_{y\in G,\ {}^yx\in\langle g\rangle} n\,\partial_{{}^yx,g}\\
&= \tfrac{1}{|P|}\textstyle\sum_{y\in G} \partial_{{}^yx,g}\\
&= \tfrac{|\mathrm{C}_G(g)|}{|P|}\,\partial_{G_x,G_g}\ .
\end{aligned}$$

Der letzte Schritt gilt, denn ist $z \in G$ mit ${}^zx = g$ gefunden, dann ist für $y \in G$ die Aussage ${}^yx = g$ äquivalent zu ${}^{yz^-}g = g$, i.e. zu $yz^- \in \mathrm{C}_G(g)$, i.e. zu $y \in \mathrm{C}_G(g)z$.

Da $|\mathrm{C}_G(g)|/|P| \not\equiv_p 0$ ist, sind (2) und (3) erfüllt. ▫

Wollte man es vermeiden, p-fastzyklische Untergruppen zu verwenden, wäre es eine naheliegende Idee, im Beweis von Lemma 157 das γ direkt von $\langle g\rangle$ nach G zu induzieren. Dann aber wäre $\gamma\uparrow^G_{\langle g\rangle}(g) = n^{-1}\sum_{y\in G,\ {}^yg\in\langle g\rangle}\gamma({}^yg) = \sum_{y\in G}\partial_{{}^yg,g} \;=\; |\mathrm{C}_G(g)|$, sodaß (2) verletzt wäre, sobald nur $|\mathrm{C}_G(g)| \equiv_p 0$ ist. Was auch bei p-regulären Elementen $g \in G$ der Fall sein kann, man denke etwa an $\mathrm{C}_G(1) = G$.

Lemma 158 *Es gibt ein* $\varphi \in \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{FZyk},p}(G)$ *mit* $\varphi(x) \in \mathbf{Z} \smallsetminus p\mathbf{Z}$ *für alle* $x \in G$.

Beweis. Sei $G = \bigsqcup_{s\in[1,t]} {}^Gg_s$. Sei o.E. $t' \in [1,t]$ so gegeben, daß g_s für $s \in [1,t']$ ein p-reguläres Element ist, für $s \in [t'+1,t]$ nicht.

Setze $\varphi := \sum_{s\in[1,t']}\varphi_{g_s} \in \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{FZyk},p}(G)$; cf. Lemma 157. Wie seine Summanden hat auch φ alle Werte in $\mathbf{Z}$; cf. Lemma 157.(1).

Sei $x \in G$. Es ist x_r konjugiert zu g_a für ein $a \in [1,t']$. Es wird

$$\varphi(x) \overset{\text{L. }156}{\equiv_p} \varphi(x_\mathrm{r}) \;=\; \varphi(g_a) \;=\; \textstyle\sum_{s\in[1,t']}\varphi_{g_s}(g_a) \overset{\text{L. }157.(3)}{=} \varphi_{g_a}(g_a) \overset{\text{L. }157.(2)}{\not\equiv_p} 0\ .$$

□

Lemma 159 *Die Ordnung der abelschen Gruppe* $\mathrm{V}(G)/\mathrm{V}_{\mathrm{FZyk},p}(G)$ *ist endlich und teilerfremd zu* p*; cf. Definition* 153.(2).

Beweis. Sei $|G| = p^a\,n$ mit $a \in \mathbf{Z}_{\geqslant 0}$ und $n \not\equiv_p 0$. Sei χ_1 der triviale Charakter von G. Schreibe $\zeta := \zeta_{|G|}$.

Da $\mathrm{V}(G)$ eine endlich erzeugte abelsche Gruppe ist, genügt es zu zeigen, daß $n\big(\mathrm{V}(G)/\mathrm{V}_{\mathrm{FZyk},p}(G)\big) \overset{!}{=} 0$ ist, i.e. daß $n\mathrm{V}(G) \overset{!}{\subseteq} \mathrm{V}_{\mathrm{FZyk},p}(G)$.

Es genügt zu zeigen, daß $n\chi_1 \overset{!}{\in} \mathrm{V}_{\mathrm{FZyk},p}(G)$. Denn es ist

$$\mathrm{V}_{\mathrm{FZyk},p}(G) \;=\; \textstyle\sum_{H\in\,\mathrm{FZyk}_p(G)} \mathrm{ind}\uparrow^G_H(\mathrm{V}(H)) \;\subseteq\; \mathrm{V}(G)$$

ein Ideal als Summe von Idealen; cf. Bemerkung 139.(2).

Es genügt zu zeigen, daß $n\chi_1 \overset{!}{\in} \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{FZyk},p}(G)$. Denn dann ist

$$\begin{aligned} n\chi_1 \quad &\in \quad \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{FZyk},p}(G) \cap \mathrm{V}(G) \\ &= \quad \mathbf{z}[\zeta]\langle \mathrm{V}_{\mathrm{FZyk},p}(G)\rangle \cap \mathrm{V}(G) \\ &\subseteq \quad \mathcal{o}\langle \mathrm{V}_{\mathrm{FZyk},p}(G)\rangle \cap \mathrm{V}(G) \\ &\overset{\text{L. }150}{=} \quad \mathrm{V}_{\mathrm{FZyk},p}(G)\ . \end{aligned}$$

Wähle zu diesem Zwecke nun $\varphi \in \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{FZyk},p}(G)$ mit $\varphi(g) \in \mathbf{Z} \smallsetminus p\mathbf{Z}$ für $g \in G$; cf. Lemma 158.

Sei $k := |\,\mathrm{GL}_1(\mathbf{Z}/p^a\mathbf{Z})|$. Es ist $\varphi^k(g) \equiv_{p^a} 1$ für $g \in G$. Also ist $(\chi_1 - \varphi^k)(g) \equiv_{p^a} 0$ und somit $(n(\chi_1 - \varphi^k))(g) \equiv_{|G|} 0$ für $g \in G$. Mit Lemma 151 folgt unter Verwendung von $\mathrm{Zyk}(G) \subseteq \mathrm{FZyk}_p(G)$, daß

$$n(\chi_1 - \varphi^k) \;\in\; \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{FZyk},p}(G)\;.$$

Da $\varphi \in \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{FZyk},p}(G)$ liegt und letzteres ein Ideal in $\mathrm{V}_{\mathrm{Z}[\zeta]}(G)$ ist nach Bemerkung 139.(2), ist auch

$$n\varphi^k \;\in\; \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{FZyk},p}(G)\;.$$

Folglich ist auch

$$n\chi_1 \;\in\; \mathrm{V}_{\mathbf{Z}[\zeta],\mathrm{FZyk},p}(G)\;.$$

als Summe dieser beiden Elemente. ▫

Ist p kein Teiler von $|G|$, so folgt Lemma 159 bereits aus Satz 145.

5.2.3.5 Der Satz von Brauer

Sei G eine endliche Gruppe.

Definition 160

(1) Eine endliche Gruppe heißt *fastzyklisch,* falls sie q-fastzyklisch ist für eine Primzahl $q \in \mathbf{Z}_{\geqslant 1}$; cf. Definition 153.

Die Menge der fastzyklischen Untergruppen von G wird $\mathrm{FZyk}(G)$ geschrieben.

(2) Sei

$$\mathrm{V}_{\mathrm{FZyk}}(G) \;:=\; \textstyle\sum_{q\text{ prim}} \mathrm{V}_{\mathrm{FZyk},q}(G) \;=\; \sum_{H\in\mathrm{FZyk}(G)} \mathrm{ind}_H^G(\mathrm{V}(H)) \;\subseteq\; \mathrm{V}(G)\;;$$

cf. Definition 153.(2).

Satz 161 (Brauer) *Es ist* $\mathrm{V}_{\mathrm{FZyk}}(G) = \mathrm{V}(G)$.

In Worten, jeder virtuelle Charakter von G, insbesondere also jeder Charakter von G, ist eine $\mathbf{Z}$-Linearkombination aus von fastzyklischen Untergruppen nach G induzierten Charakteren.

Beweis. Sei $p \in \mathbf{Z}_{\geqslant 1}$ eine Primzahl. Es ist $\mathrm{V}_{\mathrm{FZyk},p}(G) \subseteq \mathrm{V}_{\mathrm{FZyk}}(G) \subseteq \mathrm{V}(G)$. Nun ist $\mathrm{V}(G)/\mathrm{V}_{\mathrm{FZyk},p}(G)$ endlich, und daher

$$|\mathrm{V}(G)/\mathrm{V}_{\mathrm{FZyk},p}(G)| \;=\; |\mathrm{V}(G)/\mathrm{V}_{\mathrm{FZyk}}(G)| \cdot |\mathrm{V}_{\mathrm{FZyk}}(G)/\mathrm{V}_{\mathrm{FZyk},p}(G)|\;,$$

was eine zu p teilerfremde Zahl ist; cf. Lemma 159. Also ist $|\mathrm{V}(G)/\mathrm{V}_{\mathrm{FZyk}}(G)|$ endlich und teilerfremd zu p.

Da dies für alle Primzahlen p gilt, muß $|\mathrm{V}(G)/\mathrm{V}_{\mathrm{FZyk}}(G)| = 1$ sein, i.e. $\mathrm{V}_{\mathrm{FZyk}}(G) = \mathrm{V}(G)$. ▫

Im Unterschied zum Satz 145 von Artin wird nun jeder virtuelle Charakter selbst als $\mathbf{Z}$-Linearkombination geschrieben, nicht mehr nur sein $|G|$-faches, aber auf der anderen Seite nun nur noch als $\mathbf{Z}$-Linearkombination aus von fastzyklischen Untergruppen induzierten Charakteren, nicht mehr aus von zyklischen Untergruppen induzierten Charakteren.

Korollar 162 *Jeder Charakter von G ist eine $\mathbf{Z}$-Linearkombination aus Charakteren, die durch Induktion aus Charakteren von Grad 1 von Untergruppen nach G hervorgehen.*

Dabei kann von diesen Untergruppen noch verlangt werden, daß sie fastzyklisch sind.

Beweis. Mit dem Satz 161 von Brauer dürfen wir annehmen, daß G eine p-fastzyklische Gruppe ist für eine Primzahl $p \in \mathbf{Z}_{\geqslant 1}$; cf. Bemerkung 121.(2).

Ein direktes Produkt nilpotenter Gruppen ist nilpotent; cf. e.g. Satz 37. Also ist G nilpotent als direktes Produkt einer abelschen Gruppe und einer p-Gruppe; cf. Beispiel 33.(1, 2). Insbesondere ist G überauflösbar; cf. Bemerkung 31.

Folglich ist jeder Charakter von G eine $\mathbf{Z}$-Linearkombination (mit Koeffizienten $\geqslant 0$) aus Charakteren, die durch Induktion aus Charakteren von Grad 1 von Untergruppen nach G hervorgehen; cf. Lemma 148. Wie G sind auch diese Untergruppen fastzyklisch; cf. Bemerkung 154. ▫

Beispiel 163 Wir induzieren Charaktere von Grad 1 von fastzyklischen Untergruppen nach S_4 . Wir verwenden die Notation der Lösung zu Aufgabe 37.(3), was die Konjugationsklassenrepräsentanten id, $(1,2)$, $(1,2,3)$, $(1,2,3,4)$, $(1,2)(3,4)$ von S_4 und ihre Charaktertafel angeht. Zum Induzieren von kleinen Untergruppen nach S_4 können wir Korollar 118 verwenden.

Wir haben die 2-fastzyklische Untergruppe $H := \langle (1,2,3,4), (1,3) \rangle \leqslant \mathrm{S}_4$. Wir haben den Isomorphismus $f : \mathrm{D}_8 \xrightarrow{\sim} H$, $a \longmapsto (1,2,3,4)$, $b \longmapsto (1,3)$; cf. Beispiel 25. Also sind die Konjugationsklassen von H repräsentiert von $f(1) = \mathrm{id}$, $f(a^2) = (1,3)(2,4)$, $f(a) = (1,2,3,4)$, $f(ab) = (1,4)(2,3)$, $f(b) = (1,3)$; cf. Lösung zu Aufgabe 24.(1). Dieser Reihenfolge entsprechend notieren wir Charaktere als Zeilenvektoren. Es wird

$$\begin{array}{rcll} \left(1\ 1\ 1 {-1} {-1}\right)\uparrow_H^{\mathrm{S}_4} & = & \left(3 {-1}\ 0\ 1 {-1}\right) & =: \ \varphi_1 \\ \left(1\ 1 {-1} {-1}\ 1\right)\uparrow_H^{\mathrm{S}_4} & = & \left(3\ 1\ 0 {-1} {-1}\right) & =: \ \varphi_2 \ . \end{array}$$

Wir haben die zyklische Untergruppe $I := \langle (1,2,3,4) \rangle \leqslant \mathrm{S}_4$. Ihre Konjugationsklassen sind repräsentiert von id, $(1,2,3,4)$, $(1,3)(2,4)$, $(1,4,3,2)$. Dieser Reihenfolge entsprechend notieren wir Charaktere als Zeilenvektoren; cf. Beispiel 86.(2). Es wird

$$\begin{array}{rcll} \left(1\ 1\ 1\ 1\right)\uparrow_I^{\mathrm{S}_4} & = & \left(6\ 0\ 0\ 2\ 2\right) & =: \ \varphi_3 \\ \left(1 {-1}\ 1 {-1}\right)\uparrow_I^{\mathrm{S}_4} & = & \left(6\ 0\ 0 {-2}\ 2\right) & =: \ \varphi_4 \ . \end{array}$$

Wir haben die zyklische Untergruppe $J := \langle (1,2,3) \rangle \leqslant \mathrm{S}_4$. Ihre Konjugationsklassen sind repräsentiert von id, $(1,2,3)$, $(1,3,2)$. Dieser Reihenfolge entsprechend notieren wir

Charaktere als Zeilenvektoren; cf. Beispiel 86.(2). Es wird

$$\left(1\ \zeta_3\ \zeta_3^2\right)\uparrow_J^{\mathrm{S}_4} \quad = \quad \left(8\ 0\ {-1}\ 0\ 0\right) \quad =: \quad \varphi_5\ .$$

Somit ist, in der Notation der Lösung von Aufgabe 37.(3),

$$\begin{array}{rcll}
\chi_{4,1} & = & \left(1\ 1\ 1\ 1\ 1\right) & = \varphi_2 + \varphi_3 - \varphi_5 \\
\chi_{4,2} & = & \left(1\ {-1}\ 1\ {-1}\ 1\right) & = \varphi_1 + \varphi_4 - \varphi_5 \\
\chi_{4,3} & = & \left(3\ 1\ 0\ {-1}\ {-1}\right) & = \varphi_2 \\
\chi_{4,4} & = & \left(3\ {-1}\ 0\ 1\ {-1}\right) & = \varphi_1 \\
\chi_{4,5} & = & \left(2\ 0\ {-1}\ 0\ 2\right) & = -\varphi_1 - \varphi_2 + \varphi_5\ .
\end{array}$$

Damit sind alle irreduziblen – und damit alle – Charaktere von S_4 als $\mathbf{Z}$-Linearkombinationen aus Charakteren, die durch Induktion aus Charakteren von Grad 1 von fastzyklischen Untergruppen nach S_4 hervorgehen, geschrieben, was Satz 161 und Korollar 162 für $G = \mathrm{S}_4$ bestätigt.

> Cf. Lösung von Aufgabe 45, wo der Satz 145 von Artin für $G = \mathrm{S}_4$ betrachtet wird, und wo für die Darstellung der irreduziblen Charaktere von S_4 als Linearkombination aus von zyklischen Untergruppen induzierten Charakteren ein Nenner 2 benötigt wird.
>
> Cf. auch Aufgaben 50 und 52.

Anhang A

Aufgaben und Lösungen

A.1 Aufgaben

Aufgabe 1 (§1.1) Sei G eine Gruppe.

Sei $f : M \longrightarrow N$ ein Isomorphismus von G-Mengen.

Zeige, daß auch $f^- : N \longrightarrow M$ ein Isomorphismus von G-Mengen ist.

Aufgabe 2 (§1.1) Sei G eine Gruppe.

Sei I eine Menge. Sei M_i eine G-Menge für $i \in I$. Sei X eine G-Menge.

(1) Gib eine Bijektion von ${}_G(\bigsqcup_{i\in I} M_i\,, X)$ nach $\prod_{i\in I}\,{}_G(M_i\,, X)$ an.

(2) Gib eine Bijektion von ${}_G(X, \prod_{i\in I} M_i)$ nach $\prod_{i\in I}\,{}_G(X, M_i)$ an.

(3) Seien M, N und X drei G-Mengen.
Zeige, daß $(M \sqcup N) \times X$ und $(M \times X) \sqcup (N \times X)$ zueinander isomorphe G-Mengen sind.

Aufgabe 3 (§1.1) Sei G eine Gruppe. Sei M eine G-Menge. Sei $X \subseteq M$ eine Teilmenge.

(1) Zeige, daß $\mathrm{C}_G(X) \leqslant G$ und $\mathrm{N}_G(X) \leqslant G$.

(2) Sei $g \in G$. Zeige, daß $\mathrm{C}_G(gX) = {}^g\mathrm{C}_G(X)$ und $\mathrm{N}_G(gX) = {}^g\mathrm{N}_G(X)$.

Aufgabe 4 (§1.1) Betrachte die Gruppe S_3 als S_3-Menge unter Konjugation.

(1) Zerlege S_3 in Bahnen. Bestimme für je einen Bahnenrepräsentanten den Zentralisator.

(2) Sei G eine Gruppe. Sei $U \leqslant G$. Sei M eine G-Menge. Gib eine Bijektion zwischen ${}_G(G/U, M)$ und $\{\, m \in M \,:\, um = m \text{ für } u \in U \,\}$ an.

(3) Bestimme die Anzahl der S_3-äquivarianten Abbildungen von S_3 nach S_3.
(Hinweis: ${}_{\mathrm{S}_3}(\mathrm{S}_3/\mathrm{C}_{\mathrm{S}_3}(\sigma), \mathrm{S}_3)$ zusammensetzen, cf. (1), (2), Aufgabe 2.(1).)

Aufgabe 5 (§1.2) Sei $m \in \mathbf{Z}_{\geqslant 1}$.

Sei $\mathrm{C}_m = \langle x \rangle$ die zyklische Gruppe von Ordnung m. Sei d ein Teiler von m.

Zeige, daß C_m genau eine Untergruppe von Ordnung d hat.

Aufgabe 6 (§1.2) Sei p eine Primzahl. Sei G eine p-Gruppe mit $|G| > 1$. Zeige.

(1) Es ist das Zentrum $\mathrm{Z}(G) := \{\, z \in G \,:\, zg = gz \text{ für } g \in G\}$ von G ungleich 1.
(Hinweis: Lemma 14 auf G.)

(2) Sei $|G| = p^t$ für ein $t \in \mathbf{Z}_{\geqslant 1}$. Sei $s \in [0, t]$. Es ist $|\{H \leqslant G \,:\, |H| = p^s\}| \equiv_p 1$.
(Hinweis: Lemma 14 auf $\{H \leqslant G \,:\, |H| = p^s\}$.)

Aufgabe 7 (§1.2) Sei G eine endliche Gruppe. Zeige.

(1) Sei p eine Primzahl. Schreibe $|G| = p^t n$ mit $t \in \mathbf{Z}_{\geqslant 0}$ und $n \not\equiv_p 0$.
Die Anzahl der p-Sylowgruppen teilt n.
Gibt es genau eine p-Sylowgruppe in G, so ist diese ein Normalteiler in G.

(2) Sei $H \leqslant G$. Sei p eine Primzahl. Sei $P \leqslant H$ eine p-Sylowgruppe von H. Sei $\mathrm{N}_G(P) = \{\, x \in G \,:\, {}^xP = P \,\}$ der Normalisator von P in G, letztere gesehen als G-Menge via Konjugation.
Der Gruppenmorphismus $f : \mathrm{N}_G(P) \longrightarrow G/H$, $x \longmapsto xH$ ist surjektiv.

Aufgabe 8 (§1.2) Eine Gruppe G heißt *einfach,* wenn sie genau zwei Normalteiler enthält, nämlich 1 und G.

(1) Zeige, daß es keine einfache Gruppe der Ordnung 104 gibt.

(2) Sei G eine Gruppe. Sei M eine G-Menge. Zeige, daß die Abbildung $\lambda : G \longrightarrow \mathrm{S}_M$, $g \longmapsto (\lambda(g) : M \to M, m \mapsto gm)$ existiert und ein Gruppenmorphismus ist.

(3) Sei G eine Gruppe. Sei M eine endliche transitive G-Menge mit $|M| > 1$. Zeige, daß es ein $N \lhd G$ gibt, für welches $|G/N|$ ein Teiler von $|M|!$ ist. (Hinweis: Kern λ.)

(4) Zeige, daß es keine einfache Gruppe der Ordnung 72 gibt. (Hinweis: (3) auf Sylow.)

Aufgabe 9 (§1.3.2) Sei $n \geqslant 1$.

Setze

$$\mathrm{S}_{\mathrm{P},n} := \left\langle s_1 , \ldots , s_{n-1} \ : \begin{array}{ll} s_i^2 & \text{für } i \in [1, n-1] \\ (s_i s_{i+1})^3 & \text{für } i \in [1, n-2] \\ (s_i s_j)^2 & \text{für } i,\, j \in [1, n-1] \text{ mit } |i-j| \geqslant 2 \end{array} \right\rangle ;$$

cf. Beispiel 27.

Zeige, daß es den Gruppenisomorphismus

$$\begin{array}{rcll} \mathrm{S}_{\mathrm{P},n} & \xrightarrow[\sim]{f} & \mathrm{S}_n & \\ s_i & \longmapsto & (i, i+1) & \text{für } i \in [1, n-1] \end{array}$$

gibt.

Aufgabe 10 (§1.3.2) Konstruiere einen Automorphismus von S_6, der nicht inner ist, der also nicht durch Konjugation mit einem Element von S_6 gegeben ist.
(Hinweis: Aufgabe 9, $(*,*) \longmapsto (*,*)(*,*)(*,*)$.)

Aufgabe 11 (§1.4) Eine Gruppe G heißt *einfach,* wenn sie genau zwei Normalteiler enthält, nämlich 1 und G; cf. Aufgabe 8.

Sei $n \in \mathbf{Z}_{\geqslant 0}$. Sei $\mathrm{A}_n := \{ \sigma \in \mathrm{S}_n \ : \ \operatorname{sgn} \sigma = 1 \} \trianglelefteqslant \mathrm{S}_n$ die *alternierende Gruppe* auf n Ziffern.

Sei nun $n \in \mathbf{Z}_{\geqslant 5}$. Zeige.

(1) Es ist A_n von der Teilmenge aller Zykeln der Länge 3 erzeugt. Diese bilden eine Konjugationsklasse in A_n.

(2) Es ist A_n einfach. (Hinweis: bewege $\sigma \in \mathrm{A}_n \smallsetminus \{\mathrm{id}\}$ minimal viele Ziffern; zeige, daß σ ein Dreierzykel ist; ansonsten bilde $\sigma \circ \rho \circ \sigma^- \circ \rho^-$ für passendes $\rho \in \mathrm{A}_n$.)

Aufgabe 12 (§1.4) Sei H eine endliche Gruppe. Sei $K \leqslant H$. Zeige.

(1) Ist $K \trianglelefteqslant H$, ist H/K auflösbar und ist K auflösbar, dann ist H auflösbar.

(2) Ist H auflösbar, dann ist auch K auflösbar.

(3) Ist H auflösbar und ist $K \trianglelefteqslant H$, dann ist auch H/K auflösbar.

(4) Ist $K \leqslant \mathrm{Z}(H)$ und ist H/K überauflösbar, dann ist H überauflösbar.

(5) Ist H überauflösbar, dann ist auch K überauflösbar.

(6) Ist H überauflösbar und ist $K \trianglelefteqslant H$, dann ist auch H/K überauflösbar.

(7) Ist $K \leqslant \mathrm{Z}(H)$ und ist H/K nilpotent, dann ist H nilpotent.

(8) Ist H nilpotent, dann ist auch K nilpotent.

(9) Ist H nilpotent und ist $K \trianglelefteq H$, dann ist auch H/K nilpotent.

Aufgabe 13 (§1.4) Seien p und q zwei verschiedene Primzahlen. Zeige.

(1) Jede Gruppe der Ordnung pq ist überauflösbar.

(2) Jede Gruppe der Ordnung p^2q ist auflösbar.

(3) Jede Gruppe der Ordnung p^2q^2 ist auflösbar.

Aufgabe 14 (§1.3.2, §2.1) Zeige, daß

$$\begin{array}{rcl} \mathrm{S}_3 & \longrightarrow & \mathrm{GL}_2(\mathbf{Z}) \\ (1,2) & \longmapsto & \left(\begin{smallmatrix} -2 & -1 \\ 3 & 2 \end{smallmatrix}\right) \\ (2,3) & \mapsto & \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right) \end{array}$$

eine Darstellung von S_3 auf $\mathbf{Z}^{2\times 1}$ über $\mathbf{Z}$ definiert.

Aufgabe 15 (§2.2) Sei R ein kommutativer Ring. Sei G eine endliche Gruppe.

Sei RG der freie R-Modul mit Basis G.

Definiere die R-bilineare Abbildung $(\underset{RG}{\cdot}) : RG \times RG \longrightarrow RG$ durch Angabe der Bilder von Paaren von Basiselementen, viz. $(g,h) \longmapsto g \underset{RG}{\cdot} h := g \underset{G}{\cdot} h$ für $g,\, h \in G$.

Zeige, daß $(RG, +, \underset{RG}{\cdot})$ ein Ring ist.

Aufgabe 16 (§2.2) Sei $n \in \mathbf{Z}_{\geqslant 0}$. Sei R ein kommutativer Ring.

Zeige, daß $\mathrm{Z}(R^{n\times n}) = \{\, r\mathrm{E}_n \,:\, r \in R \,\} = {}_R\langle \mathrm{E}_n \rangle$.

Aufgabe 17 (§2.2) Sei $n \in \mathbf{Z}_{\geqslant 1}$. Sei $A := (\zeta_n^{ij})_{i,j\in[0,n-1]} \in \mathbf{C}^{n\times n}$.

Zeige, daß $A\bar{A} = n \cdot \mathrm{E}_n$ ist. Folgere, daß $\prod_{i,\, j\, \in\, [0,n-1],\, i<j} (\zeta_n^j - \zeta_n^i)^2 = (-1)^{\binom{n-1}{2}} n^n$ ist.

Aufgabe 18 (§2.2, §3.2.1)

(1) Zeige, daß $\mathbf{Q}\mathrm{S}_3 \simeq \mathbf{Q} \times \mathbf{Q}^{2\times 2} \times \mathbf{Q}$ als $\mathbf{Q}$-Algebren und $\mathbf{C}\mathrm{S}_3 \simeq \mathbf{C} \times \mathbf{C}^{2\times 2} \times \mathbf{C}$ als $\mathbf{C}$-Algebren. (Hinweis: Beispiel 39.$(1,3,4)$, cf. Beispiel 50, Bemerkung 60.)

(2) Beschreibe das Bild von $\mathbf{Z}\mathrm{S}_3$ in $\mathbf{Z} \times \mathbf{Z}^{2\times 2} \times \mathbf{Z}$ unter dem ersten in (1) gefundenen Isomorphismus.

Aufgabe 19 (§3.2.1) Sei R ein kommutativer Ring.

Seien $A = (A, \varphi)$, $B = (B, \psi)$ und $C = (C, \xi)$ drei R-Algebren. Zeige.

(1) Via $r \cdot a = ra := \varphi(r)a$ für $r \in R$ und $a \in A$ wird A zu einem R-Modul.

(2) Sei $f : A \longrightarrow B$ ein Ringmorphismus. Es ist f genau dann ein R-Algebrenmorphismus, wenn f eine R-lineare Abbildung ist.

(3) Seien $f : A \longrightarrow B$ und $g : B \longrightarrow C$ Abbildungen. Sei g injektiv. Seien g und $g \circ f$ Morphismen von R-Algebren. Dann ist auch f ein Morphismus von R-Algebren. Insbesondere, ist $g : B \longrightarrow C$ ein R-Algebrenisomorphismus, so auch $g^- : C \longrightarrow B$.

Aufgabe 20 (§3.2.2) Sei A ein Ring. Sei R ein kommutativer Ring.

Sei K ein algebraisch abgeschlossener Körper.

Für einen A-Modul X ist bekanntlich $\operatorname{End}_A X := \{X \xrightarrow{f} X \,:\, f \text{ ist } A\text{-linear}\}$ ein Ring.

Zeige.

(1) Seien M und N einfache A-Moduln. Es enthält $\operatorname{Hom}_A(M, N) \smallsetminus \{0\}$ nur Isomorphismen.

(2) Sei M ein einfacher A-Modul. Es ist der Ring $\operatorname{End}_A M$ ein Schiefkörper.

(3) Sei M ein einfacher A-Modul. Es gibt eine surjektive A-lineare Abbildung $A \longrightarrow M$.

(4) Sei $A = (A, \varphi)$ eine R-Algebra. Sei X ein A-Modul.
Via $R \longrightarrow \operatorname{End}_A X$, $r \longmapsto (x \mapsto \varphi(r)x)$ ist $\operatorname{End}_A X$ eine R-Algebra.

(5) Ist A eine endlichdimensionale K-Algebra und M ein einfacher A-Modul, dann ist $K \simeq \operatorname{End}_A M$ als K-Algebren.

Aufgabe 21 (§3.2.2) Sei K ein Körper.

Seien A und B endlichdimensionale K-Algebren ungleich 0.

Zeige oder widerlege.

(1) Sei $n \in \mathbf{Z}_{\geqslant 1}$. Für $j, k \in [1, n]$ schreiben wir $\mathrm{e}_{j,k} \in K^{n\times n}$ für die Matrix, die an Position (j, k) den Eintrag 1 hat, und ansonsten Nullen.
Für $i \in [1, n]$ ist $K^{n\times n}\mathrm{e}_{i,i}$ ein einfacher $K^{n\times n}$-Modul.
Es ist $K^{n\times n}$ halbeinfach.

(2) Sind A und B halbeinfach, dann auch $A \times B$.

(3) Ist A halbeinfach und ist $f : A \longrightarrow B$ ein surjektiver K-Algebrenmorphismus, dann ist auch B halbeinfach.

(4) Ist A halbeinfach und ist $g : B \longrightarrow A$ ein injektiver K-Algebrenmorphismus, dann ist auch B halbeinfach.

Aufgabe 22 (§3.2.2) Sei K ein Körper.

Sei A eine kommutative endlichdimensionale K-Algebra.

Zeige, daß es (bis auf Reihenfolge) genau eine orthogonale Zerlegung in primitive Idempotente in A gibt. (Hinweis: verwende Bemerkung 64.)

Aufgabe 23 (§3.2.2)

(1) Finde einen Wedderburnisomorphismus für $\mathbf{C}\mathrm{D}_8$.
(Hinweis: Beispiel 25; $\mathrm{D}_8 \twoheadrightarrow \mathrm{C}_2 \times \mathrm{C}_2$; D_8 operiert auf Quadrat.)

(2) Sei $\mathrm{D}_{10} := \langle\, a,\, b \,:\, a^5,\, b^2,\, (ba)^2 \,\rangle$. Finde einen Wedderburnisomorphismus für $\mathbf{C}\mathrm{D}_{10}$.
(Hinweis: $\mathrm{D}_{10} \twoheadrightarrow \mathrm{C}_2$; a auf Diagonalmatrix mit Einheitswurzeln.)

(3) Sei $\mathrm{Q}_8 := \langle\, a,\, b \,:\, a^4,\, a^2b^2,\, b^-aba \,\rangle$. Finde einen Wedderburnisomorphismus für $\mathbf{C}\mathrm{Q}_8$. (Hinweis: $\mathrm{Q}_8 \longrightarrow \mathrm{C}_2 \times \mathrm{C}_2$, Quaternionen in $\mathbf{C}^{2\times 2}$.)

Aufgabe 24 (§4.2) Sei G eine endliche Gruppe.

Erstelle die Charaktertafel von G. (Hinweis: Aufgabe 23.)

(1) $G = \mathrm{D}_8$.

(2) $G = \mathrm{D}_{10}$.

(3) $G = \mathrm{Q}_8$.

(4) Ist $\mathrm{D}_8 \simeq \mathrm{Q}_8$? Wieso stellt sich diese Frage?

Aufgabe 25 (§4.1) Sei G eine endliche Gruppe. Sei χ ein Charakter von G.

Sei $g \in G$ ein Element von Ordnung $k := |\langle g \rangle|$. Schreibe $\zeta = \zeta_k$.

(1) Zeige, daß $\chi(g) = \sum_{j\in[0,\,k-1]} x_j\, \zeta^j$ für gewisse $x_j \in \mathbf{Z}_{\geqslant 0}$ mit $\sum_{j\in[0,k-1]} x_j = \chi(1)$.

(2) Zeige, daß $\chi(g^{-1}) = \overline{\chi(g)}$ (komplexe Konjugation).

(3) Zeige, daß auch $G \longrightarrow \mathbf{C}$, $h \longmapsto \bar{\chi}(h) := \overline{\chi(h)}$ ein Charakter von G ist.
Folgt aus χ irreduzibel, daß $\bar{\chi}$ irreduzibel ist?
(Hinweis: Dualraum, oder Transposition und Inversion.)

Aufgabe 26 (§4.5.2) Seien R, S und T Ringe. Konstruiere resp. zeige.

(1) Seien M_R und ${}_RN$ gegeben. Sei A eine abelsche Gruppe. Eine Abbildung $M \times N \xrightarrow{f} A$ heißt *R-bilinear* ([3]), falls $f(mr, n) = f(m, rn)$ und $f(m+m', n+n') = f(m,n) + f(m',n) + f(m,n') + f(m',n')$ ist für m, $m' \in M$, n, $n' \in N$ und $r \in R$. Konstruiere eine abelsche Gruppe $M \underset{R}{\otimes} N$ zusammen mit einer R-bilinearen Abbildung $M \times N \xrightarrow{b} M \underset{R}{\otimes} N$, $(m,n) \longmapsto m \otimes n$ derart, daß es für jede R-bilineare Abbildung $M \times N \xrightarrow{f} A$ in eine abelsche Gruppe A genau eine $\mathbf{Z}$-lineare Abbildung $M \underset{R}{\otimes} N \xrightarrow{\tilde{f}} A$ gibt mit $\tilde{f} \circ b = f$. Es heißt $M \underset{R}{\otimes} N$ dann das *Tensorprodukt* von M und N über R.

(2) Gegeben ${}_SM_R$ und ${}_RN$. Es ist $M \underset{R}{\otimes} N$ auf kanonische Weise ein S-Linksmodul. Usf.

(3) Gegeben ${}_RN$. Es ist $R \underset{R}{\otimes} N \simeq N$ als R-Linksmoduln.

(4) Gegeben ${}_SM_R$, ${}_RN_T$ und ${}_TP$. Es ist $(M \underset{R}{\otimes} N) \underset{T}{\otimes} P \simeq M \underset{R}{\otimes} (N \underset{T}{\otimes} P)$ als S-Linksmoduln. Usf.

(5) Gegeben ${}_SM_R$, ${}_RN$ und ${}_RN'$. Es ist $M \underset{R}{\otimes} (N \oplus N') \simeq M \underset{R}{\otimes} N \oplus M \underset{R}{\otimes} N'$ als S-Linksmoduln.

(6) Im allgemeinen ist $b : M \times N \longrightarrow M \underset{R}{\otimes} N$ nicht surjektiv.

Aufgabe 27 (§4.2) Seien A und B Ringe.

Zeige, daß $\mathrm{Z}(A \times B) = \mathrm{Z}(A) \times \mathrm{Z}(B)$.

Aufgabe 28 (§4.2) Wir verwenden Notation 78.

Zeige, daß $B\mathrm{e}_{1,1}^r \not\simeq B\mathrm{e}_{1,1}^s$ als B-Moduln für r, $s \in [1,t]$ mit $r \neq s$.

Aufgabe 29 (§4.4)

Es ist $\mathcal{O} = \{\, z \in \mathbf{C} \,:\, \exists\, f(X) \in \mathbf{Z}[X] \text{ normiert mit } f(z) = 0 \,\}$; cf. Definition 100. Zeige.

(1) Sei A eine endlich erzeugte abelsche Gruppe. Sei $B \subseteq A$ eine Untergruppe.
Es ist B endlich erzeugt. Für B sind nicht mehr Erzeuger erforderlich als für A.

(2) Es ist $\mathcal{O} \subseteq \mathbf{C}$ ein Teilring.

(3) Es ist $\mathcal{O} \cap \mathbf{Q} = \mathbf{Z}$.

Aufgabe 30 (§4.1) Sei G eine endliche Gruppe. Sei χ ein Charakter von G.

Sei $\rho : G \longrightarrow \mathrm{GL}(V)$ eine Darstellung von G mit $\chi = \chi_\rho$.

Zeige, daß $\operatorname{Kern}\chi := \{\, g \in G \,:\, \chi(g) = \chi(1) \,\} \overset{!}{=} \operatorname{Kern}\rho \trianglelefteq G$ ist.

[3] Früher teilweise auch *R-balanciert.*

Aufgabe 31 (§4.6.3) Sei R ein kommutativer Ring. Seien A und B zwei R-Algebren.

Seien ${}_AM_B$, ${}_BN$ und ${}_AP$ (Bi-)Moduln wie angegeben. Zeige.

(1) Es wird $\mathrm{Hom}_A(M,P)$ zu einem B-Linksmodul vermöge $(b \cdot f)(m) := f(mb)$ für $b \in B$, $f \in \mathrm{Hom}_A(M,P)$ und $m \in M$.

(2) Die Abbildungen

$$\begin{array}{rcl} \mathrm{Hom}_A(M \underset{B}{\otimes} N,\, P) & \longleftrightarrow & \mathrm{Hom}_B(N,\, \mathrm{Hom}_A(M,P)) \\ f & \overset{\Phi}{\longmapsto} & \big(n \mapsto (m \mapsto f(m \otimes n))\big) \\ \big(m \otimes n \mapsto (g(n))(m)\big) & \overset{\Psi}{\longmapsto} & g \end{array}$$

sind sich invertierende R-lineare Abbildungen (bezüglich geeigneter R-Modulstrukturen). Cf. Aufgabe 26.(2).

(3) Sei $B \subseteq A$ als R-Teilalgebra vorausgesetzt.

Wir betrachten den Bimodul ${}_AA_B$, wobei $a \cdot x \cdot b := axb$ für $a \in A$, $x \in A$ und $b \in B$, und letzteres Produkt in A ausgeführt werde.

Sei $P|_B$ der Modul P mit der von A nach B eingeschränkten Moduloperation. Es sind

$$\begin{array}{rcl} P|_B & \longleftrightarrow & \mathrm{Hom}_A(A,P) \\ p & \longmapsto & (a \mapsto ap) \\ u(1) & \longmapsfrom & u \end{array}$$

sich invertierende B-lineare Abbildungen.

Aufgabe 32 (§4.4) Sei $\omega : \mathbf{C}\mathrm{S}_3 \longrightarrow \mathbf{C} \times \mathbf{C}^{2\times 2} \times \mathbf{C}$ wie in Aufgabe 18.(1).

Beschreibe $\omega_{\mathrm{Z}}(\mathrm{Z}(\mathbf{Z}\mathrm{S}_3)) \subseteq \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$.

Aufgabe 33 (§4.6.1)

Sei $f : H \longrightarrow G$ ein Gruppenmorphismus zwischen endlichen Gruppen.

Seien χ und ψ irreduzible Charaktere von G. Sei φ eine Klassenfunktion von G.

Zeige oder widerlege.

(1) Es ist $\chi \cdot \varphi$ ein Charakter von G.

(2) Ist $\psi(1) = 1$, dann ist $\chi \cdot \psi$ ein irreduzibler Charakter von G.

(3) Es ist $\chi \circ f$ ein irreduzibler Charakter von H.

(4) Ist f surjektiv, dann ist $\chi \circ f$ ein irreduzibler Charakter von H.

Aufgabe 34 (§4.3) Sei G eine endliche Gruppe. Wir verwenden Notation 78.

Zeige.

(1) Für $(z^s)_s \in \prod_{s\in[1,t]} \mathbf{C}^{n_s\times n_s}$ ist

$$\omega^-\big(z^1\,,\,\ldots\,,\,z^t\big) \;=\; \sum_{g\in G}\Big(\frac{1}{|G|}\sum_{s\in[1,t]} n_s\,\mathrm{tr}\,\big(\omega^s(g^-)\,z^s\big)\Big)g\;.$$

(2) Leite die Aussage von Lemma 89 aus (1) ab.

(3) Was ergibt sich bei Anwendung von $\omega\circ\omega^-$ auf ein Tupel von Matrizen mit nur einem Eintrag gleich 1, den anderen gleich 0 ?

Aufgabe 35 (§4.3) Sei G eine endliche Gruppe.

Schreibe $G = \bigsqcup_{s\in[1,t]} {}^Gg_s$, wobei $t \in \mathbf{Z}_{\geqslant 1}$ und $g_s \in G$ für $s \in [1,t]$.

Sei χ ein Charakter von G.

Zeige, daß $\sum_{s\in[1,t]} \chi(g_s) \in \mathbf{Z}_{\geqslant 0}$. (Hinweis: Skalarprodukt mit G via Konjugation.)

Aufgabe 36 (§4.5, §4.6) Sei G eine endliche Gruppe. Sei $H \leqslant G$.

Seien χ, χ', χ'' Charaktere von G ; seien M, M', M'' jeweils zugehörige $\mathbf{C}G$-Moduln. Sei ψ ein Charakter von H ; sei N ein zugehöriger $\mathbf{C}H$-Modul.

Zeige jeweils vermittels Charakteren und, alternativ, vermittels Moduln.

(1) Es ist $(\psi\cdot(\chi\rfloor_H^G))\uparrow_H^G = (\psi\uparrow_H^G)\cdot\chi$.
Äquivalent, es ist $\mathbf{C}G \underset{\mathbf{C}H}{\otimes} (N\otimes M) \simeq (\mathbf{C}G \underset{\mathbf{C}H}{\otimes} N)\otimes M$.

(2) Es ist $(\chi\cdot\chi')\cdot\chi'' = \chi\cdot(\chi'\cdot\chi'')$. Äquivalent, es ist $(M\otimes M')\otimes M'' \simeq M\otimes(M'\otimes M'')$.

(3) Es ist $\overline{\chi\cdot\chi'} = \bar\chi\cdot\bar\chi'$. Äquivalent, es ist $(M\otimes M')^* \simeq M^*\otimes M'^*$.

Aufgabe 37 (§4.6.2)

(1) Berechne $\chi_i\rfloor_{\mathrm{S}_3}^{\mathrm{S}_4}$ für $i \in [1,3]$. (Notation aus Beispiel 93.(1).)

(2) Konstruiere einen surjektiven Gruppenmorphismus $f : \mathrm{S}_4 \longrightarrow \mathrm{S}_3$ und berechne $\chi_3\circ f$.

(3) Berechne $\mathrm{X}(\mathrm{S}_4)$.
(Hinweis: Multiplizität von Trivialem und Signum in Induzierten, Produkte.)

Aufgabe 38 (§4.6.2, §1.1) Sei G eine endliche Gruppe.

Sei χ_1 der triviale Charakter von G. Sei M eine G-Menge. Zeige.

(1) Sei M transitiv. Sei $m \in M$. Es ist $\chi_{\mathbf{C}M}$ induziert vom trivialen Charakter von $\mathrm{C}_G(m)$ nach G.

(2) Sei M transitiv. Es ist ${}_G(\chi_{\mathbf{C}M}, \chi_1) = 1$.

(3) Die Anzahl der Bahnen von M ist gleich $\frac{1}{|G|} \sum_{g \in G} |\{ m \in M : gm = m \}|$.
(Hinweis: (2).)

(4) Es heiße M *doppelt transitiv,* wenn M eine transitive G-Menge ist und für ein $m \in M$ auch $M \smallsetminus \{m\}$ eine transitive $\mathrm{C}_G(m)$-Menge ist. Ist M doppelt transitiv, so ist $\chi_{\mathbf{C}M}$ Summe zweier irreduzibler Charaktere, einer davon trivial.

Aufgabe 39 (§5.1.1)
Seien $z \in \mathbf{C}$ und $r \in \mathbf{R}_{>0}$ so, daß $|z + r| = |z| + r$.

Zeige, daß $z \in \mathbf{R}_{\geqslant 0}$ ist.

Aufgabe 40 (§5.1.1)

(1) Sei L ein Körper. Sei $K \subseteq L$ ein Teilkörper. Via Inklusion wird L eine K-Algebra.

Sei Γ eine Menge von K-Algebrenmorphismen von L nach L. Zeige, daß Γ eine linear unabhängige Teilmenge des L-Vektorraums $\mathrm{Hom}_K(L, L)$ ist.

Ist L eine endlichdimensionale K-Algebra, so folgere, daß $|\Gamma| \leqslant \dim_K L$ und so insbesondere endlich ist.

(2) Definiere rekursiv $\Phi_m(X) := \frac{X^m - 1}{\prod_{d|m,\ d \neq m} \Phi_d(X)}$ für $m \in \mathbf{Z}_{\geqslant 1}$.

Sei $n \in \mathbf{Z}_{\geqslant 1}$. Schreibe $\zeta := \zeta_n$.

Zeige, daß $\Phi_n(X) \in \mathbf{Z}[X]$ liegt und daß $\Phi_n(X)$ in $\mathbf{Q}[X]$ irreduzibel ist.

Zeige, daß $\Phi_n(X) = \prod_{i \in [0, n-1],\, \mathrm{ggT}(i,n)=1} (X - \zeta^i)$ in $\mathbf{C}[X]$.

Folgere, daß es für $i \in [0, n-1]$ mit $\mathrm{ggT}(i, n) = 1$ einen Isomorphismus von $\mathbf{Q}$-Algebren $\mathbf{Q}(\zeta) \xrightarrow{\sim} \mathbf{Q}(\zeta)$ mit $\zeta \longmapsto \zeta^i$ gibt.

Folgere

$$\{ \xi \in \mathbf{Q}(\zeta) : \tau(\xi) = \xi \text{ für alle } \mathbf{Q}\text{-Algebrenisomorphismen } \mathbf{Q}(\zeta) \xrightarrow[\sim]{\tau} \mathbf{Q}(\zeta) \} = \mathbf{Q}\,.$$

Aufgabe 41 (§4) Seien G und H endliche Gruppen.

Seien χ, $\tilde{\chi}$ Charaktere von G. Sei ψ, $\tilde{\psi}$ Charaktere von H.

(1) Zeige, daß $\chi \boxdot \psi : G \times H \longrightarrow \mathbf{C}$, $(g, h) \longmapsto \chi(g) \cdot \psi(h)$ ein Charakter von $G \times H$ ist; genannt das *äußere Produkt* von χ und ψ.
(Hinweis: Tensorprodukt mit geeigneter Operation, genannt $M \boxtimes N$.)

(2) Zeige, daß ${}_{G\times H}(\chi \boxdot \psi,\, \tilde{\chi} \boxdot \tilde{\psi}) = {}_G(\chi, \tilde{\chi}) \cdot {}_H(\psi, \tilde{\psi})$ ist.

(3) Zeige, daß $\chi \boxdot \psi$ genau dann irreduzibel ist, wenn χ und ψ irreduzibel sind.

(4) Zeige, daß jeder irreduzible Charakter von $G \times H$ ein äußeres Produkt von irreduziblen Charakteren von G und von H ist.

(5) Bestimme die Charaktertafel von $\mathrm{S}_3 \times \mathrm{C}_3$.

Aufgabe 42 (§4.5.2)

(1) Sei G eine endliche Gruppe. Sei M ein endlichdimensionaler $\mathbf{C}G$-Modul. Setze

$$\begin{array}{rcl} \mathrm{S}^2M & := & {}_{\mathbf{C}}\langle\, m \otimes m' + m' \otimes m \,:\, m,\, m' \,\in\, M \,\rangle \;\subseteq\; M \otimes M \\ \Lambda^2 M & := & {}_{\mathbf{C}}\langle\, m \otimes m' - m' \otimes m \,:\, m,\, m' \,\in\, M \,\rangle \;\subseteq\; M \otimes M\,. \end{array}$$

Zeige, daß wir eine direkte Zerlegung $M \otimes M = \mathrm{S}^2M \oplus \Lambda^2 M$ in $\mathbf{C}G$-Teilmoduln haben.

Berechne $\chi_{\mathrm{S}^2 M}$ und $\chi_{\Lambda^2 M}$ ausgehend von χ_M.

(2) Bestimme die Charaktertafel von S_5. (Hinweis: Von S_4; bilde u.a. Λ^2.)

Aufgabe 43 (§4.6.2, §4.4) Sei G eine endliche Gruppe.

Sei M ein einfacher $\mathbf{C}G$-Modul. Sei $\chi := \chi_M$ der zugehörige Charakter von G. Zeige.

(1) Es ist $\chi(1)$ ein Teiler von $\frac{|G|}{|\mathrm{Z}(G)|}$. (Hinweis: Es ist $M^{\boxtimes k}$ auch eine Darstellung der Gruppe $G^{\times k}/\{\,(z_i)_i \in \mathrm{Z}(G)^{\times k} \,:\, z_1 \cdots z_k = 1\,\}$; cf. Aufgabe 41.(1, 2).)

(2) Sei $N \trianglelefteqslant G$. Es gibt $N \trianglelefteqslant H < G$ und einen irreduziblen Charakter ψ von H mit $\chi = \psi\uparrow_H^G$ oder es gibt ein primitives Idempotent $\varepsilon \in \mathrm{Z}(\mathbf{C}N)$ mit $\varepsilon M = M$.
(Hinweis: $H := \{\, g \in G \,:\, g\varepsilon M = \varepsilon M \,\}$.)

(3) Sei $A \trianglelefteqslant G$ ein abelscher Normalteiler. Es ist $\chi(1)$ ein Teiler von $\frac{|G|}{|A|}$.
(Hinweis: Induktion über $|G|$, Fälle wie in (2), verwende (1).)

Aufgabe 44 (§4.6.2, §4.6.3) Sei $H \leqslant G$.

Sei $m_G := \max\{\,\chi(1) \,:\, \chi$ ist irreduzibler Charakter von $G\,\}$. Analog m_H.

Zeige, daß $\frac{m_G}{m_H} \leqslant \frac{|G|}{|H|}$ ist. (Hinweis: Irreduzibler ψ in $\chi\downarrow_H^G$, dann Frobenius.)

Aufgabe 45 (§5.2.3.1) Sei G eine endliche Gruppe. Sei $N \trianglelefteqslant G$.

Sei $r : G \longrightarrow G/N$, $g \longmapsto gN$ der Restklassenmorphismus.

Sei $N \leqslant H \leqslant G$. Sei ψ ein Charakter von H/N.

Zeige, daß $(\psi \circ r\downarrow_H^{H/N})\uparrow_H^G \;=\; (\psi\uparrow_{H/N}^{G/N}) \circ r$ ist.

Aufgabe 46 (§5.2.2)
Bestätige den Satz 145 von Artin für $G = \mathrm{S}_4$.

Genauer gesagt, schreibe für jeden irreduziblen Charakter χ von G den Charakter $|G|\chi$ als $\mathbf{Z}$-Linearkombination aus von zyklischen Untergruppen induzierten Charakteren.

Aufgabe 47 (§4.6) Sei G eine endliche Gruppe. Sei $N \trianglelefteq G$.

Für $g \in G$ sei $c_g : N \longrightarrow N,\ n \longmapsto {}^{g^-}n$. Ist κ ein Charakter von N, so schreiben wir ${}^g\kappa := \kappa \circ c_g$. Beachte, daß ${}^1\kappa = \kappa$ und ${}^{gh}\kappa = {}^g({}^h\kappa)$ für $g,\, h \in G$. Cf. §4.6.4.

Sei χ ein irreduzibler Charakter von G.

Sei ψ ein irreduzibler Charakter von N.

Sei

$$e \ := \ {}_N(\psi, \chi\rfloor_N^G) \overset{\text{L. 120}}{=} {}_G(\psi\restriction_N^G, \chi) \ .$$

Sei $T := \{\, g \in G \,:\, {}^g\psi = \psi \,\} \leqslant G$. Sei $1 \in R \subseteq G$ so, daß $G = \bigsqcup_{r\in R} rT$.

(1) Sei $e \neq 0$ vorausgesetzt.

Zu gegebenem χ können wir ein solches ψ finden, da $\chi\rfloor_N^G \neq 0$.
Zu gegebenem ψ können wir ein solches χ finden, da $\psi\restriction_N^G \neq 0$.

Zeige.

Es ist

$$\chi\rfloor_N^G \ = \ e\textstyle\sum_{r\in R} {}^r\psi \ .$$

Es gibt einen irreduziblen Charakter φ von T mit

$$\begin{aligned} \varphi\rfloor_N^T &= e\psi \\ \varphi\restriction_T^G &= \chi \ . \end{aligned}$$

(2) Es ist $\chi = \psi\restriction_N^G$ genau dann, wenn $e = 1$ und $\chi(g) = 0$ für $g \in G \smallsetminus N$.

Folgende Aufgabe kenne ich von Martin Hertweck und Michael Kauer.

Aufgabe 48 (§4.3) Sei G eine endliche Gruppe. Sei $N \trianglelefteq G$.

Sei χ ein irreduzibler Charakter von G mit $N \not\leqslant \operatorname{Kern}\chi$; cf. Aufgabe 30.

Sei $x \in G$ mit $\mathrm{C}_G(x) \cap N = 1$ gegeben. Folgere $\chi(x) = 0$ und $\mathrm{C}_G(x) \simeq \mathrm{C}_{G/N}(xN)$.

(Hinweis: Satz 90.(2) auf G und auf G/N.)

Aufgabe 49 (§4.6) Sei G eine endliche Gruppe.

Sei $H \leqslant G$ so, daß $H \cap {}^gH = 1$ ist für $g \in G \smallsetminus H$.

Schreibe $N := \{\, n \in G \,:\, {}^Gn \cap H = \emptyset \,\} \sqcup \{1\} = (G \smallsetminus \bigcup_{g \in G} {}^gH) \sqcup \{1\}$.

Zeige $N \trianglelefteqslant G$, $N \cap H = 1$, $NH = G$ und $\mathrm{ggT}(|N|, |G|) = 1$.

Aufgabe 50 (§5.2.3) Zeige oder widerlege.

Sei G eine Gruppe. Für eine Primzahl p sei M_p die Menge der p-Untergruppen von G. Sei $M = \bigcup_{p \text{ prim}} M_p$. Sei χ ein Charakter von G. Es ist χ eine $\mathbf{Z}$-Linearkombination aus von Untergruppen aus M nach G induzierten Charakteren.

Aufgabe 51 (Aufgabe 41, §4.6.2) Seien G und H endliche Gruppen.

Sei $U \leqslant G$. Sei $V \leqslant H$.

Sei φ ein Charakter von U. Sei ψ ein Charakter von V.

Zeige.

$$(\varphi 1_U^G \boxdot \psi 1_V^H) \;=\; (\varphi \boxdot \psi) 1_{U \times V}^{G \times H}$$

Aufgabe 52 (§5.2.3)

Sei $\mathbf{F}_4 := \mathbf{F}_2[T]/(T^2 + T + 1)$ der Körper mit Kardinalität 4.

Schreibe $\alpha := T + \mathbf{F}_2[T](T^2 + T + 1)$. Also ist $\alpha^2 = \alpha + 1$.

Sei $G := \mathrm{GL}_2(\mathbf{F}_4)$.

Gib eine minimale Menge M von fastzyklischen Untergruppen von G an mit der Eigenschaft, daß

$$\begin{array}{ccc} \bigoplus_{U \in M} \mathrm{V}(U) & \xrightarrow{\mathrm{ind}|_M^G} & \mathrm{V}(G) \\ (\varphi_U)_{U \in M} & \longmapsto & \sum_{U \in M} \varphi_U 1_U^G \end{array}$$

surjektiv ist, i.e. daß jeder irreduzible Charakter von G eine $\mathbf{Z}$-Linearkombination aus von Untergruppen aus M nach G induzierten Charakteren ist.

Minimal heiße hierbei, daß jede echte Teilmenge von M diese Eigenschaft nicht mehr hat.

Aufgabe 53 (§4.4)

(1) Sei G eine Gruppe. Schreibe $[g, h] := g^- h^- g h$ für $g,\, h \in G$.

Sei $G' := \langle\, [g, h] \,:\, g,\, h \in G \,\rangle \leqslant G$.

Zeige $G' \trianglelefteqslant G$. Zeige, daß G/G' eine abelsche Gruppe ist.

Bezeichne $\rho : G \longrightarrow G/G'$, $g \longmapsto gG'$ den Restklassenmorphismus. Zeige, daß es für jeden Gruppenmorphismus $\varphi : G \longrightarrow A$ in eine abelsche Gruppe A genau einen Gruppenmorphismus $\bar{\varphi} : G/G' \xrightarrow{A}$ mit $\bar{\varphi} \circ \rho = \varphi$ gibt.

(2) Sei G eine endliche Gruppe. Sei $\mathrm{Irr}(G)$ die Menge ihrer irreduziblen Charaktere.

Zeige, daß $\iota : \mathrm{Irr}(G/G') \longrightarrow \mathrm{Irr}(G)$, $\chi \longmapsto \chi \circ \rho$ eine injektive Abbildung ist.

Zeige $\iota(\mathrm{Irr}(G/G')) = \{\, \psi \in \mathrm{Irr}(G) \,:\, \psi(1) = 1 \,\}$.

Zeige $|G/G'| = |\{\, \psi \in \mathrm{Irr}(G) \,:\, \psi(1) = 1 \,\}|$.

Zeige $G' = \{\, g \in G \,:\, \chi(g) = 1$ für alle $\chi \in \mathrm{Irr}(G)$ mit $\chi(1) = 1 \,\}$.

(3) Sei $p \geqslant 2$ eine Primzahl. Sei G eine nichtabelsche Gruppe mit $|G| = p^3$.

Zeige $|G'| = p$. Zeige, daß G genau $p - 1$ verschiedene irreduzible Charaktere von Grad p hat.

(4) Sei $p \geqslant 2$ eine Primzahl. Sei $k \geqslant 2$. Sei G eine Gruppe mit $|G| = p^k$.

Zeige $|G'| \notin \{p^{k-1}, p^k\}$. Zeige, daß es einen surjektiven Gruppenmorphismus von G nach C_{p^2} oder nach $\mathrm{C}_p \times \mathrm{C}_p$ gibt.

A.2 Lösungen

Aufgabe 1

Zu zeigen ist, daß f^- auch G-äquivariant ist. In der Tat wird

$$f^-(gn) \;=\; f^-(gf(f^-(n))) \;=\; f^-(f(gf^-(n))) \;=\; gf^-(n)$$

für $g \in G$ und $n \in N$.

Cf. Definition 4.

Aufgabe 2

(1) Wir wollen zeigen, daß

$$\begin{array}{rcl} {}_G(\bigsqcup_{i\in I} M_i\,, X) & \longleftrightarrow & \prod_{i\in I}\, {}_G(M_i\,, X) \\ f & \overset{\Phi}{\longmapsto} & (m \mapsto f((m,i)))_{i\in I} \\ ((m,i) \mapsto u_i(m)) & \overset{\Psi}{\longmapsto} & (u_i)_{i\in I} \end{array}$$

wohldefinierte und sich invertierende Abbildung sind.
Zur Wohldefiniertheit von Φ. Zu zeigen ist die G-Äquivarianz von $M_i \to X$, $m \mapsto f((m,i))$. Seien hierzu $g \in G$ und $m \in M$ gegeben. Es wird $gm \mapsto f((gm,i)) = f(g(m,i)) = gf((m,i))$.
Zur Wohldefiniertheit von Ψ. Zu zeigen ist die G-Äquivarianz von $\bigsqcup_{i\in I} M_i \to X$, $(m,i) \mapsto u_i(m)$. Seien hierzu $g \in G$, $i \in I$ und $m \in M_i$ gegeben. Es wird $g(m,i) = (gm,i) \mapsto u_i(gm) = gu_i(m)$.

Zu $\Psi \circ \Phi \overset{!}{=} \mathrm{id}$. Sei $f \in {}_G(\bigsqcup_{i\in I} M_i\,, X)$ gegeben. Es schickt Φ das Element f auf das Element $(m \mapsto f((m,i)))_{i\in I}$. Es schickt Ψ dieses Element auf

$$((m,i) \mapsto (m \mapsto f((m,i)))(m)) \;=\; ((m,i) \mapsto f((m,i))) \;=\; f\,.$$

Zu $\Phi \circ \Psi \overset{!}{=} \mathrm{id}$. Sei $(u_i)_{i\in I} \in \prod_{i\in I}\, {}_G(M_i\,, X)$ gegeben. Es schickt Ψ das Element $(u_i)_{i\in I}$ auf das Element $((m,i) \mapsto u_i(m))$. Es schickt Φ dieses Element auf

$$(m \mapsto ((m,i) \mapsto u_i(m))((m,i)))_{i\in I} \;=\; (m \mapsto u_i(m))_{i\in I} \;=\; (u_i)_{i\in I}\,.$$

(2) Ist $\xi \in \prod_{i\in I} M_i$ und $j \in I$, so bezeichne ξ_j den Eintrag von ξ bei j, i.e. $\xi = (\xi_i)_{i\in I}$.
Wir wollen zeigen, daß

$$\begin{array}{rcl} {}_G(X, \prod_{i\in I} M_i) & \longleftrightarrow & \prod_{i\in I}\, {}_G(X, M_i) \\ f & \overset{\Phi}{\longmapsto} & (x \longmapsto f(x)_i)_{i\in I} \\ (x \mapsto (v_i(x))_{i\in I}) & \overset{\Psi}{\longmapsto} & (v_i)_{i\in I} \end{array}$$

wohldefinierte und sich invertierende Abbildung sind.
Zur Wohldefiniertheit von Φ. Zu zeigen ist die G-Äquivarianz von $X \to M_i\,,\; x \longmapsto f(x)_i$. Seien hierzu $g \in G$ und $x \in X$ gegeben. Es wird $gx \mapsto f(gx)_i = (gf(x))_i = g(f(x)_i)$.
Zur Wohldefiniertheit von Ψ. Zu zeigen ist die G-Äquivarianz von $X \to \prod_{i\in I} M_i\,,\; x \mapsto (v_i(x))_{i\in I}$. Seien hierzu $g \in G$ und $x \in X$ gegeben. Es wird $gx \mapsto (v_i(gx))_{i\in I} = (gv_i(x))_{i\in I} = g(v_i(x))_{i\in I}$.

Zu $\Psi \circ \Phi \overset{!}{=} \mathrm{id}$. Sei $f \in {}_G(X, \prod_{i\in I} M_i)$ gegeben. Es schickt Φ das Element f auf das Element $(x \longmapsto f(x)_i)_{i\in I}$. Es schickt Ψ dieses Element auf

$$(x \mapsto ((x \longmapsto f(x)_i)(x))_{i\in I}) \;=\; (x \mapsto (f(x)_i)_{i\in I}) \;=\; f(x)\,.$$

Zu $\Phi \circ \Psi \overset{!}{=} \mathrm{id}$. Sei $(v_i)_{i\in I} \in \prod_{i\in I} {}_G(X, M_i)$ gegeben. Es schickt Ψ das Element $(v_i)_{i\in I}$ auf das Element $(x \mapsto (v_i(x))_{i\in I})$. Es schickt Φ dieses Element auf

$$(x \longmapsto ((x \mapsto (v_i(x))_{i\in I})(x))_i)_{i\in I} \;=\; (x \longmapsto ((v_i(x))_{i\in I})_i)_{i\in I} \;=\; (x \longmapsto v_i(x))_{i\in I} \;=\; (v_i)_{i\in I}\,.$$

(3) Wir verfügen über die sich gegenseitig invertierenden Abbildungen

$$\begin{array}{rcl} (M \sqcup N) \times X & \longrightarrow & (M \times X) \sqcup (N \times X) \\ ((a,i),x) & \overset{f}{\longmapsto} & ((a,x),i) \\ ((a,i),x) & \overset{f^-}{\longmapsto} & ((a,x),i) \end{array}$$

wobei $a \in M$ oder $a \in N$, $i \in \{1,2\}$ und $x \in X$.

Es genügt uns, dabei die G-Äquivarianz der Abbildung f zu zeigen.

Seien dazu $g \in G$ und $((a,i),x) \in (M \sqcup N) \times X$ gegeben. Wir erhalten

$$f(g((a,i),x)) \;=\; f(((ga,i),gx)) \;=\; ((ga,gx),i) \;=\; (g(a,x),i) \;=\; g((a,x),i) \;=\; gf(((a,i),x))\,.$$

Aufgabe 3

(1) Zu $\mathrm{C}_G(X) \overset{!}{\leqslant} G$. Es ist $1 \in \mathrm{C}_G(X)$, da $1x = x$ für $x \in X$. Seien $g, h \in \mathrm{C}_G(X)$. Wir haben zu zeigen, daß $gh^- \overset{!}{\in} \mathrm{C}_G(X)$. Sei $x \in X$. Wir haben zu zeigen, daß $gh^-x \overset{!}{=} x$. Aus $hx = x$ folgt $x = h^-x$. Folglich ist $gh^-x = gx = x$.

Zu $\mathrm{N}_G(X) \overset{!}{\leqslant} G$. Es ist $1 \in \mathrm{N}_G(X)$, da $1X = X$. Seien $g, h \in \mathrm{N}_G(X)$. Wir haben zu zeigen, daß $gh^- \overset{!}{\in} \mathrm{N}_G(X)$. Dazu haben wir zu zeigen, daß $gh^-X = X$. Aus $hX = X$ folgt $X = h^-X$. Folglich ist $gh^-X = gX = X$.

Cf. Definition 3.

(2) Zu $\mathrm{C}_G(gX) \overset{!}{=} {}^g\mathrm{C}_G(X)$. Sei $g \in G$. Es ist $h \in G$ genau dann in $\mathrm{C}_G(gX)$, wenn $hgx = gx$ für $x \in X$, i.e. $g^-hgx = x$ für $x \in X$, i.e. $g^-hg \in \mathrm{C}_G(X)$, i.e. $h \in {}^g\mathrm{C}_G(X)$.

Zu $\mathrm{N}_G(gX) \overset{!}{=} {}^g\mathrm{N}_G(X)$. Sei $g \in G$. Es ist $h \in G$ genau dann in $\mathrm{N}_G(gX)$, wenn $hgX = gX$, i.e. $g^-hgX = X$, i.e. $g^-hg \in \mathrm{N}_G(X)$, i.e. $h \in {}^g\mathrm{N}_G(X)$.

Aufgabe 4

(1) Die Bahnen sind die Konjugationsklassen

$$\begin{array}{rcl} K_1 & := & \{\mathrm{id}\} \\ K_2 & := & \{(1,2),\,(1,3),\,(2,3)\} \\ K_3 & := & \{(1,2,3),\,(1,3,2)\}\,. \end{array}$$

Es ist $\mathrm{C}_{\mathrm{S}_3}(\mathrm{id}) = \mathrm{S}_3$.

Es ist $\mathrm{C}_{\mathrm{S}_3}((1,2)) = \langle (1,2)\rangle$, e.g. da $(1,2)$ dazugehört, $(1,3)$ nicht, und es zwischen $\langle (1,2)\rangle$ und S_3 keine weitere Untergruppe gibt.

Es ist $\mathrm{C}_{\mathrm{S}_3}((1,2,3)) = \langle (1,2,3)\rangle$, e.g. da $(1,2,3)$ dazugehört, $(2,3)$ nicht, und es zwischen $\langle (1,2,3)\rangle$ und S_3 keine weitere Untergruppe gibt.

(2) Wir wollen zeigen, daß

$$\begin{array}{rcl} {}_G(G/U, M) & \longleftrightarrow & \{\, m \in M \,:\, um = m \text{ für } u \in U \,\} \\ f & \overset{\Phi}{\longmapsto} & f(1U) \\ (gU \mapsto gm) & \overset{\Psi}{\longleftarrow} & m \end{array}$$

wohldefinierte und sich gegenseitig invertierende Abbildungen sind.

Zur Wohldefiniertheit von Φ. Wir haben zu zeigen, daß $uf(1U) \overset{!}{=} f(1U)$ für $u \in U$. In der Tat ist $uf(1U) = f(u \cdot 1U) = f(1U)$.

Zur Wohldefiniertheit von Ψ. Wir haben zu zeigen, daß $gU \mapsto gm$ repräsentantenunabhängig definiert ist und eine G-äquivariante Abbildung ist.

Zur Repräsentantenunabhängigkeit. Seien $g, \tilde{g} \in G$ mit $gU = \tilde{g}U$ gegeben. Dann ist $g^- \tilde{g} \in U$ und also $gm = gg^- \tilde{g}m = \tilde{g}m$.

Zur G-Äquivarianz. Seien $h, g \in G$. Es wird $h \cdot gU = (hg)U \mapsto (hg)m = h \cdot (gm)$.

Zu $\Psi \circ \Phi \overset{!}{=} \mathrm{id}$. Sei $f \in {}_G(G/U, M)$ gegeben. Es schickt Φ das Element f auf das Element $f(1U)$. Es schickt Ψ dieses Element auf

$$(gU \longmapsto gf(1U)) \;=\; (gU \longmapsto f(gU)) \;=\; f\,.$$

Zu $\Phi \circ \Psi \overset{!}{=} \mathrm{id}$. Sei $m \in \{\, m \in M \,:\, um = m \text{ für } u \in U \,\}$ gegeben. Es schickt Ψ das Element m auf das Element $(gU \mapsto gm)$. Es schickt Φ dieses Element auf

$$(gU \mapsto gm)(1U) \;=\; 1m \;=\; m\,.$$

(3) Als S_3-Menge wird

$$\mathrm{S}_3 \overset{(1)}{=} K_1 \sqcup K_2 \sqcup K_3 \overset{\text{L. 5}}{\simeq} (\mathrm{S}_3/\mathrm{S}_3) \sqcup (\mathrm{S}_3/\langle(1,2)\rangle) \sqcup (\mathrm{S}_3/\langle(1,2,3)\rangle)\,.$$

Also wird

$$\begin{array}{rcl} {}_{\mathrm{S}_3}(\mathrm{S}_3\,, \mathrm{S}_3) & \simeq & {}_{\mathrm{S}_3}((\mathrm{S}_3/\mathrm{S}_3) \sqcup (\mathrm{S}_3/\langle(1,2)\rangle) \sqcup (\mathrm{S}_3/\langle(1,2,3)\rangle)\,, \mathrm{S}_3) \\ & \overset{\text{A. 2.(1)}}{\simeq} & {}_{\mathrm{S}_3}(\mathrm{S}_3/\mathrm{S}_3\,, \mathrm{S}_3) \times {}_{\mathrm{S}_3}(\mathrm{S}_3/\langle(1,2)\rangle\,, \mathrm{S}_3) \times {}_{\mathrm{S}_3}(\mathrm{S}_3/\langle(1,2,3)\rangle\,, \mathrm{S}_3) \\ & \overset{(2)}{\simeq} & \{\mathrm{id}\} \times \{\mathrm{id},\, (1,2)\} \times \{\mathrm{id},\, (1,2,3), (1,3,2)\}\,. \end{array}$$

Somit ist die Anzahl der S_3-äquivarianten Abbildungen von S_3 nach S_3 gleich $1 \cdot 2 \cdot 3 = 6$.

> Darunter sind nur 2 bijektiv, namentlich die Identität und die durch $\mathrm{id} \mapsto \mathrm{id}$, $(1,2) \mapsto (1,2)$ und $(1,2,3) \mapsto (1,3,2)$ festgelegte S_3-äquivariante Abbildung.

Aufgabe 5

Schreibe $m = de$ mit $e \in \mathbf{Z}_{\geqslant 1}$. Das Element x^e hat Ordnung d, i.e. $|\langle x^e \rangle| = d$.

Sei $U \leqslant \mathrm{C}_m$ mit $|U| = d$ gegeben. Wir haben zu zeigen, daß $U \overset{!}{=} \langle x^e \rangle$. Da $|U| = d = |\langle x^e \rangle|$, genügt es, $U \overset{!}{\leqslant} \langle x^e \rangle$ zu zeigen.

Sei $i \in \mathbf{Z}_{\geqslant 0}$ so, daß $x^i \in U$. Es ist $1 = x^{i|U|} = x^{id}$. Also ist m ein Teiler von id, und somit ist e ein Teiler von i, woraus wiederum $x^i \in \langle x^e \rangle$ folgt.

> Cf. Bemerkung 8.

Aufgabe 6

(1) Es ist

$$\mathrm{Z}(G) \;=\; \{\, z \in G \,:\, gz = zg \text{ für } g \in G \,\} \;=\; \{\, z \in G \,:\, {}^g z = z \text{ für } g \in G \,\}\,.$$

Wenden wir Lemma 14 auf die G-Menge G mit der Konjugationsoperation an, so erhalten wir daher

$$0 \;\equiv_p\; |G| \;\equiv_p\; |\{\, z \in G \,:\, {}^g z = z \text{ für } g \in G \,\}| \;=\; |\mathrm{Z}(G)|\,.$$

Also ist $\mathrm{Z}(G) \neq 1$.

(2) Es operiert G auf der Menge $M := \{H \leqslant G \,:\, |H| = p^s\}$ via Konjugation. Also wird

$$1 \overset{\text{S. 13}}{\equiv_p} |M| \overset{\text{L. 14}}{\equiv_p} |\{\, H \in M \,:\, {}^g H = H \text{ für } g \in G \,\}| \;=\; |\{\, H \trianglelefteq G \,:\, |H| = p^s \,\}|\,.$$

Ist G keine p-Gruppe, so ist i.a. $|\{H \trianglelefteq G \,:\, |H| = p^s\}| \not\equiv_p 1$. Es hat e.g. S_4 keinen Normalteiler von Ordnung 8.

Aufgabe 7

(1) Es ist die Menge $\{\, H \leqslant G \,:\, |H| = p^t \,\}$ der p-Sylowgruppen eine transitive G-Menge unter der Konjugationsoperation von G; cf. Satz 15.(2). Sei $K \leqslant G$ eine p-Sylowgruppe von G. Es wird

$$|\{\, H \leqslant G \,:\, |H| = p^t \,\}| \;=\; |\{\, {}^x K \,:\, x \in G \,\}| \overset{\text{L. 5}}{=} \frac{|G|}{|\mathrm{C}_G(\{K\})|}$$

ein Teiler von $|G| = p^t n$.

Nach Sylow-Wielandt ist aber auch $|\{\, H \leqslant G \,:\, |H| = p^t \,\}| \equiv_p 1$, insbesondere also teilerfremd zu p; cf. Satz 13.

Es folgt, daß $|\{\, H \leqslant G \,:\, |H| = p^t \,\}|$ ein Teiler von n ist.

Ist nun $H \leqslant G$ die einzige p-Sylowgruppe von G, so ist ${}^g H = H$ für $g \in G$, da ${}^g H$ ebenfalls eine p-Sylowgruppe von G ist. Also ist $H \trianglelefteq G$.

(2) Sei $g \in G$ gegeben. Um die Surjektivität von f nachzuweisen, haben wir ein Urbild von gH unter f anzugeben.

Es ist ${}^g P \leqslant {}^g H = H$ eine p-Sylowgruppe von H. Nach Sylow gibt es also ein $h \in H$ mit ${}^g P = {}^h P$; cf. Satz 15.(2). Folglich ist ${}^{h^-}{}^g P = P$. I.e. es ist $h^- g \in \mathrm{N}_G(P)$. Es bildet $h^- g$ unter f auf $h^- g H = g({}^{g^-}h^-)H = gH$ ab; beachte, daß ${}^{g^-}h^- \in H$ wegen $H \trianglelefteq G$.

Die Aussage von Aufgabe 7.(2) heißt auch Frattini-Argument.

Aufgabe 8

(1) Sei G eine Gruppe mit $|G| = 104 = 2^3 \cdot 13$. Die Anzahl der 13-Sylowgruppen von G ist $\equiv_{13} 1$, und ein Teiler von 2^3; cf. Satz 13, Aufgabe 7. Also ist die Anzahl der 13-Sylowgruppen gleich 1, und wir haben einen Normalteiler von G von Ordnung 13; cf. Aufgabe 7.(1). Damit ist G nicht einfach.

(2) Zur Existenz der Abbildung λ. Zu zeigen ist hier, daß für $g \in G$ die Abbildung $\lambda(g) : M \longrightarrow M$, $m \longmapsto gm$ bijektiv ist. In der Tat ist $\lambda(g^-) \circ \lambda(g) = \mathrm{id}_M$, da $(\lambda(g^-) \circ \lambda(g))(m) = g^- g m = 1m = m$ ist für $m \in M$; genauso ist $\lambda(g) \circ \lambda(g^-) = \mathrm{id}_M$.

Zu λ Gruppenmorphismus. Seien $g, h \in G$. Zu zeigen ist $\lambda(gh) \overset{!}{=} \lambda(g) \circ \lambda(h)$. In der Tat ist

$$(\lambda(g) \circ \lambda(h))(m) \;=\; g(hm) \;=\; (gh)m \;=\; (\lambda(gh))(m)$$

für $m \in M$.

(3) Betrachte den Gruppenmorphismus $\lambda : G \longrightarrow \mathrm{S}_M$ aus (2). Da $|M| > 1$ und da M transitiv ist, gibt es $m, m' \in M$ mit $m \neq m'$ und $g \in G$ mit $(\lambda(g))(m) = gm = m'$, insbesondere also mit $\lambda(g) \neq \mathrm{id}$. Folglich ist $\operatorname{Kern}\lambda \lhd G$.

Ferner ist $G/\operatorname{Kern}\lambda \longrightarrow \lambda(G)$, $g \operatorname{Kern}\lambda \longmapsto \lambda(g)$ wohldefiniert, da aus $g \operatorname{Kern}\lambda = g' \operatorname{Kern}\lambda$ mit $g, g' \in G$ folgt, daß $g^- g' \in \operatorname{Kern}\lambda$ ist und also $\lambda(g) = \lambda(g)\lambda(g^- g') = \lambda(gg^- g') = \lambda(g')$ ist; ein Gruppenmorphismus, da λ einer ist; surjektiv nach Konstruktion; injektiv, da aus $\lambda(g) = \mathrm{id}$ folgt, daß $g \in \operatorname{Kern}\lambda$ ist, i.e. daß $g \operatorname{Kern}\lambda = 1$ ist. Insgesamt ist also $G/\operatorname{Kern}\lambda \xrightarrow{\sim} \lambda(G) \leqslant \mathrm{S}_M$ (Homomorphiesatz).

Insbesondere ist $|G/\operatorname{Kern}\lambda| = |\lambda(G)|$ ein Teiler von $|\mathrm{S}_M| = |M|!$.

Wir können also $N := \operatorname{Kern}\lambda$ setzen.

(4) Sei G eine Gruppe mit $|G| = 72 = 2^3 \cdot 3^2$. Die Anzahl der 3-Sylowgruppen von G ist $\equiv_3 1$, und ein Teiler von 2^3. Also ist diese Anzahl in $\{1, 4\}$ enthalten.

Fall 1. Die Anzahl der 3-Sylowgruppen von G ist gleich 1. Dann ist G nicht einfach; cf. Aufgabe 7.(1).

Fall 2. Die Anzahl der 3-Sylowgruppen von G ist gleich 4. Dann ist $\{\, H \leqslant G \,:\, |H| = 9 \,\}$ eine transitive G-Menge von Länge 4. Mit (3) gibt es also ein $N \lhd G$ so, daß $|G/N|$ ein Teiler von $4! = 24$ ist. Da $|G| = 72$, folgt $N \neq 1$. Somit ist G nicht einfach.

Aufgabe 9

Zeigen wir zunächst, daß f als Gruppenmorphismus existiert wie angegeben. In der Tat wird

$$\begin{array}{llllll}
(i,i+1)^2 & & & = & \mathrm{id} & \text{für } i \in [1,n-1] \\
((i,i+1)\circ(i+1,i+2))^3 & = & (i,i+1,i+2)^3 & = & \mathrm{id} & \text{für } i \in [1,n-2] \\
((i,i+1)\circ(j,j+1))^2 & = & (i,i+1)^2 \circ (j,j+1)^2 & = & \mathrm{id} & \text{für } i, j \in [1,n-1] \text{ mit } |i-j| \geqslant 2\,.
\end{array}$$

Gemäß universeller Eigenschaft der präsentierten Gruppe $\mathrm{S}_{\mathrm{P},n}$ können wir also die Abbildung

$$\begin{array}{rcll}
\{s_1, \ldots, s_n\} & \longrightarrow & \mathrm{S}_n & \\
s_i & \longmapsto & (i,i+1) & \text{für } i \in [1,n-1]
\end{array}$$

zum angegebenen Gruppenmorphismus f fortsetzen; cf. Satz 24.

Es ist f surjektiv, da $\mathrm{S}_n = \langle (1,2), (2,3), \ldots, (n-1,n) \rangle$.

Um zu zeigen, daß f ein Isomorphismus ist, bleibt also nachzuweisen, daß $|\mathrm{S}_{\mathrm{P},n}| \leqslant n!$. Wir führen eine Induktion nach $n \geqslant 1$.

Für $n = 1$ ist $\mathrm{S}_{\mathrm{P},n} = 1$, da $\mathrm{F}(\emptyset) = \{[\emptyset]\} = 1$, und jede Faktorgruppe davon ebenfalls einelementig ist.

Sei $n \geqslant 2$. Sei bekannt, daß $|\mathrm{S}_{\mathrm{P},n-1}| \leqslant (n-1)!$. Wir wollen zeigen, daß $|\mathrm{S}_{\mathrm{P},n}| \overset{!}{\leqslant} n!$.

Mittels universeller Eigenschaft der präsentierten Gruppe $\mathrm{S}_{\mathrm{P},n-1}$ erhalten wir den Gruppenmorphismus

$$\begin{array}{rcll}
\mathrm{S}_{\mathrm{P},n-1} & \xrightarrow{h} & \mathrm{S}_{\mathrm{P},n} & \\
s_i & \longmapsto & s_i & \text{für } i \in [1,n-2]\,,
\end{array}$$

da $s_i^2 = 1$ für $i \in [1,n-2]$ und $(s_i s_{i+1})^3 = 1$ für $i \in [1,n-3]$ und $(s_i s_j)^2 = 1$ für $i, j \in [1,n-2]$ mit $|i-j| \geqslant 2$ auch in $\mathrm{S}_{\mathrm{P},n}$ gelten.

Sei $H := h(\mathrm{S}_{\mathrm{P},n-1}) \leqslant \mathrm{S}_{P,n}$. Es ist $|H| \leqslant |\mathrm{S}_{\mathrm{P},n-1}| \overset{\text{I.V.}}{\leqslant} (n-1)!$. Können wir zeigen, daß $|\mathrm{S}_{P,n}/H| \overset{!}{\leqslant} n$, dann folgt

$$|\mathrm{S}_{P,n}| \;=\; |\mathrm{S}_{P,n}/H| \cdot |H| \;\leqslant\; n \cdot (n-1)! \;=\; n!\,.$$

Bleibt also zu zeigen, daß $|\mathrm{S}_{P,n}/H| \overset{!}{\leqslant} n$.

Beachte allgemein, daß in $\mathrm{S}_{P,n}$ gilt, daß $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ für $i \in [1, n-2]$, wie aus $(s_i s_{i+1})^3 = 1$ und $s_i^2 = s_{i+1}^2 = 1$ folgt. Ferner ist dort $s_i s_j = s_j s_i$ für $i, j \in [1, n]$ mit $|i-j| \geqslant 2$, wie aus $(s_i s_j)^2 = 1$ und $s_i^2 = s_j^2 = 1$ folgt.

Wir behaupten dazu, daß

$$\mathrm{S}_{P,n} \stackrel{!}{=} \bigcup_{i \in [1,n]} H s_{n-1} s_{n-2} \cdots s_i \ .$$

Zu zeigen ist $\stackrel{!}{\subseteq}$. Gegeben sei dazu ein Element $\xi \in \mathrm{S}_{P,n}$.

Es ist ξ ein Produkt in den Elementen $s_1, \ldots, s_{n-1}$.

Taucht s_{n-1} in einer dieser Faktordarstellungen von ξ nicht als Faktor auf, so ist $\xi \in H$ und ist mithin in unserer Vereinigungsmenge enthalten.

Wähle ansonsten eine Faktordarstellung von ξ, für welche der ersten Faktor von links aus gesehen, der gleich s_{n-1} ist, rechts neben sich eine minimale Anzahl von Faktoren stehen hat.

Annahme, es ist das Teilprodukt rechts von diesem Faktor s_{n-1} nicht von der Form $s_{n-1} s_{n-2} \cdots s_k$ für ein $k \in [1, n-1]$. Dann gibt es ein Teilprodukt rechts von diesem Faktor der Form $s_{n-1} s_{n-2} \cdots s_\ell s_i$ mit $i \in [1, n] \smallsetminus \{\ell - 1\}$.

Fall $i \in [1, \ell - 2]$. Wir können den Faktor s_i am Teilprodukt $s_{n-1} s_{n-2} \cdots s_\ell$ vorbei nach links tauschen und erhalten eine weitere Faktordarstellung von ξ, welche rechts vom ersten Faktor s_{n-1} weniger Faktoren als in ersterer enthält, im *Widerspruch* zur minimalen Wahl der Anzahl dieser Faktoren.

Fall $i = \ell < n - 1$. Wir können wegen $s_\ell s_i = 1$ diese beiden Faktoren streichen und erhalten eine weitere Faktordarstellung von ξ, welche rechts vom ersten Faktor s_{n-1} weniger Faktoren als in ersterer enthält, im *Widerspruch* zur minimalen Wahl der Anzahl dieser Faktoren.

Fall $i = \ell = n - 1$. Wir können wegen $s_\ell s_i = 1$ diese beiden Faktoren streichen und erhalten eine weitere Faktordarstellung von ξ, welche einen weiteren Faktor s_{n-1} weiter rechts besitzen muß, im *Widerspruch* zur minimalen Wahl der Anzahl der Faktoren rechts vom ersten Faktor s_{n-1}.

Fall $i \in [\ell + 1, n - 2]$. Wir können ein Teilprodukt wie folgt umformen.

$$\begin{aligned} & s_{n-1} s_{n-2} \cdots s_{i+1} s_i s_{i-1} s_{i-2} s_{i-3} \cdots s_\ell s_i \\ = \ & s_{n-1} s_{n-2} \cdots s_{i+1} s_i s_{i-1} s_i s_{i-2} s_{i-3} \cdots s_\ell \\ = \ & s_{n-1} s_{n-2} \cdots s_{i+1} s_{i-1} s_i s_{i-1} s_{i-2} s_{i-3} \cdots s_\ell \\ = \ & s_{i-1} s_{n-1} s_{n-2} \cdots s_{i+1} s_i s_{i-1} s_{i-2} s_{i-3} \cdots s_\ell \end{aligned}$$

So haben wir eine weitere Faktordarstellung von ξ erhalten, welche rechts vom ersten Faktor s_{n-1} weniger Faktoren als in ersterer enthält, im *Widerspruch* zur minimalen Wahl der Anzahl dieser Faktoren.

Fall $i = n - 1 > \ell$. Wir können ein Teilprodukt wie folgt umformen.

$$\begin{aligned} & s_{n-1} s_{n-2} s_{n-3} \cdots s_\ell s_{n-1} \\ = \ & s_{n-1} s_{n-2} s_{n-1} s_{n-3} \cdots s_\ell \\ = \ & s_{n-2} s_{n-1} s_{n-2} s_{n-3} \cdots s_\ell \end{aligned}$$

So haben wir eine weitere Faktordarstellung von ξ erhalten, welche rechts vom ersten Faktor s_{n-1} weniger Faktoren als in ersterer enthält, im *Widerspruch* zur minimalen Wahl der Anzahl dieser Faktoren.

Cf. Beispiel 27.

Aufgabe 10

Wir wollen zunächst die Existenz des Gruppenmorphismus

$$\begin{array}{rcl} \mathrm{S}_{\mathrm{P},6} & \xrightarrow{b} & \mathrm{S}_6 \\ s_1 & \longmapsto & (1,2)(3,4)(5,6) \\ s_2 & \longmapsto & (1,6)(2,3)(4,5) \\ s_3 & \longmapsto & (1,3)(2,4)(5,6) \\ s_4 & \longmapsto & (1,2)(3,6)(4,5) \\ s_5 & \longmapsto & (1,4)(2,3)(5,6) \end{array}$$

nachweisen.

> Die Wahl der Bildelemente ist nicht eindeutig, es gibt noch weitere nicht innere Automorphismen. Denn das Kompositum eines nicht inneren Automorphismus mit einem der zahlreichen inneren Automorphismen gibt wieder einen nicht inneren Automorphismus.

Das Bild von s_i verschwindet im Quadrat für $i \in [1,5]$.

Das Bild des Produktes $s_i s_j$ liegt für $i,\, j \in [1,5]$ mit $|i-j| \geqslant 2$ in je einer Kleinschen Vierergruppe und verschwindet daher im Quadrat.

Die Bilder der übrigen Relationen ergeben sich zu

$$\begin{array}{lcllcll} (s_1 s_2)^3 & \longmapsto & ((1,2)(3,4)(5,6) \circ (1,6)(2,3)(4,5))^3 & = & ((1,5,3)(2,4,6))^3 & = & \mathrm{id} \\ (s_2 s_3)^3 & \longmapsto & ((1,6)(2,3)(4,5) \circ (1,3)(2,4)(5,6))^3 & = & ((1,2,5)(3,6,4))^3 & = & \mathrm{id} \\ (s_3 s_4)^3 & \longmapsto & ((1,3)(2,4)(5,6) \circ (1,2)(3,6)(4,5))^3 & = & ((1,4,6)(2,3,5))^3 & = & \mathrm{id} \\ (s_4 s_5)^3 & \longmapsto & ((1,2)(3,6)(4,5) \circ (1,4)(2,3)(5,6))^3 & = & ((1,5,3)(2,6,4))^3 & = & \mathrm{id} \end{array}$$

Somit ist b ein wohldefinierter Gruppenmorphismus; cf. Satz 24.

Wir verwenden den Isomorphismus $f : \mathrm{S}_{\mathrm{P},6} \xrightarrow{\sim} \mathrm{S}_6$ mit $f(s_i) = (i, i+1)$ für $i \in [1,5]$ aus Aufgabe 9.

Sei $a := b \circ f^-$. Dies ist ein Gruppenmorphismus von S_6 nach S_6, der wie folgt abbildet.

$$\begin{array}{rcl} \mathrm{S}_6 & \xrightarrow{a} & \mathrm{S}_6 \\ (1,2) & \longmapsto & (1,2)(3,4)(5,6) \\ (2,3) & \longmapsto & (1,6)(2,3)(4,5) \\ (3,4) & \longmapsto & (1,3)(2,4)(5,6) \\ (4,5) & \longmapsto & (1,2)(3,6)(4,5) \\ (5,6) & \longmapsto & (1,4)(2,3)(5,6) \end{array}$$

Da a nicht den Zykeltyp bewahrt, ist a nicht durch Konjugation mit einem Element aus S_6 gegeben.

Um zu zeigen, daß a bijektiv ist, zeigen wir, daß a^2 bijektiv ist. Vorbereitend wird

$$\begin{array}{lcrcl} & & \mathrm{S}_6 & \xrightarrow{a} & \mathrm{S}_6 \\ (1,3) & = & {}^{(2,3)}(1,2) & \longmapsto & {}^{(1,6)(2,3)(4,5)}(1,2)(3,4)(5,6) = (6,3)(2,5)(4,1) = (1,4)(2,5)(3,6) \\ (2,4) & = & {}^{(2,3)}(3,4) & \longmapsto & {}^{(1,6)(2,3)(4,5)}(1,3)(2,4)(5,6) = (6,2)(3,5)(4,1) = (1,4)(2,6)(3,5) \\ (1,4) & = & {}^{(1,2)}(2,4) & \longmapsto & {}^{(1,2)(3,4)(5,6)}(1,4)(2,6)(3,5) = (2,3)(1,5)(4,6) = (1,5)(2,3)(4,6) \\ (3,5) & = & {}^{(4,5)}(3,4) & \longmapsto & {}^{(1,2)(3,6)(4,5)}(1,3)(2,4)(5,6) = (2,6)(1,5)(4,3) = (1,5)(2,6)(3,4) \\ (3,6) & = & {}^{(5,6)}(3,5) & \longmapsto & {}^{(1,4)(2,3)(5,6)}(1,5)(2,6)(3,4) = (4,6)(3,5)(2,1) = (1,2)(3,5)(4,6) \\ (1,6) & = & {}^{(1,3)}(3,6) & \longmapsto & {}^{(1,4)(2,5)(3,6)}(1,2)(3,5)(4,6) = (4,5)(6,2)(1,3) = (1,3)(2,6)(4,5)\,. \end{array}$$

Somit ergibt sich

$$\begin{array}{ccccccccccc}
\mathrm{S}_6 & \overset{a}{\longrightarrow} & \mathrm{S}_6 & \overset{a}{\longrightarrow} & \mathrm{S}_6 & & & & & & \\
(1,2) & \longmapsto & (1,2)(3,4)(5,6) & \longmapsto & (1,2)(3,4)(5,6)\circ(1,3)(2,4)(5,6)\circ(1,4)(2,3)(5,6) & = & (5,6) & = & (6,5) \\
(2,3) & \longmapsto & (1,6)(2,3)(4,5) & \longmapsto & (1,3)(2,6)(4,5)\circ(1,6)(2,3)(4,5)\circ(1,2)(3,6)(4,5) & = & (4,5) & = & (5,4) \\
(3,4) & \longmapsto & (1,3)(2,4)(5,6) & \longmapsto & (1,4)(2,5)(3,6)\circ(1,4)(2,6)(3,5)\circ(1,4)(2,3)(5,6) & = & (1,4) & = & (4,1) \\
(4,5) & \longmapsto & (1,2)(3,6)(4,5) & \longmapsto & (1,2)(3,4)(5,6)\circ(1,2)(3,5)(4,6)\circ(1,2)(3,6)(4,5) & = & (1,2) & = & (1,2) \\
(5,6) & \longmapsto & (1,4)(2,3)(5,6) & \longmapsto & (1,5)(2,3)(4,6)\circ(1,6)(2,3)(4,5)\circ(1,4)(2,3)(5,6) & = & (2,3) & = & (2,3)\,.
\end{array}$$

Also ist $a^2(\sigma) = {}^{(1,6,3,4)(2,5)}\sigma$ für $\sigma \in \{\,(1,2),\,(2,3),\,(3,4),\,(4,5),\,(5,6)\,\}$.

Da $\mathrm{S}_6 = \langle\,(1,2),\,(2,3),\,(3,4),\,(4,5),\,(5,6)\,\rangle$, folgt, daß $a^2(\sigma) = {}^{(1,6,3,4)(2,5)}\sigma$ für $\sigma \in \mathrm{S}_6$.

Und es ist $a^2 : \mathrm{S}_6 \longrightarrow \mathrm{S}_6\,,\ \sigma \longmapsto {}^{(1,6,3,4)(2,5)}\sigma$ bijektiv.

Der Automorphismus

$$\begin{array}{ccc}
\mathrm{S}_6 & \to & \mathrm{S}_6 \\
(1,2) & \mapsto & (1,2)(3,4)(5,6) \\
(2,3) & \mapsto & (1,5)(2,4)(3,6) \\
(3,4) & \mapsto & (1,2)(3,5)(4,6) \\
(4,5) & \mapsto & (1,3)(2,4)(5,6) \\
(5,6) & \mapsto & (1,2)(3,6)(4,5)
\end{array}$$

hat bereits in $\operatorname{Aut}\mathrm{S}_6$ die Ordnung 2, nicht erst, wie obiges a, in $\operatorname{Out}\mathrm{S}_6$ (S. Klenk, F. Müller).

Aufgabe 11

(1) *Erzeugnis.* Jedes Element von A_n ist ein Produkt einer geraden Anzahl von Transpositionen, i.e. von Zykeln der Länge 2.

In einer solchen Produktdarstellung dürfen wir annehmen, daß nicht zwei gleiche Transpositionen nebeneinanderstehen.

Somit genügt es zu zeigen, daß Produkte von je zwei ungleichen Transpositionen im Erzeugnis aller Dreierzykel liegen; also Produkte der Form $(i,j)\circ(i,k)$ oder $(i,j)\circ(k,\ell)$, wobei $i,\ j,\ k,\ \ell \in [1,n]$ mit $|\{i,\ j,\ k,\ \ell\}| = 4$. In der Tat ist

$$\begin{array}{rcl}
(i,j)\circ(i,k) & = & (i,k,j) \\
(i,j)\circ(k,\ell) & = & (i,j,k)\circ(j,k,\ell)\,.
\end{array}$$

Konjugationsklasse. Sei $(i,j,k) \in \mathrm{A}_n$ gegeben, wobei $i,\ j,\ k \in [1,n]$ mit $|\{i,\ j,\ k\}| = 3$. Sei $\sigma \in \mathrm{S}_n$ mit ${}^{\sigma}(1,2,3) = (i,j,k)$.

Ist $\operatorname{sgn}\sigma = +1$, so ist nachgewiesen, daß (i,j,k) und $(1,2,3)$ in A_n konjugiert sind.

Ist $\operatorname{sgn}\sigma = -1$, so ist $\operatorname{sgn}(\sigma(4,5)) = +1$. Dann ist auch ${}^{\sigma(4,5)}(1,2,3) = {}^{\sigma}(1,2,3) = (i,j,k)$. Somit ist auch diesenfalls nachgewiesen, daß (i,j,k) und $(1,2,3)$ in A_n konjugiert sind.

Dagegen sind in A_4 die Elemente $(1,2,3)$ und $(1,3,2)$ nicht zueinander konjugiert.

(2) Sei $1 \neq N \trianglelefteq \mathrm{A}_n$. Wir müssen zeigen, daß $N \overset{!}{=} \mathrm{A}_n$. Dank (1) genügt es zu zeigen, daß N einen Zykel der Länge 3 enthält.

Sei ein $\sigma \in N \setminus \{\mathrm{id}\}$ gewählt, für welches die Zahl der bewegten Punkte

$$n_\sigma \ :=\ n - |\{\,i \in [1,n]\ :\ \sigma(i) = i\,\}|$$

minimal ist. Wir wollen zeigen, daß σ ein Zykel der Länge 3 ist.

Es ist $n_\sigma \geqslant 3$.

Fall $n_\sigma = 3$. Es ist σ ein Zykel der Länge 3, und wir sind fertig.

Fall $n_\sigma = 4$. Da $\operatorname{sgn}\sigma = +1$, ist $\sigma = (i,j)(k,\ell)$, wobei $i,\ j,\ k,\ \ell,\ m \in [1,n]$ mit $|\{i,\ j,\ k,\ \ell,\ m\}| = 5$, was wegen $n \geqslant 5$ möglich ist.

Es ist auch

$$(i,j)(k,\ell) \circ (i,m,j) \circ (i,j)(k,\ell) \circ (i,j,m) \ = \ (i,m,j)$$

in $N \smallsetminus \{\mathrm{id}\}$ und bewegt weniger Punkte als σ, im *Widerspruch* zur Wahl von σ, so daß dieser Fall nicht eintritt.

Fall $n_\sigma \geqslant 5$.

Subfall: σ *enthält einen Zykel von Länge* $k \geqslant 4$, sagen wir $(i_1\,,\ldots,i_k)$, wobei $i_j \in [1,n]$ für $j \in [1,k]$ mit $|\{\, i_j \,:\, j \in [1,k]\,\}| = k$.

Es ist $n_\sigma \geqslant 5$.

Es ist auch

$$\begin{aligned} \sigma \circ (i_1\,,i_2\,,i_3) \circ \sigma^- \circ (i_1\,,i_2\,,i_3)^- &= (i_1\,,\ldots,i_k) \circ (i_1\,,i_2\,,i_3) \circ (i_1\,,\ldots,i_k)^- \circ (i_1\,,i_2\,,i_3)^- \\ &= (i_1\,,i_4\,,i_2) \end{aligned}$$

in $N \smallsetminus \{\mathrm{id}\}$ enthalten und bewegt weniger Punkte als σ, im *Widerspruch* zur Wahl von σ, so daß dieser Subfall nicht eintritt.

Subfall: σ *enthält wenigstens* 2 *Zykel von Länge* 3*, und keinen größerer Länge.*

Enthalte σ also die Zykel $(i,j,k)(s,t,u)$, wobei $i,\ j,\ k,\ s,\ t,\ u \in [1,n]$ mit $|\{\, i,\ j,\ k,\ s,\ t,\ u\,\}| = 6$.

Es ist $n_\sigma \geqslant 6$.

Es ist auch

$$\begin{aligned} \sigma \circ (j,k,s) \circ \sigma^- \circ (j,k,s)^- &= (i,j,k)(s,t,u) \circ (j,k,s) \circ ((i,j,k)(s,t,u))^- \circ (j,k,s)^- \\ &= (i,t,k,j,s) \end{aligned}$$

in $N \smallsetminus \{\mathrm{id}\}$ enthalten und bewegt weniger Punkte als σ, im *Widerspruch* zur Wahl von σ, so daß dieser Subfall nicht eintritt.

Subfall: σ *enthält genau einen Zykel von Länge* 3*, und keinen größerer Länge.*

Es ist $n_\sigma \geqslant 5$.

Es ist mit σ^2 ein Zykel der Länge 3 in $N \smallsetminus \{\mathrm{id}\}$ enthalten, bewegt aber weniger Punkte als σ, im *Widerspruch* zur Wahl von σ, so daß dieser Subfall nicht eintritt.

Subfall: σ *enthält wenigstens* 3 *Zykel von Länge* 2*, und keinen größerer Länge.*

Es ist $n_\sigma \geqslant 6$.

Enthalte σ also die Zykel $(i,j)(k,s)(t,u)$, wobei $i,\ j,\ k,\ s,\ t,\ u \in [1,n]$ mit $|\{\, i,\ j,\ k,\ s,\ t,\ u\,\}| = 6$.

Es ist auch

$$\begin{aligned} \sigma \circ (j,k,s) \circ \sigma^- \circ (j,k,s)^- &= (i,j)(k,s)(t,u) \circ (j,k,s) \circ ((i,j)(k,s)(t,u))^- \circ (j,k,s)^- \\ &= (i,s)(j,k) \end{aligned}$$

in $N \smallsetminus \{\mathrm{id}\}$ enthalten und bewegt weniger Punkte als σ, im *Widerspruch* zur Wahl von σ, so daß dieser Subfall nicht eintritt.

Aufgabe 12

(1) Sei $\ell \in \mathbf{Z}_{\geqslant 0}$ und

$$1 \ = \ K_\ell \ \trianglelefteq \ K_{\ell-1} \ \trianglelefteq \ \cdots \ \trianglelefteq \ K_1 \ \trianglelefteq \ K_0 \ = \ K$$

gewählt mit K_i/K_{i+1} stets abelsch.

Sei $m \in \mathbf{Z}_{\geqslant 0}$ und

$$K/K \;=\; U_m/K \;\trianglelefteqslant\; U_{m-1}/K \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; U_1/K \;\trianglelefteqslant\; U_0/K \;=\; H/K\,.$$

gewählt mit $(U_j/K)/(U_{j+1}/K)$ stets abelsch; wobei wir schon die Tatsache verwandt haben, daß sich jede Untergruppe von H/K als U/K schreiben läßt für eine Untergruppe $K \leqslant U \leqslant H$.

Beachte, daß dann $U_{j+1} \trianglelefteqslant U_j$ und $(U_j/K)/(U_{j+1}/K) \simeq U_j/U_{j+1}$ für $j \in [0, m-1]$.

Wir erhalten also die Kette

$$1 \;=\; K_\ell \;\trianglelefteqslant\; K_{\ell-1} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; K_1 \;\trianglelefteqslant\; K \;\trianglelefteqslant\; U_{m-1} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; U_1 \;\trianglelefteqslant\; U_0 \;=\; H$$

mit K_i/K_{i+1} und U_j/U_{j+1} stets abelsch, wobei $K_0 = K = U_m$.

Dies zeigt die Auflösbarkeit von H.

(2) Sei $n \in \mathbf{Z}_{\geqslant 0}$ und

$$1 \;=\; H_n \;\trianglelefteqslant\; H_{n-1} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \;\trianglelefteqslant\; H_0 \;=\; H$$

gewählt mit H_i/H_{i+1} stets abelsch.

Beachte, daß für $1 \leqslant U \trianglelefteqslant V \leqslant H$ auch $1 \leqslant U \cap K \trianglelefteqslant V \cap K \leqslant H$, da ein Element $x \in V \cap K$ in der Tat ${}^x(U \cap K) = {}^xU \cap {}^xK = U \cap K$ ist, wobei ${}^xU = U$ wegen $x \in V$ und ${}^xK = K$ wegen $x \in K$ gilt.

Ferner haben wir in dieser Situation den injektiven Gruppenmorphismus

$$\begin{array}{rcl} (V \cap K)/(U \cap K) & \longrightarrow & V/U \\ x(U \cap K) & \longmapsto & xU\,, \end{array}$$

da ein Element $x \in V \cap K$ genau dann in U liegt, wenn es in $U \cap K$ liegt. Falls also V/U abelsch ist, so auch $(V \cap K)/(U \cap K)$.

> Man kann auch aus V/U abelsch und aus $(V \cap K)/(U \cap K) = (V \cap K)/(U \cap (V \cap K)) \simeq U(V \cap K)/U \leqslant V/U$ folgern, daß $(V \cap K)/(U \cap K)$ abelsch ist; cf. Bemerkung 32.

Somit ist in der Kette

$$1 \;=\; H_n \cap K \;\trianglelefteqslant\; H_{n-1} \cap K \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \cap K \;\trianglelefteqslant\; H_0 \cap K \;=\; K$$

von Untergruppen von K jeder Subfaktor $(H_i \cap K)/(H_{i+1} \cap K)$ abelsch.

Dies zeigt die Auflösbarkeit von K.

(3) Sei $n \in \mathbf{Z}_{\geqslant 0}$ und

$$1 \;=\; H_n \;\trianglelefteqslant\; H_{n-1} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \;\trianglelefteqslant\; H_0 \;=\; H$$

gewählt mit H_i/H_{i+1} stets abelsch.

Beachte, daß für $1 \leqslant U \trianglelefteqslant V \leqslant H$ auch $K/K \leqslant UK/K \trianglelefteqslant VK/K \leqslant H/K$, da für $u \in U$ und $v \in V$ gilt, daß

$${}^{vK}uK \;=\; ({}^vu)K \;\in\; UK/K\,.$$

Ferner haben wir in dieser Situation $(VK/K)/(UK/K) \simeq VK/UK$ und dafür wiederum den surjektiven Gruppenmorphismus

$$\begin{array}{rcl} V/U & \longrightarrow & VK/UK \\ vU & \longmapsto & vUK\,, \end{array}$$

da $U \leqslant UK$ und da für $v \in V$ und $k \in K$ auch $vkUK = vkKU = vKU = vUK$ ist. Falls also V/U abelsch ist, so auch $(VK/K)/(UK/K)$.

Man kann auch aus V/U abelsch und aus $(VK/K)/(UK/K) \simeq (VK)/(UK) = (V(UK))/UK \simeq V/(V \cap (UK))$ Faktorgruppe von V/U schließen, daß V/U abelsch ist; cf. Bemerkung 32.

Somit wird in der Kette

$$K/K \;=\; H_nK/K \;\trianglelefteqslant\; H_{n-1}K/K \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1K/K \;\trianglelefteqslant\; H_0K/K \cap K \;=\; H/K$$

von Untergruppen von H/K jeder Subfaktor $(H_iK/K)/(H_{i+1}K/K)$ abelsch.

Dies zeigt die Auflösbarkeit von H/K.

(4) Da H/K überauflösbar ist, gibt es, wenn man noch Urbilder unter $H \longrightarrow\!\!\!\!\!\rightarrow H/K$, $h \longmapsto hK$ nimmt, ein $\ell \in \mathbf{Z}_{\geqslant 0}$ und eine Kette

$$K \;=\; H_\ell \;\trianglelefteqslant\; H_{\ell-1} \;\trianglelefteqslant\; H_{\ell-2} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \;\trianglelefteqslant\; H_0 \;=\; H$$

mit H_j/H_{j+1} zyklisch für $j \in [0, \ell-1]$ und $H_j \trianglelefteqslant H$ für $j \in [0, \ell]$.

Nach dem Hauptsatz über endliche abelsche Gruppen aus der Linearen Algebra ist K isomorph zu einem direkten Produkt zyklischer Gruppen. Folglich gibt es ein $m \in \mathbf{Z}_{\geqslant 0}$ und eine Kette

$$1 \;=\; K_m \;\trianglelefteqslant\; K_{m-1} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; K_1 \;\trianglelefteqslant\; K_0 \;=\; K$$

so, daß K_j/K_{j+1} zyklisch ist für $j \in [0, m-1]$. Da $K \leqslant \mathrm{Z}(H)$, ist $K_j \trianglelefteqslant H$ für $j \in [0, m]$. Die zusammengesetzte Kette

$$1 \;=\; K_m \;\trianglelefteqslant\; K_{m-1} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; K_1 \;\trianglelefteqslant\; K_0 \;=\; K \;=\; H_\ell \;\trianglelefteqslant\; H_{\ell-1} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \;\trianglelefteqslant\; H_0 \;=\; H$$

zeigt also, daß H überauflösbar ist.

(5) Sei $n \in \mathbf{Z}_{\geqslant 0}$ und

$$1 \;=\; H_n \;\trianglelefteqslant\; H_{n-1} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \;\trianglelefteqslant\; H_0 \;=\; H$$

gewählt mit $H_i \trianglelefteqslant H$ stets und H_i/H_{i+1} stets zyklisch.

Beachte, daß für $1 \leqslant U \trianglelefteqslant V \leqslant H$ auch $1 \leqslant U \cap K \trianglelefteqslant V \cap K \leqslant H$ ist und daß wir einen injektiven Gruppenmorphismus $(V \cap K)/(U \cap K) \longrightarrow\!\!\!\!\!\rightarrow V/U$ haben; cf. Lösung zu (2).

Ist also V/U zyklisch, so auch $(V \cap K)/(U \cap K)$; cf. Lösung zu Aufgabe 5.

Somit ist in der Kette

$$1 \;=\; H_n \cap K \;\trianglelefteqslant\; H_{n-1} \cap K \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \cap K \;\trianglelefteqslant\; H_0 \cap K \;=\; K$$

von Untergruppen von K zum einen $H_i \cap K \trianglelefteqslant K$ stets und zum anderen jeder Subfaktor $(H_i \cap K)/(H_{i+1} \cap K)$ zyklisch.

Dies zeigt die Überauflösbarkeit von K.

(6) Sei $n \in \mathbf{Z}_{\geqslant 0}$ und

$$1 \;=\; H_n \;\trianglelefteqslant\; H_{n-1} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \;\trianglelefteqslant\; H_0 \;=\; H$$

gewählt mit $H_i \trianglelefteqslant H$ stets und H_i/H_{i+1} stets zyklisch.

Beachte, daß für $1 \leqslant U \trianglelefteqslant V \leqslant H$ auch $K/K \leqslant UK/K \trianglelefteqslant VK/K \leqslant H/K$ und daß wir einen surjektiven Gruppenmorphismus $V/U \longrightarrow\!\!\!\!\!\rightarrow (VK/K)/(UK/K)$ haben; cf. Lösung zu (3).

Ist also V/U zyklisch, so auch $(VK/K)/(UK/K)$.

Somit wird in der Kette

$$K/K \;=\; H_nK/K \;\trianglelefteqslant\; H_{n-1}K/K \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1K/K \;\trianglelefteqslant\; H_0K/K \cap K \;=\; H/K$$

von Untergruppen von H/K zum einen $H_iK/K \trianglelefteqslant H/K$ stets und zum anderen jeder Subfaktor $(H_iK/K)/(H_{i+1}K/K)$ zyklisch.

Dies zeigt die Überauflösbarkeit von H/K.

(7) Da H/K nilpotent ist, gibt es, wenn man noch Urbilder unter $H \longrightarrow H/K$, $h \longmapsto hK$ nimmt, ein $\ell \in \mathbf{Z}_{\geqslant 0}$ und eine Kette

$$K \;=\; H_\ell \;\trianglelefteqslant\; H_{\ell-1} \;\trianglelefteqslant\; H_{\ell-2} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \;\trianglelefteqslant\; H_0 \;=\; H$$

mit $H_j \trianglelefteqslant H$ für $j \in [0,\ell]$ und $H_j/H_{j+1} \leqslant \mathrm{Z}(H/H_{j+1})$ für $j \in [0,\ell-1]$.

Setze $H_{\ell+1} := 1$. Dann ist in der Kette

$$1 \;=\; H_{\ell+1} \;\trianglelefteqslant\; H_\ell \;\trianglelefteqslant\; H_{\ell-1} \;\trianglelefteqslant\; H_{\ell-2} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \;\trianglelefteqslant\; H_0 \;=\; H$$

auch $H_j \trianglelefteqslant H$ für $j \in [0,\ell+1]$ und $H_j/H_{j+1} \leqslant \mathrm{Z}(H/H_{j+1})$ für $j \in [0,\ell]$, wobei letzteres gilt, da $H_\ell = K \leqslant \mathrm{Z}(H)$.

(8) Sei $n \in \mathbf{Z}_{\geqslant 0}$ und

$$1 \;=\; H_n \;\trianglelefteqslant\; H_{n-1} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \;\trianglelefteqslant\; H_0 \;=\; H$$

gewählt mit $H_i \trianglelefteqslant H$ und $H_i/H_{i+1} \leqslant \mathrm{Z}(H/H_{i+1})$ stets.

Ist $i \in [0,\ell-1]$, $x \in H_i \cap K$ und $h \in K$, dann ist $xH_{i+1} = {}^h xH_{i+1}$, i.e. $x^-({}^h x) \in H_{i+1}$, da $H_i/H_{i+1} \leqslant \mathrm{Z}(H/H_{i+1})$, und $x^-({}^h x) \in K$ da $h,\, x \in K$. Insgesamt ist so $x^-({}^h x) \in H_{i+1} \cap K$. In anderen Worten, es ist

$${}^{h(H_{i+1}\cap K)}x(H_{i+1}\cap K) \;=\; ({}^h x)(H_{i+1}\cap K) \;=\; x(H_{i+1}\cap K)$$

in $K/(H_{i+1}\cap K)$.

Daher ist auch in der Kette

$$1 \;=\; H_n\cap K \;\trianglelefteqslant\; H_{n-1}\cap K \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1\cap K \;\trianglelefteqslant\; H_0\cap K \;=\; K$$

von Untergruppen von K zum einen $H_i \cap K \trianglelefteqslant K$ stets und, dank obiger Rechnung, zum anderen $(H_i\cap K)/(H_{i+1}\cap K) \leqslant \mathrm{Z}(K/(H_{i+1}\cap K))$ stets.

Dies zeigt die Nilpotenz von K.

(9) Sei $n \in \mathbf{Z}_{\geqslant 0}$ und

$$1 \;=\; H_n \;\trianglelefteqslant\; H_{n-1} \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1 \;\trianglelefteqslant\; H_0 \;=\; H$$

gewählt mit $H_i \trianglelefteqslant H$ stets und $H_i/H_{i+1} \leqslant \mathrm{Z}(H/H_{i+1})$ stets.

Ist $i \in [0,\ell-1]$, $x \in H_i$ und $h \in H$, dann ist

$$({}^h x)H_{i+1} \;=\; {}^{hH_{i+1}}xH_{i+1} \;=\; xH_{i+1}\,,$$

i.e. $x^-\,({}^h x) \in H_{i+1}$. Also ist auch

$$\begin{aligned}(xK)(H_{i+1}K/K)^-\,{}^{(hK)(H_{i+1}K/K)}(xK)(H_{i+1}K/K) &= ((xK)^-\,{}^{hK}xK)(H_{i+1}K/K)\\ &= ((x^-\,{}^h x)K)(H_{i+1}K/K)\\ &= 1\,,\end{aligned}$$

i.e. $(xK)(H_{i+1}K/K) = {}^{(hK)(H_{i+1}K/K)}(xK)(H_{i+1}K/K)$. Somit wird in der Kette

$$K/K \;=\; H_nK/K \;\trianglelefteqslant\; H_{n-1}K/K \;\trianglelefteqslant\; \cdots \;\trianglelefteqslant\; H_1K/K \;\trianglelefteqslant\; H_0K/K \;=\; H/K$$

von Untergruppen von H/K zum einen $H_iK/K \trianglelefteqslant H/K$ stets und, dank obiger Rechnung, zum anderen $(H_iK/K)/(H_{i+1}K/K) \leqslant \mathrm{Z}((H/K)/(H_{i+1}K/K))$ stets.

Dies zeigt die Nilpotenz von H/K.

Aufgabe 13

(1) Sei G eine Gruppe mit $|G| = pq$. Sei o.E. $p < q$.

Die Anzahl der q-Sylowgruppen ist $\equiv_q 1$ und ein Teiler von p; cf. Satz 13 und Aufgabe 7.(1).

Also gibt es in G einen Normalteiler $Q \trianglelefteq G$ der Ordnung q; cf. Aufgabe 7.(1).

Es sind sowohl Q als auch G/Q von Primzahlordnung und mithin zyklisch.

Also zeigt die Kette

$$1 \trianglelefteq Q \trianglelefteq G\,,$$

daß G überauflösbar ist.

(2) Sei $p < q$ angenommen. Wir wollen erstens zeigen, daß eine Gruppe der Ordnung p^2q auflösbar ist, und zweitens, daß eine Gruppe der Ordnung pq^2 auflösbar ist.

Fall: Sei G eine Gruppe mit $|G| = p^2q$. Sei k die Anzahl ihrer q-Sylowgruppen. Dann ist $k \equiv_q 1$ und k ein Teiler von p^2; cf. Satz 13 und Aufgabe 7.(1).

Subfall $k = 1$. Wir haben einen Normalteiler Q von Ordnung q. Es ist Q zyklisch, also abelsch, also auflösbar. Es ist G/Q von Ordnung p^2, also eine p-Gruppe, also nilpotent, also auflösbar; cf. Bemerkung 31, Beispiel 33.(2). Somit ist G auflösbar; cf. Aufgabe 12.(1).

> Man kann sich auch überlegen, daß eine Gruppe H der Ordnung p^2 abelsch ist. Denn ihr Zentrum hat p oder p^2 Elemente; cf. Aufgabe 6.(1). Ersterenfalls ist $H/\mathrm{Z}(H)$ zyklisch, sagen wir $H/\mathrm{Z}(H) = \langle x\mathrm{Z}(H)\rangle$. Also ist jedes Element von H von der Form $x^i z$ mit $i \in \mathbf{Z}$ und $z \in \mathrm{Z}(H)$. Folglich ist H abelsch. Also kann $|\mathrm{Z}(H)|$ nicht gleich p gewesen sein.

Subfall $k = p$. Da $p \in [2, q-1]$ ist, ist $p \not\equiv_q 1$, dieser Subfall tritt also nicht ein.

Subfall $k = p^2$. Aus $k = p^2 \equiv_q 1$ und $\mathbf{F}_q$ Körper folgt, daß $p \equiv_q \pm 1$. Da $p \in [2, q-1]$, folgt $p = q-1$, mithin $p = 2$ und $q = 3$.

Es liegt also eine Gruppe der Ordnung 12 vor, mit vier 3-Sylowgruppen. Da diese paarweise ungleich sind, haben sie paarweise den Schnitt 1. Somit haben in G gerade $4 \cdot (3-1)$ Elemente Ordnung 3. Sei P eine 2-Sylowgruppe. Es ist $|P| = 4$, also muß P aus den 4 Elementen von G bestehen, die nicht von Ordnung 3 sind. Also ist P die einzige 2-Sylowgruppe in G. Es folgt $P \trianglelefteq G$; cf. Aufgabe 7.(1). Die Kette

$$1 \trianglelefteq P \trianglelefteq G$$

zeigt wegen $|P| = 4$, also P nilpotent, und $|G/P| = 3$, also G/P zyklisch, daß G auflösbar ist; cf. Bemerkung 31, Beispiel 33.(2), Aufgabe 12.(1).

> Es ist P auch abelsch, cf. oben.
>
> Alternativ kann man auch in G bei p^2 paarweise verschiedene Untergruppen von Ordnung q auf genau $p^2q - p^2(q-1) = p^2$ Elemente schließen, die nicht von Ordnung q sind und so folgern, daß jede p-Sylowgruppe von G aus ebendiesen zu bestehen hat.

Fall: Sei G eine Gruppe mit $|G| = pq^2$. Die Anzahl ihrer q-Sylowgruppen ist $\equiv_q 1$ und ein Teiler von p, also gleich 1; cf. Satz 13 und Aufgabe 7.(1). Folglich haben wir einen Normalteiler Q von Ordnung q^2. Analog zum vorstehenden Fall zeigt die Kette $1 \trianglelefteq Q \trianglelefteq G$ wegen $|Q| = q^2$ und $|G/Q| = p$, daß G auflösbar ist.

(3) Sei G eine Gruppe mit $|G| = p^2q^2$. Sei k die Anzahl ihrer q-Sylowgruppen. Es ist $k \equiv_q 1$ und ein Teiler von p^2.

Fall $k = 1$. Wir haben einen Normalteiler $Q \trianglelefteq G$ mit $|Q| = q^2$. Die Kette $1 \trianglelefteq Q \trianglelefteq G$ zeigt, daß G auflösbar ist.

Fall $k = p$. Da $p \in [2, q-1]$ ist, ist $p \not\equiv_q 1$, dieser Fall tritt also nicht ein.

Subfall $k = p^2$. Aus $k = p^2 \equiv_q 1$ und $\mathbf{F}_q$ Körper folgt, daß $p \equiv_q \pm 1$. Da $p \in [2, q-1]$, folgt $p = q-1$, mithin $p = 2$ und $q = 3$.

Es ist also $|G| = 36$, und es gibt in G vier 3-Sylowgruppen. Dann aber gibt es einen Normalteiler $N \lhd G$ mit $|G/N|$ einem Teiler von $4! = 24$, also von 12; cf. Aufgabe 8.(3), Satz 15.(2).

In der Kette $1 \lhd N \lhd G$ sind $|N|$ und $|G/N|$ echte Teiler von p^2q^2. Dies zeigt mit $(1, 2)$ und Aufgabe 12.(1), daß G auflösbar ist.

Man könnte auch zu tricksen versuchen, nur (3) zeigen (wobei man dann den Fall $|G| = 36$ ad hoc zeigen muß), für (1) die Gruppe G mit $|G| = pq$ als Untergruppe von $G \times \mathrm{C}_p \times \mathrm{C}_q$ auffassen und mit Aufgabe 12.(2) folgern, daß G auflösbar ist. Entsprechend für (2).

Der Satz von Burnside, ein Ziel dieser Vorlesung, besagt, daß in der Tat für beliebige Exponenten $a,\ b \in \mathbf{Z}_{\geqslant 1}$ eine Gruppe von Ordnung $p^a q^b$ auflösbar ist; cf. Satz 131.

Aufgabe 14

Es genügt zu zeigen, daß

$$\begin{array}{rcl} \mathrm{S}_{\mathrm{P},3} & \longrightarrow & \mathrm{GL}_2(\mathbf{Z}) \\ s_1 & \longmapsto & \left(\begin{smallmatrix} -2 & -1 \\ 3 & 2 \end{smallmatrix}\right) \\ s_2 & \longmapsto & \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right) \end{array}$$

einen Gruppenmorphismus definiert, da wir dann mit dem Inversen des Isomorphismus $\mathrm{S}_{\mathrm{P},3} \xrightarrow{\sim} \mathrm{S}_3$, $s_i \longmapsto (i, i+1)$ aus Aufgabe 9 komponieren können und so die gewünschte Darstellung erhalten.

Mit der universellen Eigenschaft dieser präsentierten Gruppe $\mathrm{S}_{\mathrm{P},3} = \langle\, s_1\,,\, s_2 \,:\, s_1^2\,,\ s_2^2\,,\ (s_1 s_2)^3 \,\rangle$ bleibt also nachzurechnen, daß $\left(\begin{smallmatrix} -2 & -1 \\ 3 & 2 \end{smallmatrix}\right)^2 \overset{!}{=} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)^2 \overset{!}{=} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ und $\left(\left(\begin{smallmatrix} -2 & -1 \\ 3 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)\right)^3 \overset{!}{=} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Matrixmultiplikation zeigt, daß dies in der Tat der Fall ist.

Aufgabe 15

Seien $r_g\,, \tilde{r}_g\,,\ s_g\,,\ \tilde{s}_g\,,\ t_g \ \in\ R$ für $g \in G$.

Nach Konstruktion ist $(RG, +)$ eine abelsche Gruppe.

Sei $1 = 1_{RG} := 1_G$.

Es wird

$$1_{RG} \underset{RG}{\cdot} (\sum_h s_h h) \ =\ 1_G \underset{RG}{\cdot} (\sum_h s_h h) \ =\ \sum_h s_h\, 1_G \underset{G}{\cdot} h \ =\ \sum_h s_h h\,.$$

Analog wird $(\sum_{h\in G} s_h h) \underset{RG}{\cdot} 1_{RG} = \sum_{h\in G} s_h h$.

Es wird

$$\begin{array}{rcl} ((\sum_g r_g\, g) \underset{RG}{\cdot} (\sum_h s_h h)) \underset{RG}{\cdot} (\sum_k t_k k) & = & (\sum_{g,h} r_g s_h\, g \underset{G}{\cdot} h) \underset{RG}{\cdot} (\sum_k t_k k) \\ & = & \sum_{g,h,k} r_g s_h t_k\, (g \underset{G}{\cdot} h) \underset{G}{\cdot} k \\ & = & \sum_{g,h,k} r_g s_h t_k\, g \underset{G}{\cdot} (h \underset{G}{\cdot} k) \\ & = & (\sum_g r_g\, g) \underset{RG}{\cdot} (\sum_{h,k} s_h t_k\, h \underset{G}{\cdot} k) \\ & = & (\sum_g r_g\, g) \underset{RG}{\cdot} ((\sum_h s_h h) \underset{RG}{\cdot} (\sum_k t_k k))\,. \end{array}$$

Es wird

$$\begin{aligned}
& ((\textstyle\sum_g r_g\, g) + (\sum_g \tilde{r}_g\, g)) \underset{RG}{\cdot} ((\textstyle\sum_h s_h h) + (\sum_h \tilde{s}_h h)) \\
= \;& (\textstyle\sum_g (r_g + \tilde{r}_g)\, g) \underset{RG}{\cdot} (\sum_h (s_h + \tilde{s}_h) h) \\
= \;& \textstyle\sum_{g,h} (r_g + \tilde{r}_g)(s_h + \tilde{s}_h)\, g \underset{G}{\cdot} h \\
= \;& \textstyle\sum_{g,h} (r_g s_h + \tilde{r}_g s_h + r_g \tilde{s}_h + \tilde{r}_g \tilde{s}_h)\, g \underset{G}{\cdot} h \\
= \;& (\textstyle\sum_{g,h} r_g s_h\, g \underset{G}{\cdot} h) + (\sum_{g,h} \tilde{r}_g s_h\, g \underset{G}{\cdot} h) + (\sum_{g,h} r_g \tilde{s}_h\, g \underset{G}{\cdot} h) + (\sum_{g,h} \tilde{r}_g \tilde{s}_h\, g \underset{G}{\cdot} h) \\
= \;& (\textstyle\sum_g r_g\, g) \underset{RG}{\cdot} (\sum_h s_h h) + (\sum_g \tilde{r}_g\, g) \underset{RG}{\cdot} (\sum_h s_h h) + (\sum_g r_g\, g) \underset{RG}{\cdot} (\sum_h \tilde{s}_h h) + (\sum_g \tilde{r}_g\, g) \underset{RG}{\cdot} (\sum_h \tilde{s}_h h)\,.
\end{aligned}$$

Also ist $(RG, +, \underset{RG}{\cdot})$ ein Ring.

Cf. Definition 42.

Aufgabe 16

Zu zeigen ist nur $\mathrm{Z}(R^{n\times n}) \overset{!}{\subseteq} {}_R\langle \mathrm{E}_n \rangle$.

Sei $A = (\alpha_{i,j})_{i,j} \in \mathrm{Z}(R^{n\times n})$ gegeben. Zu zeigen ist $\alpha_{\ell,k} \overset{!}{=} 0$ und $\alpha_{k,k} = \alpha_{\ell,\ell}$ für $k,\, \ell \in [1,n]$ mit $k \neq \ell$.

Es bezeichne $\mathrm{e}_{i,j} \in R^{n\times n}$ die Matrix, die an Position (i,j) den Eintrag 1 hat, und 0 sonst, wobei $i,\, j \in [1,n]$.

Seien $k,\, \ell \in [1,n]$ mit $k \neq \ell$ gegeben. Es wird

$$0 \;=\; A(\mathrm{E}_n + \mathrm{e}_{k,\ell}) - (\mathrm{E}_n + \mathrm{e}_{k,\ell})A \;=\; A\mathrm{e}_{k,\ell} - \mathrm{e}_{k,\ell}A\,.$$

Insbesondere verschwindet der Eintrag an Position (ℓ,ℓ) dieser Matrix, viz. $\alpha_{\ell,k}$.

Ferner verschwindet der Eintrag an Position (k,ℓ) dieser Matrix, viz. $\alpha_{k,k} - \alpha_{\ell,\ell}$.

Cf. Beispiel 47.

Aufgabe 17

Schreibe $\zeta := \zeta_n$.

Sei $m \in \mathbf{Z}$.

Falls $m \equiv_n 0$, so ist

$$\textstyle\sum_{k\in[0,n-1]} \zeta^{km} \;=\; \sum_{k\in[0,n-1]} 1 \;=\; n\,.$$

Falls $m \not\equiv_n 0$, so ist

$$\begin{aligned}
(1-\zeta^m)(\textstyle\sum_{i\in[0,n-1]} \zeta^{im}) &= (\textstyle\sum_{i\in[0,n-1]} \zeta^{im}) - (\sum_{i\in[0,n-1]} \zeta^{(i+1)m}) \\
&= (\textstyle\sum_{i\in[0,n-1]} \zeta^{im}) - (\sum_{i\in[1,n]} \zeta^{im}) \\
&= \zeta^{0\cdot m} - \zeta^{n\cdot m} \\
&= 1 - 1 \\
&= 0\,;
\end{aligned}$$

da $\zeta^m \neq 1$ ist, folgt diesenfalls

$$\textstyle\sum_{i\in[0,n-1]} \zeta^{im} \;=\; 0\,.$$

Zusammengefaßt wird $\sum_{i\in[0,n-1]} \zeta^{im} = n \cdot \partial_{m+n\mathbf{Z}\,,\,0+n\mathbf{Z}}$.

Seien $k\,,\,\ell \in [0,n-1]$ gegeben. Der Eintrag von $A\bar{A}$ an Position $(k+1,\ell+1)$ ergibt sich zu

$$\sum_{i\in[0,n-1]} \zeta^{ki}\zeta^{-i\ell} \;=\; \sum_{i\in[0,n-1]} \zeta^{i(k-\ell)} \;=\; n \cdot \partial_{k+n\mathbf{Z}\,,\,\ell+n\mathbf{Z}} \;=\; n \cdot \partial_{k,\ell}\ .$$

Dies zeigt $A\bar{A} = n\mathrm{E}_n$.

Somit ist $n^n = \det(A\bar{A}) = \det(A)\det(\bar{A}) = \det(A)\,\overline{\det(A)}$.

Nach Vandermonde ist $\det(A) = \prod_{i,\,j\,\in\,[0,n-1],\;i<j}(\zeta^j - \zeta^i)$. Also ist

$$\overline{\det(A)} \;=\; \prod_{i,\,j\,\in\,[0,n-1],\;i<j}(\zeta^{-j} - \zeta^{-i}) \;=\; (-1)^{\binom{n-1}{2}} \prod_{i,\,j\,\in\,[0,n-1],\;i<j}(\zeta^j - \zeta^i) \;=\; (-1)^{\binom{n-1}{2}} \det(A)\ ,$$

da das linke Produkt alle Faktoren des rechten durchläuft, nur diejenigen, die keinen Exponenten 0 involvieren, jeweils negativ. Es folgt

$$(-1)^{\binom{n-1}{2}} n^n \;=\; \det(A)^2 \;=\; \prod_{i,\,j\,\in\,[0,n-1],\;i<j}(\zeta^j - \zeta^i)^2\ .$$

Cf. Beispiel 50.

Alternativ kann man auch $\bar{A}$ durch eine Spaltenpermutation aus A gewinnen und hat sich dann um das Signum dieser Permutation zu kümmern (Vorschlag von S. Schmid).

Aufgabe 18

(1) Wir haben den Gruppenmorphismus

$$\begin{array}{rcccccccc}
\mathrm{S}_3 & \xrightarrow{\gamma} & \mathrm{GL}_1(\mathbf{Q}) & \times & \mathrm{GL}_2(\mathbf{Q}) & \times & \mathrm{GL}_1(\mathbf{Q}) & = & \mathrm{U}(\mathbf{Q}\times\mathbf{Q}^{2\times 2}\times\mathbf{Q}) \\
(1,2) & \longmapsto & (1 & , & \left(\begin{smallmatrix}-2 & -1\\ 3 & 2\end{smallmatrix}\right) & , & -1) & \\
(2,3) & \longmapsto & (1 & , & \left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right) & , & -1)\ ; &
\end{array}$$

cf. Beispiel 39.$(1,3,4)$. Dieser bildet insgesamt

$$\begin{array}{rcccccccc}
\mathrm{S}_3 & \xrightarrow{\gamma} & \mathrm{GL}_1(\mathbf{Q}) & \times & \mathrm{GL}_2(\mathbf{Q}) & \times & \mathrm{GL}_1(\mathbf{Q}) & = & \mathrm{U}(\mathbf{Q}\times\mathbf{Q}^{2\times 2}\times\mathbf{Q}) \\
\mathrm{id} & \longmapsto & (1 & , & \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) & , & 1) & \\
(1,2) & \longmapsto & (1 & , & \left(\begin{smallmatrix}-2 & -1\\ 3 & 2\end{smallmatrix}\right) & , & -1) & \\
(2,3) & \longmapsto & (1 & , & \left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right) & , & -1) & \\
(1,3) & \longmapsto & (1 & , & \left(\begin{smallmatrix}1 & 0\\ -3 & -1\end{smallmatrix}\right) & , & -1) & \\
(1,2,3) & \longmapsto & (1 & , & \left(\begin{smallmatrix}-2 & -1\\ 3 & 1\end{smallmatrix}\right) & , & 1) & \\
(1,3,2) & \longmapsto & (1 & , & \left(\begin{smallmatrix}1 & 1\\ -3 & -2\end{smallmatrix}\right) & , & 1) &
\end{array}$$

ab.

Gemäß universeller Eigenschaft der Gruppenalgebra in der Version von Bemerkung 60 gibt es den $\mathbf{Q}$-Algebrenmorphismus

$$\begin{array}{rcl}
\mathbf{Q}\mathrm{S}_3 & \xrightarrow{\omega} & \mathbf{Q}\times\mathbf{Q}^{2\times 2}\times\mathbf{Q} \\
\sum_{\sigma\in\mathrm{S}_3} x_\sigma\sigma & \longmapsto & \sum_{\sigma\in\mathrm{S}_3} \varphi(x_\sigma)\gamma(\sigma)\ .
\end{array}$$

Dieser ist insbesondere $\mathbf{Q}$-linear. Bezüglich der Basis S_3 der linken und der Standardbasis der rechten Seite ist diese $\mathbf{Q}$-lineare Abbildung beschrieben durch die Matrix

$$A \;:=\; \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1\\
1 & -2 & 1 & 1 & -2 & 1\\
0 & -1 & 1 & 0 & -1 & 1\\
0 & 3 & 0 & -3 & 3 & -3\\
1 & 2 & -1 & -1 & 1 & -2\\
1 & -1 & -1 & -1 & 1 & 1
\end{pmatrix} \;\in\; \mathbf{Q}^{6\times 6}\ .$$

Diese hat Determinante -54, ist also invertierbar. Somit ist ω bijektiv. Damit ist ω ein Isomorphismus von $\mathbf{Q}$-Algebren.

In diesem Argument kann man $\mathbf{Q}$ durch $\mathbf{C}$ ersetzen und erhält $\mathbf{C}\mathrm{S}_3 \simeq \mathbf{C}\times\mathbf{C}^{2\times 2}\times\mathbf{C}$ als $\mathbf{C}$-Algebren.

(2) Wir verwenden die Abbildung ω aus (1). Ersichtlich ist $\omega(\mathbf{Z}\mathrm{S}_3) \subseteq \mathbf{Z}\times\mathbf{Z}^{2\times 2}\times\mathbf{Z}$. Es ist

$$A^{-1} \;=\; \frac{1}{6}\begin{pmatrix} 1 & 2 & 0 & 0 & 2 & 1 \\ 1 & -4 & 6 & -2 & 4 & -1 \\ 1 & 2 & 0 & 2 & -2 & -1 \\ 1 & 2 & -6 & 0 & -2 & -1 \\ 1 & 2 & -6 & 2 & -4 & 1 \\ 1 & -4 & 6 & -2 & 2 & 1 \end{pmatrix} \;\in\; \mathbf{Q}^{6\times 6}\,.$$

Wir haben zu untersuchen, wann $A^{-1}z$ ganzzahlig ist für $z \in \mathbf{Z}^{6\times 1}$. Denn genau dann liegt ein Element z von $\mathbf{Z}\times\mathbf{Z}^{2\times 2}\times\mathbf{Z}$, dargestellt als Vektor in der Standardbasis, im Bild $\omega(\mathbf{Z}\mathrm{S}_3)$.

Aus A wird durch $\mathrm{SL}_6(\mathbf{Z})$-Multiplikation von links

$$\frac{1}{6}\begin{pmatrix} 1 & 2 & 0 & 0 & 2 & 1 \\ 1 & -4 & 6 & -2 & 4 & -1 \\ 1 & 2 & 0 & 2 & -2 & -1 \\ 1 & 2 & -6 & 0 & -2 & -1 \\ 1 & 2 & -6 & 2 & -4 & 1 \\ 1 & -4 & 6 & -2 & 2 & 1 \end{pmatrix} \rightsquigarrow \frac{1}{6}\begin{pmatrix} 1 & 2 & 0 & 0 & 2 & 1 \\ 0 & -6 & 6 & -2 & 2 & -2 \\ 0 & 0 & 0 & 2 & -4 & -2 \\ 0 & 0 & -6 & 0 & -4 & -2 \\ 0 & 0 & -6 & 2 & -6 & 0 \\ 0 & -6 & 6 & -2 & 0 & 0 \end{pmatrix} \rightsquigarrow \frac{1}{6}\begin{pmatrix} 1 & 2 & 0 & 0 & 2 & 1 \\ 0 & -6 & 0 & 0 & -4 & -2 \\ 0 & 0 & 6 & 0 & 2 & -2 \\ 0 & 0 & -6 & 0 & -4 & -2 \\ 0 & 0 & -6 & 2 & -6 & 0 \\ 0 & -6 & 0 & 0 & -6 & 0 \end{pmatrix} \rightsquigarrow \frac{1}{6}\begin{pmatrix} 1 & 2 & 0 & 0 & 2 & 1 \\ 0 & -6 & -6 & 0 & -6 & 0 \\ 0 & 0 & 6 & 0 & 2 & -2 \\ 0 & 0 & -12 & 0 & -6 & 0 \\ 0 & 0 & -6 & 2 & -6 & 0 \\ 0 & -6 & 0 & 0 & -6 & 0 \end{pmatrix}.$$

Wir lesen ab, daß

$$\begin{aligned} \mathbf{Z}\mathrm{S}_3 &\simeq \omega(\mathbf{Z}\mathrm{S}_3) \\ &= \{\,(a, \left(\begin{smallmatrix} b & c \\ d & e \end{smallmatrix}\right), f) \in \mathbf{Z}\times\mathbf{Z}^{2\times 2}\times\mathbf{Z} \,:\, a+2b+2e+f \equiv_6 0,\ e \equiv_3 f,\ d \equiv_3 0\,\} \\ &= \{\,(a, \left(\begin{smallmatrix} b & c \\ d & e \end{smallmatrix}\right), f) \in \mathbf{Z}\times\mathbf{Z}^{2\times 2}\times\mathbf{Z} \,:\, a \equiv_2 f,\ a+2b+2e+f \equiv_3 0,\ e \equiv_3 f,\ d \equiv_3 0\,\} \\ &= \{\,(a, \left(\begin{smallmatrix} b & c \\ d & e \end{smallmatrix}\right), f) \in \mathbf{Z}\times\mathbf{Z}^{2\times 2}\times\mathbf{Z} \,:\, a \equiv_2 f,\ a \equiv_3 b,\ e \equiv_3 f,\ d \equiv_3 0\,\}\,. \end{aligned}$$

Aufgabe 19

(1) Es ist $(A,+)$ eine abelsche Gruppe, da A ein Ring ist.

Es ist $1_R \cdot a = \varphi(1_R)a = 1_A a = a$ für $a \in A$.

Es ist $(rs)\cdot a = \varphi(rs)a = \varphi(r)\varphi(s)a = r\cdot(s\cdot a)$ für $r,\, s \in R$ und $a \in A$.

Es ist $(r+\tilde r)\cdot(a+\tilde a) = \varphi(r+\tilde r)(a+\tilde a) = (\varphi(r)+\varphi(\tilde r))(a+\tilde a) = \varphi(r)a + \varphi(\tilde r)a + \varphi(r)\tilde a + \varphi(\tilde r)\tilde a = r\cdot a + \tilde r\cdot a + r\cdot\tilde a + \tilde r\cdot\tilde a$ für $r,\, \tilde r \in R$ und $a,\, \tilde a \in A$.

(2) Sei f ein R-Algebrenmorphismus, i.e. sei $f\circ\varphi = \psi$ erfüllt. Da f ein Ringmorphismus ist, ist f mit der Addition verträglich. Ferner ist $f(r\cdot a) = f(\varphi(r)a) = f(\varphi(r))f(a) = \psi(r)f(a) = r\cdot f(a)$. Zusammen ist f somit R-linear.

Sei f umgekehrt nun R-linear. Wir haben zu zeigen, daß $f\circ\varphi \stackrel{!}{=} \psi$. Sei $r \in R$. Es wird $(f\circ\varphi)(r) = f(\varphi(r)) = f(\varphi(r)1_A) = f(r\cdot 1_A) = r\cdot f(1_A) = \psi(r)1_B = \psi(r)$.

(3) Für $a,\, \tilde a \in A$ ist

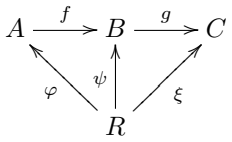
$$\begin{array}{lcll} g(f(1_A)) & = & 1_C & = & g(1_B) \\ g(f(a+\tilde a)) & = & g(f(a)) + g(f(\tilde a)) & = & g(f(a)+f(\tilde a)) \\ g(f(a\cdot\tilde a)) & = & g(f(a))\cdot g(f(\tilde a)) & = & g(f(a)\cdot f(\tilde a)) \end{array}$$

Dank Injektivität von g folgt hieraus, daß

$$\begin{array}{lcl} f(1_A) & = & 1_B \\ f(a+\tilde a) & = & f(a)+f(\tilde a) \\ f(a\cdot\tilde a) & = & f(a)\cdot f(\tilde a) \end{array}$$

ist. Also ist f ein Ringmorphismus.

Ferner ist $g \circ f \circ \varphi = \xi = g \circ \psi$, wegen g injektiv also $f \circ \varphi = \psi$.



Ist nun g bijektiv, so können wir $f := g^-$ setzen und erhalten wegen g injektiver R-Algebrenmorphismus und wegen $g \circ g^- = \mathrm{id}_C$ ein R-Algebrenmorphismus mit vorigem, daß auch g^- ein R-Algebrenmorphismus ist.

Cf. Bemerkung 61, Definition 57.(2).

Aufgabe 20

(1) Sei $f \in \mathrm{Hom}_A(M, N) \setminus \{0\}$. Wir haben zu zeigen, daß f ein Isomorphismus ist.
Es ist $\mathrm{Kern}\, f \subseteq M$ ein Teilmodul. Da $f \neq 0$, ist $\mathrm{Kern}\, f \neq M$. Da M einfach ist, folgt $\mathrm{Kern}\, f = 0$.
Es ist $\mathrm{Im}\, f \subseteq N$ ein Teilmodul. Da $f \neq 0$, ist $\mathrm{Im}\, f \neq 0$. Da N einfach ist, folgt $\mathrm{Im}\, f = N$.
Da $\mathrm{Kern}\, f = 0$ und $\mathrm{Im}\, f = N$ ist, ist f ein Isomorphismus.

(2) Da $M \neq 0$ ist, ist $0 \neq \mathrm{id}_M \in \mathrm{End}_A M$. Nach (1) sind alle Elemente von $\mathrm{End}_A M$ ungleich 0 invertierbar. Also ist $\mathrm{End}_A M$ ein Schiefkörper.

(3) Sei $m \in M \setminus \{0\}$. Es ist $f : A \longrightarrow M$, $a \longmapsto am$ eine A-lineare Abbildung. Es ist $\mathrm{Im}\, f$ ein Teilmodul von M. Da $m = 1 \cdot m \in \mathrm{Im}\, f$, ist $\mathrm{Im}\, f \neq 0$. Da M einfach ist, ist $\mathrm{Im}\, f = M$.

(4) Wir behaupten die Existenz des Ringmorphismus

$$\begin{array}{ccc} R & \xrightarrow{\psi} & \mathrm{End}_A X \\ r & \longmapsto & (x \mapsto \varphi(r)x)\ . \end{array}$$

Es ist ψ wohldefiniert, da $\varphi(r) \in \mathrm{Z}(A)$ ist und also $X \to X$, $x \mapsto \varphi(r)x$ eine A-lineare Abbildung ist.
Es ist ψ ein Ringmorphismus, da mit 1, Addition und Multiplikation verträglich; letzteres, da für $r, s \in R$ sich

$$(x \mapsto \varphi(r)x) \circ (x \mapsto \varphi(s)x) \;=\; (x \mapsto \varphi(r)\varphi(s)x) \;=\; (x \mapsto \varphi(rs)x)$$

ergibt.
Ferner ist $\psi(r) = (x \mapsto \varphi(r)x)$ zentral in $\mathrm{End}_A X$, da wir für $f \in \mathrm{End}_A X$ und $y \in X$

$$\begin{array}{rcl} (\psi(r) \circ f)(y) & = & (x \mapsto \varphi(r)x)f(y) \\ & = & \varphi(r)f(y) \\ & = & f(\varphi(r)y) \\ & = & (f \circ (x \mapsto \varphi(r)x))(y) \\ & = & (f \circ \psi(r))(y) \end{array}$$

erhalten.

(5) Wir schreiben $D := \mathrm{End}_A M$. Es ist D ein Schiefkörper; cf. Lemma 66.(3).
Nach (3) gibt es eine surjektive A-lineare Abbildung $A \longrightarrow M$. Da diese auch K-linear ist und da A endlichdimensional über K ist, folgt, daß M endlichdimensional über K ist. Also ist auch $\mathrm{End}_K M$ endlichdimensional über K. Folglich ist auch der Teilraum $D \subseteq \mathrm{End}_K M$ endlichdimensional über K.

Es ist $D \neq 0$, da $M \neq 0$ und also auch $0 \neq \mathrm{id}_M = 1_D \in D$.

Wir haben den algebrendefinierenden Ringmorphismus $f : K \longrightarrow D$; cf. (4). Dieser ist nicht null, da er 1_K nach $1_D \neq 0$ schickt. Da K als Körper nur die Ideale 0 und K hat, folgt, daß Kern $f = 0$ und also f injektiv ist.

Schreibe $K' := f(K) \subseteq D$. Es ist $f|^{K'} : K \longrightarrow K'$ ein Isomorphismus. Es ist D via $K' \hookrightarrow D$ ein eine K'-Algebra, endlichdimensional, da darin eine K'-lineare Basis auch eine K-lineare Basis ist.

Wir müssen zeigen, daß $K' \stackrel{!}{=} D$ ist. Sei $d \in D$. Wir haben zu zeigen, daß $d \stackrel{!}{\in} K'$ ist.

Der Kern des K'-Algebrenmorphismus $h : K'[X] \longrightarrow D$, $u(X) \longmapsto u(d)$ ist ungleich 0, da D endlichdimensional über K' ist. Also ist er von einem normierten Polynom $v(X)$ erzeugt.

Annahme, es ist $v(X)$ reduzibel. Dann ist $v(X) = a(X) \cdot b(X)$ mit normierten Polynomen $a(X)$ und $b(X)$ von Grad $\geqslant 1$. Es folgt $0 = v(d) = a(d) \cdot b(d)$, und somit $a(d) = 0$ oder $b(d) = 0$. O.E. sei $a(d) = 0$. Also ist $a(X)$ im Kern von h, und somit ein Vielfaches von $v(X)$. Da $\deg v - \deg a = \deg b \geqslant 1$, ist dies aber *nicht möglich.*

Somit ist $v(X)$ irreduzibel. Da aber K' ($\simeq K$) algebraisch abgeschlossen ist, folgt, daß $\deg v = 1$; da $v(d) = 0$ also $v(X) = X - d$, insbesondere also $d \in K'$.

> Alternativ können wir wie folgt argumentieren. Sei $f \in \mathrm{End}_A M$. Wir wollen zeigen, daß $f = \lambda\,\mathrm{id}_M$ für ein $\lambda \in K$. Da f auch ein K-linearer Endomorphismus von M ist und da K algebraisch abgeschlossen ist, hat f einen Eigenwert $\lambda \in K$. Es ist der Eigenraum $\mathrm{Kern}(\lambda\,\mathrm{id}_M - f)$ ungleich 0. Wir wollen zeigen, daß er gleich M ist, denn dann ist $\lambda\,\mathrm{id}_M - f = 0$. Da M ein einfacher A-Modul ist, genügt es zu zeigen, daß $\mathrm{Kern}(\lambda\,\mathrm{id}_M - f)$ ein A-Teilmodul von M ist. Das aber folgt daraus, daß $\lambda\,\mathrm{id}_M$ und f beide A-linear sind.
>
> Cf. Lemma 66.

Aufgabe 21

(1) Die Aussage trifft zu.

Es ist $(\mathrm{e}_{1,1}, \ldots, \mathrm{e}_{n,n})$ eine orthogonale Zerlegung in Idempotente. Mithin ist

$$K^{n\times n} \;=\; \bigoplus_{i\in[1,n]} K^{n\times n}\mathrm{e}_{i,i}\;.$$

Sei $i \in [1,n]$. Wir *behaupten,* daß $K^{n\times n}\mathrm{e}_{i,i}$ ein einfacher $K^{n\times n}$-Modul ist.

Sei $0 \neq X \subseteq K^{n\times n}\mathrm{e}_{i,i}$ ein Teilmodul. Wir haben $X \stackrel{!}{=} K^{n\times n}\mathrm{e}_{i,i}$ nachzuweisen. Sei

$$x \;=\; \textstyle\sum_{j\in[1,n]} \xi_j \mathrm{e}_{j,i} \;\in\; X \smallsetminus \{0\}\;,$$

wobei $\xi_j \in K$ für $j \in [1,n]$. Sei $\ell \in [1,n]$ mit $\xi_\ell \neq 0$. Für $k \in [1,n]$ wird

$$X \;\ni\; \xi_\ell^{-1}\mathrm{e}_{k,\ell}\textstyle\sum_{j\in[1,n]} \xi_j \mathrm{e}_{j,i} \;=\; \mathrm{e}_{k,i}\;.$$

Also liegt von der K-linearen Basis $(\mathrm{e}_{1,i}, \ldots, \mathrm{e}_{n,i})$ von $K^{n\times n}\mathrm{e}_{i,i}$ jeder Eintrag im Teilraum X. Dies zeigt $X = K^{n\times n}\mathrm{e}_{i,i}$ und damit die *Behauptung.*

Nach Lemma 65.(3) ist also $K^{n\times n}$ halbeinfach.

(2) Die Aussage trifft zu.

Ist $S \subseteq A$ ein einfacher A-Teilmodul, so ist $S \times 0 \subseteq A \times B$ ein einfacher $A \times B$-Teilmodul von $A \times B$, da in der ersten Komponente nur A operiert.

Analog in zweiter Komponente.

Schreibe $A = \bigoplus_{i\in[1,m]} S_i$, wobei $S_i \subseteq A$ ein einfacher A-Teilmodul ist für $i \in [1,m]$; cf. Lemma 65.

Schreibe $B = \bigoplus_{j\in[1,n]} T_j$, wobei $T_j \subseteq B$ ein einfacher B-Teilmodul ist für $j \in [1,n]$; cf. Lemma 65.

Es ist

$$A \times B \;=\; (A \times 0) \oplus (0 \times B) \;=\; \Big(\bigoplus_{i \in [1,m]} S_i \times 0 \Big) \oplus \Big(\bigoplus_{j \in [1,n]} 0 \times T_j \Big) \,.$$

Nach Lemma 65 ist also $A \times B$ halbeinfach.

(3) Die Aussage trifft zu.

Sei M ein endlichdimensionaler B-Modul. Sei $N \subseteq M$ ein B-Teilmodul. Wir haben einen B-Teilmodul $X \subseteq M$ so zu finden, daß $M = N \oplus X$. Denn gemäß Lemma 65 zeigt dies die Halbeinfachheit von B.

Es ist M ein A-Modul via $a \cdot m := f(a)m$ für $a \in A$ und $m \in M$. Es ist $N \subseteq M$ auch ein A-Teilmodul. Da A halbeinfach ist, gibt es einen A-Teilmodul $X \subseteq M$ mit $M = N \oplus X$. Da $f : A \to B$ surjektiv ist, ist $X \subseteq M$ auch ein B-Teilmodul.

(4) Die Aussage trifft nicht zu.

Sei etwa $A = K^{2\times 2} = \left(\begin{smallmatrix} K & K \\ K & K \end{smallmatrix}\right)$, halbeinfach nach (1). Sei $B = \left(\begin{smallmatrix} K & K \\ 0 & K \end{smallmatrix}\right)$, und sei $g : B \to A$ die Inklusion.

Es ist B nicht halbeinfach. Denn es ist zwar $e := \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in B$ primitiv, da es sogar in A primitiv ist; cf. Beispiel 54 ([4]). Aber $Be = \left(\begin{smallmatrix} 0 & K \\ 0 & K \end{smallmatrix}\right)$ ist kein einfacher B-Linksmodul, sondern weist vielmehr den Teilmodul $\left(\begin{smallmatrix} 0 & K \\ 0 & 0 \end{smallmatrix}\right)$ auf.

Aufgabe 22

Wir erinnern daran, daß primitive Idempotente insbesondere ungleich 0 sind.

Nach Bemerkung 64 gibt es in A eine orthogonale Zerlegung $\underline{e} = (e_1 \,, \ldots \,, e_n)$ in primitive Idempotente.

Wir haben zu zeigen, daß dies (bis auf Reihenfolge) die einzige Zerlegung in primitive Idempotente in A ist.

Sei f ein primitives Idempotent in A. Es genügt zu zeigen, daß $f \stackrel{!}{=} e_i$ ist für ein $i \in [1, n]$.

Denn dann können in einer orthogonalen Zerlegung $\underline{\tilde{e}}$ in primitive Idempotente in A nur Einträge von $\underline{e}$ auftreten. Wegen Orthogonalität kann $\underline{\tilde{e}}$ jeden Eintrag von $\underline{e}$ höchstens einmal beinhalten. Da die Summe der Einträge von $\underline{\tilde{e}}$ gleich 1 ist, kann auch kein Eintrag von $\underline{e}$ in $\underline{\tilde{e}}$ fehlen; beachte, daß Summe jedes nichtleeren Teiltupels von $\underline{e}$ nicht null ist, wie man durch Multiplikation mit einem beteiligten Eintrag erkennt. Insgesamt stimmen $\underline{e}$ und $\underline{\tilde{e}}$ dann bis auf Reihenfolge überein.

Betrachten wir also unser f. Es ist $f = fe_1 + \cdots + fe_n$. Da $f \neq 0$, gibt es ein $i \in [1, n]$ mit $fe_i \neq 0$.

Es ist $f = fe_i + f(1 - e_i)$. Da A kommutativ ist, sind fe_i und $f(1 - e_i)$ Idempotente. Da A kommutativ ist, ist $(fe_i)(f(1-e_i)) = 0$ und $(f(1-e_i))(fe_i) = 0$. Da f primitiv ist und da $fe_i \neq 0$, folgt $f(1-e_i) = 0$, also $f = fe_i$.

Es ist $e_i = fe_i + (1-f)e_i$. Da A kommutativ ist, sind fe_i und $(1-f)e_i$ Idempotente. Da A kommutativ ist, ist $(fe_i)((1-f)e_i) = 0$ und $((1-f)e_i)(fe_i) = 0$. Da e_i primitiv ist und da $fe_i \neq 0$, folgt $(1-f)e_i = 0$, also $e_i = fe_i$.

Insgesamt ist $f = fe_i = e_i$ gezeigt.

[4] Oder Beweis zu (1), Bemerkung 55 : Es ist Ae einfach, also unzerlegbar, also e primitiv.

Aufgabe 23

(1) Es ist $\mathrm{D}_8 := \langle\, a,\, b \,:\, a^4,\, b^2,\, (ba)^2 \,\rangle$. Es ist $|\mathrm{D}_8| = 8$. Es ist $\mathrm{D}_8 = \{\, a^i b^j \,:\, i \in [0,3],\ j \in [0,1] \,\}$. Cf. Beispiel 25.

Sei $\mathrm{C}_2 \times \mathrm{C}_2 = \langle x : x^2 \rangle \times \langle y : y^2 \rangle$.

Wir haben den surjektiven Gruppenmorphismus $p : \mathrm{D}_8 \longrightarrow \mathrm{C}_2 \times \mathrm{C}_2$, $a \longmapsto (x,1)$, $b \longmapsto (1,y)$, da $(x,1)^4 = 1$, $(1,y)^2 = 1$ und $((1,y)(x,1))^2 = 1$; cf. Satz 24.

Wir haben die Darstellungen $\mathrm{C}_2 \times \mathrm{C}_2 \longrightarrow \mathrm{GL}_1(\mathbf{C})$, $(x,1) \longmapsto \pm 1$, $(1,y) \longmapsto \pm 1$.

Komposition mit p gibt die Darstellungen

$$\begin{array}{ccc} \mathrm{D}_8 & \longrightarrow & \mathrm{GL}_1(\mathbf{C}) \\ a & \longmapsto & +1 \\ b & \longmapsto & +1 \end{array}$$

(trivial),

$$\begin{array}{ccc} \mathrm{D}_8 & \longrightarrow & \mathrm{GL}_1(\mathbf{C}) \\ a & \longmapsto & +1 \\ b & \longmapsto & -1\,, \end{array}$$

$$\begin{array}{ccc} \mathrm{D}_8 & \longrightarrow & \mathrm{GL}_1(\mathbf{C}) \\ a & \longmapsto & -1 \\ b & \longmapsto & +1 \end{array}$$

und

$$\begin{array}{ccc} \mathrm{D}_8 & \longrightarrow & \mathrm{GL}_1(\mathbf{C}) \\ a & \longmapsto & -1 \\ b & \longmapsto & -1\,. \end{array}$$

Es operiert D_8 auf einem Quadrat. Die entsprechende Darstellung über lineare Selbstabbildungen der Ebene ist e.g. gegeben durch

$$\begin{array}{ccc} \mathrm{D}_8 & \longrightarrow & \mathrm{GL}_2(\mathbf{C}) \\ a & \longmapsto & \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \\ b & \longmapsto & \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \end{array}$$

Eine kurze Rechnung bestätigt auch abermals via Satz 24, daß all diese Darstellungen existieren.

Wir erhalten den $\mathbf{C}$-Algebrenmorphismus

$$\begin{array}{rcccccccccc} \mathbf{C}\mathrm{D}_8 & \overset{\omega}{\longrightarrow} & (\mathbf{C} & \times & \mathbf{C} & \times & \mathbf{C} & \times & \mathbf{C} & \times & \mathbf{C}^{2\times 2}) \\ a^0 & \longmapsto & (1 & , & 1 & , & 1 & , & 1 & , & \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) \\ a^1 & \longmapsto & (1 & , & 1 & , & -1 & , & -1 & , & \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)) \\ a^2 & \longmapsto & (1 & , & 1 & , & 1 & , & 1 & , & \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)) \\ a^3 & \longmapsto & (1 & , & 1 & , & -1 & , & -1 & , & \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)) \\ a^0 b & \longmapsto & (1 & , & -1 & , & 1 & , & -1 & , & \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)) \\ a^1 b & \longmapsto & (1 & , & -1 & , & -1 & , & 1 & , & \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)) \\ a^2 b & \longmapsto & (1 & , & -1 & , & 1 & , & -1 & , & \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) \\ a^3 b & \longmapsto & (1 & , & -1 & , & -1 & , & 1 & , & \left(\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right))\,. \end{array}$$

Dies liefert die folgende beschreibende Matrix bezüglich der Basis D_8 von $\mathbf{C}\mathrm{D}_8$ und der Standardbasis der rechten Seite.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \end{pmatrix}$$

Diese hat Determinante ist 2^{10}. Folglich ist ω ein $\mathbf{C}$-Algebrenisomorphismus.

In diesem Argument kann man auch $\mathbf{C}$ durch $\mathbf{Q}$ ersetzen.

(2) In D_{10} gilt $a^5 = 1$, $b^2 = 1$ und $baba = 1$, also auch $ba = a^4 b$. Also ist

$$\mathrm{D}_{10} \;=\; \{\, a^i b^j \;:\; i \in [0,4],\; j \in [0,1] \,\} \,.$$

Wir haben den Gruppenmorphismus

$$\begin{array}{ccc} \mathrm{D}_{10} & \longrightarrow & \mathrm{S}_5 \\ a & \longmapsto & (1,2,3,4,5) \\ b & \longmapsto & (2,5)(3,4) \,, \end{array}$$

da $(1,2,3,4,5)^5 = \mathrm{id}$, $((2,5)(3,4))^2 = \mathrm{id}$ und $((2,5)(3,4) \circ (1,2,3,4,5))^2 = ((1,5)(2,4))^2 = \mathrm{id}$.

Das Bild $\langle (1,2,3,4,5), (2,5)(3,4) \rangle$ dieses Gruppenmorphismus hat 10 Elemente, denn es hat $\leqslant 10$ Elemente, es hat eine Untergruppe von Ordnung 5 und es hat eine Untergruppe von Ordnung 2.

Also ist $|\mathrm{D}_{10}| = 10$.

Betrachte $\mathrm{C}_2 = \langle x : x^2 \rangle$. Wir haben den Gruppenmorphismus $p : \mathrm{D}_{10} \longrightarrow \mathrm{C}_2$, $a \longmapsto 1$, $b \longmapsto x$, da $1^5 = 1$, $x^2 = 1$ und $(1 \cdot x)^2 = 1$.

Wir haben die Darstellungen $\mathrm{C}_2 \longrightarrow \mathrm{GL}_1(\mathbf{C})$, $x \longmapsto \pm 1$.

Komposition mit p gibt die Darstellungen

$$\begin{array}{ccc} \mathrm{D}_{10} & \longrightarrow & \mathrm{GL}_1(\mathbf{C}) \\ a & \longmapsto & +1 \\ b & \longmapsto & +1 \end{array}$$

(trivial) und

$$\begin{array}{ccc} \mathrm{D}_{10} & \longrightarrow & \mathrm{GL}_1(\mathbf{C}) \\ a & \longmapsto & +1 \\ b & \longmapsto & -1 \,. \end{array}$$

Schreibe $\zeta := \zeta_5$. Wir haben ferner die Darstellung

$$\begin{array}{ccc} \mathrm{D}_{10} & \longrightarrow & \mathrm{GL}_2(\mathbf{C}) \\ a & \longmapsto & \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right) \\ b & \longmapsto & \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \,. \end{array}$$

Ganz ähnlich ergibt sich die Darstellung

$$\begin{array}{ccc} \mathrm{D}_{10} & \longrightarrow & \mathrm{GL}_2(\mathbf{C}) \\ a & \longmapsto & \left(\begin{smallmatrix} \zeta^2 & 0 \\ 0 & \zeta^{-2} \end{smallmatrix}\right) \\ b & \longmapsto & \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \,. \end{array}$$

Eine kurze Rechnung bestätigt auch abermals via Satz 24, daß all diese Darstellungen existieren.

Wir erhalten den $\mathbf{C}$-Algebrenmorphismus

$$\begin{array}{rcccccccc}
\mathbf{C}\mathrm{D}_{10} & \xrightarrow{\omega} & (\mathbf{C} & \times & \mathbf{C} & \times & \mathbf{C}^{2\times 2} & \times & \mathbf{C}^{2\times 2} \\
a^0 & \longmapsto & (1 & , & 1 & , & \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) & , & \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)) \\
a^1 & \longmapsto & (1 & , & 1 & , & \left(\begin{smallmatrix}\zeta&0\\0&\zeta^{-1}\end{smallmatrix}\right) & , & \left(\begin{smallmatrix}\zeta^2&0\\0&\zeta^{-2}\end{smallmatrix}\right)) \\
a^2 & \longmapsto & (1 & , & 1 & , & \left(\begin{smallmatrix}\zeta^2&0\\0&\zeta^{-2}\end{smallmatrix}\right) & , & \left(\begin{smallmatrix}\zeta^4&0\\0&\zeta^{-4}\end{smallmatrix}\right)) \\
a^3 & \longmapsto & (1 & , & 1 & , & \left(\begin{smallmatrix}\zeta^3&0\\0&\zeta^{-3}\end{smallmatrix}\right) & , & \left(\begin{smallmatrix}\zeta^6&0\\0&\zeta^{-6}\end{smallmatrix}\right)) \\
a^4 & \longmapsto & (1 & , & 1 & , & \left(\begin{smallmatrix}\zeta^4&0\\0&\zeta^{-4}\end{smallmatrix}\right) & , & \left(\begin{smallmatrix}\zeta^8&0\\0&\zeta^{-8}\end{smallmatrix}\right)) \\
a^0b & \longmapsto & (1 & , & -1 & , & \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right) & , & \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)) \\
a^1b & \longmapsto & (1 & , & -1 & , & \left(\begin{smallmatrix}0&\zeta\\\zeta^{-1}&0\end{smallmatrix}\right) & , & \left(\begin{smallmatrix}0&\zeta^2\\\zeta^{-2}&0\end{smallmatrix}\right)) \\
a^2b & \longmapsto & (1 & , & -1 & , & \left(\begin{smallmatrix}0&\zeta^2\\\zeta^{-2}&0\end{smallmatrix}\right) & , & \left(\begin{smallmatrix}0&\zeta^4\\\zeta^{-4}&0\end{smallmatrix}\right)) \\
a^3b & \longmapsto & (1 & , & -1 & , & \left(\begin{smallmatrix}0&\zeta^3\\\zeta^{-3}&0\end{smallmatrix}\right) & , & \left(\begin{smallmatrix}0&\zeta^6\\\zeta^{-6}&0\end{smallmatrix}\right)) \\
a^4b & \longmapsto & (1 & , & -1 & , & \left(\begin{smallmatrix}0&\zeta^4\\\zeta^{-4}&0\end{smallmatrix}\right) & , & \left(\begin{smallmatrix}0&\zeta^8\\\zeta^{-8}&0\end{smallmatrix}\right)) \,.
\end{array}$$

Dies liefert die folgende beschreibende Matrix bezüglich der Basis D_{10} von $\mathbf{C}\mathrm{D}_{10}$ und der Standardbasis der rechten Seite.

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\
1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 \\
0 & 0 & 0 & 0 & 0 & 1 & \zeta^{-1} & \zeta^{-2} & \zeta^{-3} & \zeta^{-4} \\
1 & \zeta^{-1} & \zeta^{-2} & \zeta^{-3} & \zeta^{-4} & 0 & 0 & 0 & 0 & 0 \\
1 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^8 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^8 \\
0 & 0 & 0 & 0 & 0 & 1 & \zeta^{-2} & \zeta^{-4} & \zeta^{-6} & \zeta^{-8} \\
1 & \zeta^{-2} & \zeta^{-4} & \zeta^{-6} & \zeta^{-8} & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Diese hat Determinante ist $-2 \cdot 5^5$. Folglich ist ω ein $\mathbf{C}$-Algebrenisomorphismus.

(3) In Q_8 gilt $a^4 = 1$. Wegen $a^2b^2 = 1$ folgt $b^4 = a^{-4} = 1$. Insbesondere wird $a^2 = b^{-2} = b^2 =: z$. Es wird $az = za$, $bz = zb$, also ist $z \in \mathrm{Z}(\mathrm{Q}_8)$.

Wegen $b^-aba = 1$ ist $ba = a^-b = zab$. Folglich ist jedes Element von Q_8 von der Form a^ib^j mit $i, j \in [0,3]$. Unter Verwendung von z wird also

$$\mathrm{Q}_8 \;=\; \{\, a^ib^jz^k \;:\; i, j, k \in \{0,1\} \,\}\,.$$

Insbesondere ist $|\mathrm{Q}_8| \leqslant 8$.

Man kann auch

$$\mathrm{Q}_8 \;=\; \{\, a^ib^j \;:\; i \in [0,3],\; j \in [0,1] \,\}\,.$$

schreiben.

Die Quaternionen als Teilring von $\mathbf{C}^{2\times 2}$ realisiert geben einen Hinweis auf die Darstellung

$$\begin{array}{rcl}
\mathrm{Q}_8 & \longrightarrow & \mathrm{GL}_2(\mathbf{C}) \\
a & \longmapsto & \left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right) \\
b & \longmapsto & \left(\begin{smallmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{smallmatrix}\right)\,,
\end{array}$$

die man mit Satz 24 bestätigt.

Ihr Bild ist gegeben durch $\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \pm\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right), \pm\left(\begin{smallmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{smallmatrix}\right), \pm\left(\begin{smallmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{smallmatrix}\right), \}$, wie eine direkte Rechnung ergibt.

Es folgt $|\mathrm{Q}_8| = 8$.

Wir betrachten $\mathrm{C}_2 \times \mathrm{C}_2 = \langle x : x^2 \rangle \times \langle y : y^2 \rangle$. Wir haben den Gruppenmorphismus $\mathrm{Q}_8 \twoheadrightarrow \mathrm{C}_2 \times \mathrm{C}_2$, $a \mapsto (x, 1)$, $b \mapsto (1, y)$, wie man mit Satz 24 bestätigt. Dies gibt weiters die Darstellungen

$$\begin{array}{rcl} \mathrm{Q}_8 & \longrightarrow & \mathrm{GL}_1(\mathbf{C}) \\ a & \longmapsto & +1 \\ b & \longmapsto & +1 \end{array}$$

(trivial),

$$\begin{array}{rcl} \mathrm{Q}_8 & \longrightarrow & \mathrm{GL}_1(\mathbf{C}) \\ a & \longmapsto & +1 \\ b & \longmapsto & -1\,, \end{array}$$

$$\begin{array}{rcl} \mathrm{Q}_8 & \longrightarrow & \mathrm{GL}_1(\mathbf{C}) \\ a & \longmapsto & -1 \\ b & \longmapsto & +1 \end{array}$$

und

$$\begin{array}{rcl} \mathrm{Q}_8 & \longrightarrow & \mathrm{GL}_1(\mathbf{C}) \\ a & \longmapsto & -1 \\ b & \longmapsto & -1\,. \end{array}$$

Wir erhalten den $\mathbf{C}$-Algebrenmorphismus

$$\begin{array}{rcl} \mathbf{C}\mathrm{Q}_8 & \xrightarrow{\omega} & (\mathbf{C} \times \mathbf{C} \times \mathbf{C} \times \mathbf{C} \times \mathbf{C}^{2\times 2}) \\ a^0 & \longmapsto & (1, 1, 1, 1, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) \\ a^1 & \longmapsto & (1, 1, -1, -1, \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)) \\ a^2 & \longmapsto & (1, 1, 1, 1, \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)) \\ a^3 & \longmapsto & (1, 1, -1, -1, \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)) \\ a^0 b & \longmapsto & (1, -1, 1, -1, \left(\begin{smallmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{smallmatrix}\right)) \\ a^1 b & \longmapsto & (1, -1, -1, 1, \left(\begin{smallmatrix} 0 & -\mathrm{i} \\ -\mathrm{i} & 0 \end{smallmatrix}\right)) \\ a^2 b & \longmapsto & (1, -1, 1, -1, \left(\begin{smallmatrix} -\mathrm{i} & 0 \\ 0 & \mathrm{i} \end{smallmatrix}\right)) \\ a^3 b & \longmapsto & (1, -1, -1, 1, \left(\begin{smallmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{smallmatrix}\right))\,. \end{array}$$

Dies liefert die folgende beschreibende Matrix bezüglich der Basis Q_8 von $\mathbf{C}\mathrm{Q}_8$ und der Standardbasis der rechten Seite.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 0 & -1 & 0 & \mathrm{i} & 0 & -\mathrm{i} & 0 \\ 0 & 1 & 0 & -1 & 0 & -\mathrm{i} & 0 & \mathrm{i} \\ 0 & -1 & 0 & 1 & 0 & -\mathrm{i} & 0 & \mathrm{i} \\ 1 & 0 & -1 & 0 & -\mathrm{i} & 0 & \mathrm{i} & 0 \end{pmatrix}$$

Diese hat Determinante ist -2^{10}. Folglich ist ω ein $\mathbf{C}$-Algebrenisomorphismus.

Aufgabe 24

(1) Es ist $\mathrm{D}_8 = \langle\, a : a^4,\, b^2,\, (ba)^2 \,\rangle = \{\, a^i b^j \,:\, i \in [0,3],\ j \in [0,1] \,\}$; cf. Beispiel 25.

Beachte, daß ${}^b a = bab = a^-$ und ${}^a b = aba^- = a^2 b$ ist.

Die Konjugationsklassen in D_8 ergeben sich zu $\{1\}$, $\{a^2\}$, $\{a, a^3\}$, $\{ab, a^3 b\}$, $\{b, a^2 b\}$.

Als Repräsentanten wählen wir e.g. $g_1 := 1$, $g_2 := a^2$, $g_3 := a$, $g_4 := ab$ und $g_5 := b$.

Der Wedderburnisomorphismus von Aufgabe 23.(1) ergab

$$\begin{array}{rcrcl}
 & & \mathbf{C}\mathrm{D}_8 & \xrightarrow{\omega} & (\mathbf{C} \times \mathbf{C} \times \mathbf{C} \times \mathbf{C} \times \mathbf{C}^{2\times 2}) \\
 & & \xi & \longmapsto & (\omega^1(\xi)\,,\ \omega^2(\xi)\,,\ \omega^3(\xi)\,,\ \omega^4(\xi)\,,\ \omega^5(\xi)) \\
g_1 & = & 1 & \longmapsto & (1\ ,\ 1\ ,\ 1\ ,\ 1\ ,\ \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)) \\
g_2 & = & a^2 & \longmapsto & (1\ ,\ 1\ ,\ 1\ ,\ 1\ ,\ \left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)) \\
g_3 & = & a & \longmapsto & (1\ ,\ 1\ ,\ -1\ ,\ -1\ ,\ \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)) \\
g_4 & = & ab & \longmapsto & (1\ ,\ -1\ ,\ -1\ ,\ 1\ ,\ \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)) \\
g_5 & = & b & \longmapsto & (1\ ,\ -1\ ,\ 1\ ,\ -1\ ,\ \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right))\,.
\end{array}$$

Spurbildung $\chi_s(g_u) = \operatorname{tr}\omega^s(g_u)$ für $s,\, u \in [1,5]$ führt zur Charaktertafel

$$\mathrm{X}(\mathrm{D}_8) \;=\; \begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \\ \chi_5 \end{array}\!\!\begin{array}{c} \begin{array}{ccccc} 1 & a^2 & a & ab & b \end{array} \\ \left[\begin{array}{ccccc} 1 & 1 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ 2 & -2 & 0 & 0 & 0 \end{array}\right] \end{array},$$

wobei für spätere Zwecke direkt unter den Konjugationsklassenrepräsentanten die Länge ihrer Konjugationsklassen notiert wurde.

(2) Schreibe $\zeta := \zeta_5$.

Es ist $\mathrm{D}_{10} := \langle\, a,\, b \,:\, a^5,\, b^2,\, (ba)^2 \,\rangle = \{\, a^i b^j \,:\, i \in [0,4],\ j \in [0,1] \,\}$; cf. Aufgabe 23.(2) und Lösung dazu.

Beachte, daß ${}^b a = bab = a^-$ und ${}^a b = aba^- = a^2 b$ ist.

Die Konjugationsklassen in D_{10} ergeben sich zu $\{1\}$, $\{a,\, a^4\}$, $\{a^2,\, a^3\}$ und $\{b,\, ab,\, a^2b,\, a^3b,\, a^4b\}$.

Als Repräsentanten wählen wir e.g. $g_1 := 1$, $g_2 := a$, $g_3 := a^2$ und $g_4 := b$.

Der Wedderburnisomorphismus von Aufgabe 23.(2) ergab

$$\begin{array}{rcrcl}
 & & \mathbf{C}\mathrm{D}_{10} & \xrightarrow{\omega} & (\mathbf{C} \times \mathbf{C} \times \mathbf{C}^{2\times 2} \times \mathbf{C}^{2\times 2} \\
 & & \xi & \longmapsto & (\omega^1(\xi)\,,\ \omega^2(\xi)\,,\ \omega^3(\xi)\ ,\ \omega^4(\xi)) \\
g_1 & = & 1 & \longmapsto & (1\ ,\ 1\ ,\ \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\ ,\ \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)) \\
g_2 & = & a & \longmapsto & (1\ ,\ 1\ ,\ \left(\begin{smallmatrix}\zeta&0\\0&\zeta^{-1}\end{smallmatrix}\right)\ ,\ \left(\begin{smallmatrix}\zeta^2&0\\0&\zeta^{-2}\end{smallmatrix}\right)) \\
g_3 & = & a^2 & \longmapsto & (1\ ,\ 1\ ,\ \left(\begin{smallmatrix}\zeta^2&0\\0&\zeta^{-2}\end{smallmatrix}\right)\ ,\ \left(\begin{smallmatrix}\zeta^4&0\\0&\zeta^{-4}\end{smallmatrix}\right)) \\
g_4 & = & b & \longmapsto & (1\ ,\ -1\ ,\ \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\ ,\ \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right))\,.
\end{array}$$

Spurbildung $\chi_s(g_u) = \operatorname{tr}\omega^s(g_u)$ für $s,\, u \in [1,4]$ führt zur Charaktertafel

$$\mathrm{X}(\mathrm{D}_{10}) \;=\; \begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 1 & a & a^2 & b \end{array} \\ \left[\begin{array}{cccc} 1 & 2 & 2 & 5 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 2 & \zeta+\zeta^{-1} & \zeta^2+\zeta^{-2} & 0 \\ 2 & \zeta^2+\zeta^{-2} & \zeta+\zeta^{-1} & 0 \end{array}\right] \end{array},$$

wobei für spätere Zwecke direkt unter den Konjugationsklassenrepräsentanten die Länge ihrer Konjugationsklassen notiert wurde.

(3) Es ist $\mathrm{Q}_8 = \langle\, a, b \,:\, a^4, a^2b^2, b^-aba \,\rangle = \{\, a^ib^jz^k \,:\, i, j, k \in \{0,1\}\,\}$, wobei $z := a^2 = b^2$; cf. Aufgabe 23.(3) und Lösung dazu.

Beachte, daß $z \in \mathrm{Z}(\mathrm{Q}_8)$, $abab^- = {}^b(b^-aba) = 1$, ${}^ba = bab^- = a^- = za$ und ${}^ab = aba^- = zaba = zb$.

Die Konjugationsklassen in Q_8 ergeben sich zu $\{1\}$, $\{z\}$, $\{a, za\}$, $\{ab, zab\}$ und $\{b, zb\}$.

Als Repräsentanten wählen wir e.g. $g_1 := 1$, $g_2 := z$, $g_3 := a$, $g_4 := ab$ und $g_5 := b$.

Der Wedderburnisomorphismus von Aufgabe 23.(3) ergab

$$\begin{array}{rcrcl}
 & & \mathbf{C}\mathrm{Q}_8 & \xrightarrow{\ \omega\ } & (\mathbf{C} \times \mathbf{C} \times \mathbf{C} \times \mathbf{C} \times \mathbf{C}^{2\times 2}) \\
 & & \xi & \longmapsto & (\omega^1(\xi)\,,\ \omega^2(\xi)\,,\ \omega^3(\xi)\,,\ \omega^4(\xi)\,,\ \omega^5(\xi)) \\
g_1 & = & 1 & \longmapsto & (1\ ,\ 1\ ,\ 1\ ,\ 1\ ,\ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) \\
g_2 & = & z & \longmapsto & (1\ ,\ 1\ ,\ 1\ ,\ 1\ ,\ \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)) \\
g_3 & = & a & \longmapsto & (1\ ,\ 1\ ,\ -1\ ,\ -1\ ,\ \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)) \\
g_4 & = & ab & \longmapsto & (1\ ,\ -1\ ,\ -1\ ,\ 1\ ,\ \left(\begin{smallmatrix} 0 & -\mathrm{i} \\ -\mathrm{i} & 0 \end{smallmatrix}\right)) \\
g_5 & = & b & \longmapsto & (1\ ,\ -1\ ,\ 1\ ,\ -1\ ,\ \left(\begin{smallmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{smallmatrix}\right))
\end{array}$$

Spurbildung $\chi_s(g_u) = \operatorname{tr}\omega^s(g_u)$ für $s, u \in [1,4]$ führt zur Charaktertafel

$$\mathrm{X}(\mathrm{Q}_8) \;=\; \begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \\ \chi_5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & z & a & ab & b \end{array} \\ \left[\begin{array}{ccccc} 1 & 1 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ 2 & -2 & 0 & 0 & 0 \end{array}\right] \end{array},$$

wobei für spätere Zwecke direkt unter den Konjugationsklassenrepräsentanten die Länge ihrer Konjugationsklassen notiert wurde.

(4) Es fällt auf, daß $\mathrm{X}(\mathrm{D}_8) = \mathrm{X}(\mathrm{Q}_8)$ (bei geeigneter Sortierung der Charaktere und der Konjugationsklassen).

Begründen wir daher noch, daß $\mathrm{D}_8 \overset{!}{\ncong} \mathrm{Q}_8$.

In Q_8 gibt es genau 1 Element von Ordnung 2, nämlich z. Beachte hierzu insbesondere, daß wegen $b^-aba = 1$ auch $(ab)^2 = abab = b^2 = z$ ist.

In D_8 gibt es genau 5 Elemente von Ordnung 2, nämlich a^2, b, ab, a^2b und a^3b. Beachte hierzu, daß $(ab)^2 = abab = aa^- = 1$.

Also ist $\mathrm{D}_8 \ncong \mathrm{Q}_8$.

> Insbesondere ist auch $\mathbf{C}\mathrm{D}_8 \simeq \mathbf{C}^{\times 4} \times \mathbf{C}^{2\times 2} \simeq \mathbf{C}\mathrm{Q}_8$.
> Dieses Phänomen trifft man bereits bei $\mathbf{C}\mathrm{C}_4 \simeq \mathbf{C}^{\times 4} \simeq \mathbf{C}(\mathrm{C}_2 \times \mathrm{C}_2)$ an – beachte, daß wegen $\mathbf{C}\mathrm{C}_4$ und $\mathbf{C}(\mathrm{C}_2 \times \mathrm{C}_2)$ kommutativ in der jeweiligen Wedderburnzerlegung keine Matrixkantenlänge $\geqslant 2$ auftreten darf.

Aufgabe 25

Schreibe $n := \chi(1)$. Sei $\rho : G \longrightarrow \mathrm{GL}_n(\mathbf{C})$ eine zu χ gehörige Darstellung, sei also $\chi(g) = \chi_\rho(g) = \operatorname{tr}\rho(g)$. Sei $S \in \mathrm{GL}_n(\mathbf{C})$ gefunden mit $J := S\rho(g)S^{-1}$ in Jordanform. Da $\rho(g)^k = \mathrm{E}_n$ ist, ist auch $J^k = \mathrm{E}_n$. Also ist J eine Diagonalmatrix, und die Diagonaleinträge sind Nullstellen von $z^k - 1$. In anderen Worten, es ist

$$J \;=\; \begin{pmatrix} \zeta^{m_1} & & \\ & \ddots & \\ & & \zeta^{m_n} \end{pmatrix}$$

für gewisse $m_i \in [0, k-1]$ für $i \in [1, n]$.

(1) Wir erhalten

$$\chi(g) \;=\; \operatorname{tr}\rho(g) \;=\; \operatorname{tr}(SJS^{-1}) \;=\; \operatorname{tr} J \;=\; \sum_{i\in[1,n]} \zeta^{m_i} \;=\; \sum_{j\in[0,k-1]} \underbrace{|\{\, i\in[1,n] \,:\, m_i = j \,\}|}_{=:\, x_j} \cdot \zeta^j \;.$$

(2) Beachte, daß $\overline{\zeta} = \zeta^{-1}$ wegen $|\zeta| = 1$.
Wir erhalten

$$\begin{aligned}
\chi(g^{-1}) &= \operatorname{tr}\rho(g^{-1}) \\
&= \operatorname{tr} J^{-1} \\
&= \operatorname{tr}\begin{pmatrix} \zeta^{-m_1} & & \\ & \ddots & \\ & & \zeta^{-m_n} \end{pmatrix} \\
&= \textstyle\sum_{i\in[1,n]} \zeta^{-m_i} \\
&= \textstyle\sum_{i\in[1,n]} \overline{\zeta^{m_i}} \\
&= \overline{\textstyle\sum_{i\in[1,n]} \zeta^{m_i}} \\
&= \overline{\chi(g)} \;.
\end{aligned}$$

(3) Sei M ein endlichdimensionaler $\mathbf{C}G$-Modul mit $\chi = \chi_M$.
Werde der Dualraum $M^* := \operatorname{Hom}_{\mathbf{C}}(M, \mathbf{C})$ ausgestattet mit der Linksmultiplikation

$$\big(h \cdot f\big)(m) \;:=\; f(h^- m)$$

für $h \in G$, $f \in M^*$ und $m \in M$. Dies liefert eine Darstellung

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{GL}(M^*) \\ h & \longmapsto & (f \mapsto h \cdot f) \;, \end{array}$$

von G auf M^*, da sich

$$\big((h\tilde{h}) \cdot f\big)(m) \;=\; f((h\tilde{h})^- m) \;=\; f(\tilde{h}^- h^- m) \;=\; \big(\tilde{h} \cdot f\big)(h^- m) \;=\; \big(h \cdot (\tilde{h} \cdot f)\big)(m)$$

ergibt für $h, \tilde{h} \in G$, $f \in M^*$ und $m \in M$, i.e. $h\tilde{h} \longmapsto (h \cdot (-)) \circ (\tilde{h} \cdot (-))$.
Sei $(m_1 \,, \ldots \,, m_n)$ eine Basis von M. Sei $(m_1^* \,, \ldots \,, m_n^*)$ die dazu duale Basis von M^*.
Sei $h \in G$. Sei $h^- m_i = \sum_j z_{j,i}\, m_j$ für $i \in [1,n]$, wobei $z_{j,i} \in \mathbf{C}$.
Dann ist

$$(h m_k^*)(m_i) \;=\; m_k^*(h^- m_i) \;=\; \textstyle\sum_j z_{j,i}\, m_k^*(m_j) \;=\; \sum_j z_{j,i}\, \partial_{k,j} \;=\; z_{k,i} \;,$$

sowie

$$(\textstyle\sum_j z_{k,j}\, m_j^*)(m_i) \;=\; \sum_j z_{k,j}\, \partial_{j,i} \;=\; z_{k,i}$$

für $i,\, k \in [1,n]$. Dies zeigt $h m_k^* = \sum_j z_{k,j}\, m_j^*$ für $k \in [1,n]$.
Für die zugehörigen Darstellungen ist bezüglich dieser Basen also $\rho_{M^*}(h) = \rho_M(h^-)^{\mathrm{t}}$ für $h \in G$; es folgt

$$\chi_{M^*}(h) \;=\; \operatorname{tr}\rho_{M^*}(h) \;=\; \operatorname{tr}\rho_M(h^-)^{\mathrm{t}} \;=\; \chi_M(h^-) \;=\; \chi(h^-) \;\overset{(2)}{=}\; \overline{\chi(h)} \;.$$

Wir *behaupten,* daß aus χ irreduzibel folgt, daß auch $\bar{\chi}$ irreduzibel ist.
Wir müssen dazu M als einfach voraussetzen und zeigen, daß auch M^* einfach ist.
Zum einen ist $\dim_{\mathbf{C}} M^* = \dim_{\mathbf{C}} M > 0$, also $M^* \neq 0$.
Zum anderen, ist $N \subseteq M^*$ ein Teilmodul, so ist auch

$$N' \;:=\; \{\, m \in M \,:\, f(m) = 0 \text{ für } f \in N \,\} \;\subseteq\; M$$

ein Teilmodul. Denn es ist ein $\mathbf{C}$-Teilraum. Und für $n' \in N'$ und $h \in G$ ist $hn' \in N'$, da $f(hn') = (h^- f)(n') = 0$ für $f \in N$, da mit f auch $h^- f$ in N liegt. Da M einfach ist, ist $N' = 0$ oder $N' = M$.

Es ist $\dim_{\mathbf{C}} N' + \dim_{\mathbf{C}} N = \dim_{\mathbf{C}} M$, wie man mit einer Basis von N, die zu einer Basis von M^* ergänzt wird, und deren Dualbasis von M erkennt. Also ist $N = 0$ oder $N = M$.

Dies zeigt die *Behauptung.*

S. Schmid gab folgende einfache Lösung des ersten Teils von (3).

Setze $\bar{\rho}(g) := \overline{\rho(g)}$ für $g \in G$. Beobachte, daß $\chi_{\bar{\rho}} = \overline{\chi_\rho} = \bar{\chi}$ ist.

Wir wollen daher noch zeigen, daß die Moduln zu $G \to \mathrm{GL}_n(\mathbf{C})$, $g \mapsto \bar{\rho}(g)$ und zu $G \to \mathrm{GL}_n(\mathbf{C})$, $g \mapsto \rho(g^-)^{\mathrm{t}}$ isomorph sind (ohne Verwendung von Bemerkung 95.(2)).

Operiere G via ρ auf $\mathbf{C}^{n\times 1}$. Für $x,\, y \in \mathbf{C}^{n\times 1}$ sei $(x, y) := \sum_{h\in G} (hx)^{\mathrm{t}}(\overline{hy})$. Es wird so $(-,=)$ ein hermitesches Skalarprodukt, da $(x, x) = \sum_{h\in G} (hx)^{\mathrm{t}}(\overline{hx}) \in \mathbf{R}_{>0}$ für $x \in \mathbf{C}^{n\times 1} \smallsetminus \{0\}$.

Sei $(b_1, \ldots, b_n)$ eine Orthonormalbasis von $\mathbf{C}^{n\times 1}$ bezüglich $(-,=)$, erhältlich e.g. via Gram-Schmidt.

Ist $A := \sum_h \rho(h)^{\mathrm{t}}\, \overline{\rho(h)}$ die Grammatrix von $(-,=)$ bezüglich der Standardbasis von $\mathbf{C}^{n\times 1}$, so ist $\rho(g)^{\mathrm{t}} A\, \overline{\rho(g)} = A$ für $g \in G$.

Ist $B \in \mathrm{GL}_n(\mathbf{C})$ die Matrix mit Spaltentupel $(b_1, \ldots, b_n)$, so wird $B^{\mathrm{t}} A \bar{B} = \mathrm{E}_n$, also $A = (B^{\mathrm{t}})^{-1} \bar{B}^{-1}$.

Für $g \in G$ wird

$$\begin{array}{rcl} (B^{-1}\rho(g)B)^{\mathrm{t}}\, (\overline{B^{-1}\rho(g)B}) & = & B^{\mathrm{t}}\rho(g)^{\mathrm{t}}(B^{\mathrm{t}})^{-1}\bar{B}^{-1}\overline{\rho(g)}\bar{B} \\ & = & B^{\mathrm{t}}\rho(g)^{\mathrm{t}} A\, \overline{\rho(g)}\bar{B} \\ & = & B^{\mathrm{t}} A \bar{B} \\ & = & \mathrm{E}_n\ , \end{array}$$

also $G \to \mathrm{U}_n(\mathbf{C}) \leqslant \mathrm{GL}_n(\mathbf{C})$, $g \mapsto B^{-1}\rho(g)B$.

Daraus resultiert $\bar{B}^{-1}\overline{\rho(g)}\bar{B} = B^{\mathrm{t}}\rho(g^-)^{\mathrm{t}}(B^{\mathrm{t}})^{-1}$, und also

$$\overline{\rho(g)} \;=\; (\bar{B}B^{\mathrm{t}})\rho(g^-)^{\mathrm{t}}(\bar{B}B^{\mathrm{t}})^{-1}\ .$$

Somit sind die betrachteten Moduln isomorph; cf. Bemerkung 45.

Unter Verwendung von Bemerkung 94.(2) kann man übrigens problemlos auch ohne Betrachtung des Moduls folgern, daß aus χ irreduzibel folgt, daß $\bar{\chi}$ irreduzibel ist; cf. Lemma 106.

Aufgabe 26

(1) Sei $\mathbf{Z}(M \times N)$ die freie abelsche Gruppe auf der Menge $M \times N$.

Sei

$$\begin{array}{rcl} U & := & \Big\langle \begin{array}{ll} (mr, n) - (m, rn) & :\ m \in M,\ n \in N,\ r \in R \\ (m + m', n + n') - (m, n) - (m', n) - (m, n') - (m', n') & :\ m,\, m' \in M,\ n,\, n' \in N \end{array} \Big\rangle_{\mathbf{Z}} \\ & \subseteq & \mathbf{Z}(M \times N)\ . \end{array}$$

Sei

$$M \underset{R}{\otimes} N \;:=\; \mathbf{Z}(M \times N)/U\ .$$

Werde die Restklasse eines Erzeugers (m, n) in $M \underset{R}{\otimes} N$ mit $m \otimes n := (m, n) + U$ bezeichnet, und sei

$$\begin{array}{ccccc} M & \times & N & \xrightarrow{\ b\ } & M \underset{R}{\otimes} N \\ (m & , & n) & \longmapsto & m \otimes n\ . \end{array}$$

die Restklassenabbildung. Nach Konstruktion ist b eine R-bilineare Abbildung.

Unter $m \otimes n$ darf man sich ein "noch nicht ausgewertetes Skalarprodukt" von m und n vorstellen.

Wir wollen eine R-bilineare Abbildung $M \times N \xrightarrow{f} A$ in eine abelsche Gruppe A auf eindeutige Weise über b und eine $\mathbf{Z}$-lineare Abbildung $M \underset{R}{\otimes} N \xrightarrow{\tilde{f}} A$ faktorisieren.

Zur Eindeutigkeit der Faktorisierung. Das Bild von b enthält ein $\mathbf{Z}$-lineares Erzeugendensystem von $M \underset{R}{\otimes} N$, was die Eindeutigkeit der $\mathbf{Z}$-linearen Faktorisierung $M \underset{R}{\otimes} N \xrightarrow{\tilde{f}} A$ einer bilinearen Abbildung $M \times N \xrightarrow{f} A$ in eine abelsche Gruppe A sichert.

Zur Existenz der Faktorisierung. Zunächst können wir zur $\mathbf{Z}$-linearen Abbildung

$$\begin{array}{rcl} \mathbf{Z}(M \times N) & \xrightarrow{\hat{f}} & A \\ \sum_{(m,n)} z_{(m,n)}(m,n) & \longmapsto & \sum_{(m,n)} z_{(m,n)} f((m,n)) \end{array}$$

fortsetzen, wobei $z_{(m,n)} \in \mathbf{Z}$ für $(m,n) \in M \times N$.

Nun heißt R-Bilinearität von f gerade, daß $\hat{f}(U) = 0$ ist. Also gibt es die $\mathbf{Z}$-lineare Abbildung

$$\begin{array}{rcccl} M & \underset{R}{\otimes} & N & = \mathbf{Z}(M \times N)/U & \xrightarrow{\tilde{f}} & A \\ & & & \xi + U & \longmapsto & \hat{f}(\xi) \\ m & \otimes & n & = (m,n) + U & \longmapsto & \hat{f}((m,n)) = f((m,n)) \end{array}$$

Da diese $m \otimes n$ nach $f((m,n))$ abbildet für $(m,n) \in M \times N$, ist in der Tat $f = \tilde{f} \circ b$.

> Diese universelle Eigenschaft von $M \underset{R}{\otimes} N$ wird folgendermaßen zur Konstruktion von $\mathbf{Z}$-linearen Abbildungen aus dem Tensorprodukt verwandt. Es ist
>
> $$\begin{array}{rcccl} M & \underset{R}{\otimes} & N & \xrightarrow{g} & A \\ m & \otimes & n & \longmapsto & g(m,n) \\ \sum_{(m,n)\in M\times N} z_{(m,n)}\, m & \otimes & n & \longmapsto & \sum_{(m,n)\in M\times N} z_{(m,n)}\, g(m,n) \end{array} \qquad \text{(wobei } z_{(m,n)} \in \mathbf{Z} \text{ für } (m,n) \in M \times N\text{)}$$
>
> wohldefiniert und $\mathbf{Z}$-linear, falls g additiv in m und n ist, und falls stets $g(mr,n) = g(m,rn)$ ist. Man "kennt" das Tensorprodukt weniger über die Elemente, die es enthält – $\mathbf{Z}$-Linearkombinationen von *Elementartensoren* der Form $m \otimes n$ – als über diese Eigenschaft. Will man z.B. wissen, daß $m \otimes n \neq m' \otimes n'$, so empfiehlt es sich, eine Abbildung aus dem Tensorprodukt heraus anzugeben, für die sich die *Bilder* dieser beiden Elementartensoren unterscheiden.

(2) Für $s \in S$ ist die Abbildung

$$\begin{array}{ccccc} M & \underset{R}{\otimes} & N & \xrightarrow{(-)s} & M & \underset{R}{\otimes} & N \\ m & \otimes & n & \longmapsto & (sm) & \otimes & n \end{array}$$

wohldefiniert und $\mathbf{Z}$-linear, da

$$\begin{array}{rcl} (s(m+m')) \otimes (n+n') & = & (sm+sm') \otimes (n+n') \\ & = & (sm) \otimes n + (sm') \otimes n + (sm) \otimes n' + (sm') \otimes n' \\ (s(mr)) \otimes n & = & (sm)r \otimes n \\ & = & (sm) \otimes rn\ . \end{array}$$

für $m,\, m' \in M$, $n,\, n' \in N$ und $r \in R$.

Wir können also in wohldefinierter Weise

$$s \cdot \left(\sum_{(m,n)} z_{(m,n)}\, m \otimes n\right) := \sum_{(m,n)} z_{(m,n)} (sm) \otimes n$$

setzen, wobei $s \in S$ und $z_{(m,n)} \in \mathbf{Z}$ für $(m,n) \in M \times N$. Insbesondere wird $s \cdot (m \otimes n) = (sm) \otimes n$ für $s \in S$ und $(m,n) \in M \times N$.

Es operiert 1_S identisch, da

$$1_S \cdot (\sum_{(m,n)}\ z_{(m,n)}\, m \otimes n) \ = \ \sum_{(m,n)}\ z_{(m,n)}\, (1_S \cdot m) \otimes n \ = \ \sum_{(m,n)}\ z_{(m,n)}\, m \otimes n\ ,$$

wobei $z_{(m,n)} \in \mathbf{Z}$ für $(m,n) \in M \times N$.
Die Operation ist assoziativ, da

$$\begin{array}{rcl} (ss')(\sum_{(m,n)}\ z_{(m,n)}\, m \otimes n) & = & \sum_{(m,n)}\ z_{(m,n)}\, ((ss')m) \otimes n \\ & = & \sum_{(m,n)}\ z_{(m,n)}\, (s(s'm)) \otimes n \\ & = & s(\sum_{(m,n)}\ z_{(m,n)}\, (s'm) \otimes n) \\ & = & s(s'(\sum_{(m,n)}\ z_{(m,n)}\, m \otimes n))\ , \end{array}$$

wobei $s,\ s' \in S$ und $z_{(m,n)} \in \mathbf{Z}$ für $(m,n) \in M \times N$.
Die Operation ist distributiv, da

$$\begin{array}{rcl} & & (s+s')((\sum_{(m,n)}\ z_{(m,n)}\, m \otimes n) + (\sum_{(m,n)}\ z'_{(m,n)}\, m \otimes n)) \\ & = & (s+s')(\sum_{(m,n)}\ (z_{(m,n)} + z'_{(m,n)})\, m \otimes n) \\ & = & \sum_{(m,n)}\ (z_{(m,n)} + z'_{(m,n)})\, ((s+s')m) \otimes n \\ & = & \sum_{(m,n)}\ (z_{(m,n)} + z'_{(m,n)})\, (sm + s'm) \otimes n \\ & = & \sum_{(m,n)}\ (z_{(m,n)} + z'_{(m,n)})\, ((sm) \otimes n + (s'm) \otimes n) \\ & = & (\sum_{(m,n)}\ z_{(m,n)}\, (sm) \otimes n) + (\sum_{(m,n)}\ z'_{(m,n)}\, (sm) \otimes n) \\ & + & (\sum_{(m,n)}\ z_{(m,n)}\, (s'm) \otimes n) + (\sum_{(m,n)}\ z'_{(m,n)}\, (s'm) \otimes n) \\ & = & s(\sum_{(m,n)}\ z_{(m,n)}\, m \otimes n) + s(\sum_{(m,n)}\ z'_{(m,n)})\, m \otimes n) \\ & + & s'(\sum_{(m,n)}\ z_{(m,n)}\, m \otimes n) + s'(\sum_{(m,n)}\ z'_{(m,n)}\, m \otimes n)\ , \end{array}$$

wobei $s,\ s' \in S$ und $z_{(m,n)},\ z'_{(m,n)} \in \mathbf{Z}$ für $(m,n) \in M \times N$.
Usf., i.e. für eine Rechtsmodulstruktur auf einem Tensorprodukt aus einem Rechtsmodul und einem Bimodul analog.

(3) Hierzu haben wir $R = {}_RR_R$ als R-R-Bimodul anzusehen.
Die Abbildung

$$\begin{array}{ccccc} R & \underset{R}{\otimes} & N & \xrightarrow{\ f\ } & N \\ r & \otimes & n & \longmapsto & rn \end{array}$$

ist wohldefiniert und $\mathbf{Z}$-linear, da

$$\begin{array}{l} (rr')n \ = \ r(r'n) \\ (r+r')(n+n') \ = \ rn + r'n + rn' + r'n' \end{array}$$

für $r,\ r' \in R$ und $n,\ n' \in N$.
Es ist f auch R-linear, da

$$\begin{array}{rcl} f(r'(\sum_{(r,n)}\ z_{(r,n)}\, r \otimes n)) & = & f(\sum_{(r,n)}\ z_{(r,n)}\, (r'r) \otimes n)) \\ & = & \sum_{(r,n)}\ z_{(r,n)}\, (r'r)n \\ & = & r'(\sum_{(r,n)}\ z_{(r,n)}\, rn) \\ & = & r'f(\sum_{(r,n)}\ z_{(r,n)}\, r \otimes n)\ , \end{array}$$

wobei $r' \in R$ und $z_{(r,n)} \in \mathbf{Z}$ für $(r,n) \in R \times N$.

Betrachten wir ferner die $\mathbf{Z}$-lineare Abbildung

$$\begin{array}{ccccc} N & \xrightarrow{g} & R & \underset{R}{\otimes} & N \\ n & \longmapsto & 1 & \otimes & n\,. \end{array}$$

Es ist $(f \circ g)(n) = f(1 \otimes n) = 1 \cdot n = n$ für $n \in N$, also $f \circ g = \mathrm{id}_N$.
Es ist $(g \circ f)(r \otimes n) = g(rn) = 1 \otimes rn = r \otimes n$ für $r \in R$ und $n \in N$, also $g \circ f = \mathrm{id}_{R \underset{R}{\otimes} N}$.

Also ist f bijektiv und $g = f^-$. Es folgt, daß $R \underset{R}{\otimes} N \simeq N$ als R-Moduln.

(4) Wir müssen zeigen, daß

$$\begin{array}{ccccccccccc} (M & \underset{R}{\otimes} & N) & \underset{T}{\otimes} & P & \xrightarrow{f} & M & \underset{R}{\otimes} & (N & \underset{T}{\otimes} & P) \\ (m & \otimes & n) & \otimes & p & \longmapsto & m & \otimes & (n & \otimes & p) \end{array}$$

wohldefiniert und S-linear ist.

Mit einem analogen Argument sieht man dann, daß auch die Abbildung in die Rückichtung $(m \otimes n) \otimes p \longmapsto m \otimes (n \otimes p)$ wohldefiniert ist; diese beiden Abbildungen invertieren sich dann in beiden Richtungen.

Zur verlangten Wohldefiniertheit. Wir definieren zunächst eine Abbildung

$$\begin{array}{ccccccccccc} (M & \underset{R}{\otimes} & N) & \times & P & \xrightarrow{h} & M & \underset{R}{\otimes} & (N & \underset{T}{\otimes} & P) \\ (m & \otimes & n & , & p) & \longmapsto & m & \otimes & (n & \otimes & p)\,. \end{array}$$

Sei $p \in P$ fixiert. Dann ist

$$\begin{array}{ccccccccc} M & \underset{R}{\otimes} & N & \xrightarrow{h_p} & M & \underset{R}{\otimes} & (N & \underset{T}{\otimes} & P) \\ m & \otimes & n & \longmapsto & m & \otimes & (n & \otimes & p)\,. \end{array}$$

wohldefiniert und $\mathbf{Z}$-linear, da für $r \in R$, m, $m' \in M$ und n, $n' \in N$ gilt, daß

$$\begin{aligned} mr \otimes (n \otimes p) &= m \otimes r(n \otimes p) \\ &= m \otimes (rn \otimes p) \\ (m + m') \otimes ((n + n') \otimes p) &= (m + m') \otimes (n \otimes p + n' \otimes p) \\ &= m \otimes (n \otimes p) + m' \otimes (n \otimes p) + m \otimes (n' \otimes p) + m' \otimes (n' \otimes p)\,. \end{aligned}$$

Setze nun

$$h(\textstyle\sum_{(m,n)} z_{(m,n)}\, m \otimes n,\, p) \;:=\; h_p(\sum_{(m,n)} z_{(m,n)}\, m \otimes n) \;=\; \sum_{(m,n)} z_{(m,n)}\, m \otimes (n \otimes p)\,,$$

wobei $z_{(m,n)} \in \mathbf{Z}$ für $(m, n) \in M \times N$ und $p \in P$.

Um die Wohldefiniertheit und $\mathbf{Z}$-Linearität von f zu erhalten, ist zu zeigen, daß h eine T-bilineare Abbildung ist.

In der Tat wird

$$\begin{aligned} h((\textstyle\sum_{(m,n)} z_{(m,n)}\, m \otimes n)t,\, p) &= h(\sum_{(m,n)} z_{(m,n)}\, m \otimes (nt),\, p) \\ &= \textstyle\sum_{(m,n)} z_{(m,n)}\, m \otimes ((nt) \otimes p) \\ &= \textstyle\sum_{(m,n)} z_{(m,n)}\, m \otimes (n \otimes tp) \\ &= h(\textstyle\sum_{(m,n)} z_{(m,n)}\, m \otimes n,\, tp)\,, \end{aligned}$$

wobei $t \in T$, $z_{(m,n)} \in \mathbf{Z}$ für $(m,n) \in M \times N$ und $p \in P$ ist, und

$$\begin{aligned}
& h((\textstyle\sum_{(m,n)}\ z_{(m,n)}\, m \otimes n) + (\sum_{(m,n)}\ z'_{(m,n)}\, m \otimes n),\ p + p') \\
= \ & h(\textstyle\sum_{(m,n)} (z_{(m,n)} + z'_{(m,n)})\, m \otimes n,\ p + p') \\
= \ & \textstyle\sum_{(m,n)} (z_{(m,n)} + z'_{(m,n)})\, m \otimes (n \otimes (p + p')) \\
= \ & \textstyle\sum_{(m,n)} (z_{(m,n)} + z'_{(m,n)})\, m \otimes (n \otimes p + n \otimes p') \\
= \ & \textstyle\sum_{(m,n)} (z_{(m,n)} + z'_{(m,n)})\, (m \otimes (n \otimes p) + m \otimes (n \otimes p')) \\
= \ & (\textstyle\sum_{(m,n)}\ z_{(m,n)}\, m \otimes (n \otimes p)) + (\sum_{(m,n)}\ z'_{(m,n)}\, m \otimes (n \otimes p)) \\
+ \ & (\textstyle\sum_{(m,n)}\ z_{(m,n)}\, m \otimes (n \otimes p')) + (\sum_{(m,n)}\ z'_{(m,n)}\, m \otimes (n \otimes p')) \\
= \ & h(\textstyle\sum_{(m,n)}\ z_{(m,n)}\, m \otimes n,\ p) + h(\sum_{(m,n)}\ z'_{(m,n)}\, m \otimes n,\ p) \\
+ \ & h(\textstyle\sum_{(m,n)}\ z_{(m,n)}\, m \otimes n,\ p') + h(\sum_{(m,n)}\ z'_{(m,n)}\, m \otimes n,\ p')\ ,
\end{aligned}$$

wobei $z_{(m,n)}\,,\ z'_{(m,n)} \in \mathbf{Z}$ für $(m,n) \in M \times N$ und $p,\ p' \in P$ ist.
Es bleibt die S-Linearität von f zu verifizieren. Es wird

$$\begin{aligned}
f(s(\textstyle\sum_{(m,n,p)}\ z_{(m,n,p)}\, (m \otimes n) \otimes p)) &= f(\textstyle\sum_{(m,n,p)}\ z_{(m,n,p)}\, (s(m \otimes n)) \otimes p) \\
&= f(\textstyle\sum_{(m,n,p)}\ z_{(m,n,p)}\, ((sm) \otimes n) \otimes p) \\
&= \textstyle\sum_{(m,n,p)}\ z_{(m,n,p)}\, (sm) \otimes (n \otimes p) \\
&= s(\textstyle\sum_{(m,n,p)}\ z_{(m,n,p)}\, m \otimes (n \otimes p)) \\
&= s(f(\textstyle\sum_{(m,n,p)}\ z_{(m,n,p)}\, (m \otimes n) \otimes p))\ ,
\end{aligned}$$

wobei $s \in S$ und $z_{(m,n,p)} \in \mathbf{Z}$ für $(m,n,p) \in M \times N \times P$ ist.

(5) Für eine R-lineare Abbildung ${}_RX \xrightarrow{f} {}_RY$ zwischen R-Linksmoduln definieren wir

$$\begin{array}{ccccc}
M & \underset{R}{\otimes} & X & \xrightarrow{M \underset{R}{\otimes} f} & M & \underset{R}{\otimes} & Y \\
m & \otimes & x & \longmapsto & m & \otimes & f(x)\ .
\end{array}$$

Dies ist wohldefiniert und $\mathbf{Z}$-linear, da

$$\begin{aligned}
& mr \otimes f(x) \ = \ m \otimes rf(x) \ = \ m \otimes f(rx) \\
& (m + m') \otimes f(x + x') \ = \ (m + m') \otimes (f(x) + f(x')) \ = \ m \otimes f(x) + m' \otimes f(x) + m \otimes f(x') + m' \otimes f(x')
\end{aligned}$$

ist für $r \in R$, $m,\ m' \in N$ und $x,\ x' \in X$.
Dies ist auch S-linear, denn für $\mathbf{Z}$-lineare Erzeuger ergibt sich

$$(M \underset{R}{\otimes} f)(s(m \otimes x)) \ = \ (M \underset{R}{\otimes} f)((sm) \otimes x) \ = \ (sm) \otimes f(x) \ = \ s(m \otimes f(x)) \ = \ s(M \underset{R}{\otimes} f)(m \otimes x)\ ,$$

wobei $s \in S$, $m \in M$ und $x \in X$.

Beachte, daß für R-lineare Abbildungen ${}_RX \underset{f'}{\overset{f}{\rightrightarrows}} {}_RY \xrightarrow{g} {}_RZ$ gilt, daß

$$\begin{aligned}
M \underset{R}{\otimes} (f + f') &= (M \underset{R}{\otimes} f) + (M \underset{R}{\otimes} f') \\
M \underset{R}{\otimes} (g \circ f) &= (M \underset{R}{\otimes} g) \circ (M \underset{R}{\otimes} f) \\
M \underset{R}{\otimes} \mathrm{id}_X &= \mathrm{id}_{M \underset{R}{\otimes} X}\ .
\end{aligned}$$

Nun zur Verträglichkeit der Operation $M \underset{R}{\otimes} -$ mit direkten Summen.

Wir haben die folgenden R-linearen Abbildungen.

$$\begin{array}{rcl} N & \stackrel{\iota}{\longrightarrow} & N \oplus N' \\ n & \longrightarrow & (n,0) \\ N' & \stackrel{\iota'}{\longrightarrow} & N \oplus N' \\ n' & \longrightarrow & (0,n') \\ N \oplus N' & \stackrel{\pi}{\longrightarrow} & N \\ (n,n') & \longmapsto & n \\ N \oplus N' & \stackrel{\pi'}{\longrightarrow} & N' \\ (n,n') & \longmapsto & n' \end{array}$$

Wir wollen zeigen, daß sich

$$\begin{array}{rcl} (M \underset{R}{\otimes} N) \oplus (M \underset{R}{\otimes} N') & \stackrel{\alpha}{\longrightarrow} & M \underset{R}{\otimes} (N \oplus N') \\ (\xi, \xi') & \longmapsto & (M \underset{R}{\otimes} \iota)(\xi) + (M \underset{R}{\otimes} \iota')(\xi') \\ (M \underset{R}{\otimes} N) \oplus (M \underset{R}{\otimes} N') & \stackrel{\beta}{\longleftarrow} & M \underset{R}{\otimes} (N \oplus N') \\ ((M \underset{R}{\otimes} \pi)(\eta), (M \underset{R}{\otimes} \pi')(\eta)) & \longmapsfrom & \eta \end{array}$$

gegenseitig invertieren. Es genügt, dies auf $\mathbf{Z}$-linearen Erzeugern zu verifizieren.

Zum einen wird

$$\begin{array}{rcl} (m \otimes n, 0) & \stackrel{\alpha}{\longmapsto} & m \otimes \iota(n) + m \otimes \iota'(0) \\ & = & m \otimes (n,0) \\ & \stackrel{\beta}{\longmapsto} & (m \otimes \pi(n,0), m \otimes \pi'(n,0)) \\ & = & (m \otimes n, 0)\ , \end{array}$$

wobei $m \in M$ und $n \in N$. Analog in zweiter Komponente.

Zum anderen wird

$$\begin{array}{rcl} m \otimes (n,n') & \stackrel{\beta}{\longmapsto} & (m \otimes \pi(n,n'), m \otimes \pi'(n,n')) \\ & = & (m \otimes n,\ m \otimes n') \\ & \stackrel{\alpha}{\longmapsto} & m \otimes \iota(n) + m \otimes \iota'(n') \\ & = & m \otimes (n,0) + m \otimes (0,n') \\ & = & m \otimes (n,n')\ , \end{array}$$

wobei $m \in M$ und $n,\ n' \in N'$.

Usf., i.e. auch im vorderen Tensorfaktor hat man diese Verträglichkeit mit der direkten Summe.

(6) Sei etwa $R = \mathbf{F}_5$, $M = {}_{\mathbf{F}_5}\mathbf{F}_5^{\oplus 3}{}_{\mathbf{F}_5}$ und $N = {}_{\mathbf{F}_5}\mathbf{F}_5^{\oplus 3}$.

Es ist $|M \times N| = |M||N| = 5^3 \cdot 5^3 = 5^6$.

Es ist

$$M \underset{R}{\otimes} N \ = \ \mathbf{F}_5^{\oplus 3} \underset{\mathbf{F}_5}{\otimes} \mathbf{F}_5^{\oplus 3} \ \overset{(5)}{\simeq}\ (\mathbf{F}_5 \underset{\mathbf{F}_5}{\otimes} \mathbf{F}_5^{\oplus 3})^{\oplus 3} \ \overset{(3)}{\simeq}\ (\mathbf{F}_5^{\oplus 3})^{\oplus 3} \ \simeq\ \mathbf{F}_5^{\oplus 9}\ .$$

Insbesondere ist $|M \underset{R}{\otimes} N| = 5^9$.

Somit kann $b : M \times N \longrightarrow M \underset{R}{\otimes} N$ nicht surjektiv sein.

Aufgabe 27

Sei $(a,b) \in A \times B$.

Es ist $(a,b) \in \mathrm{Z}(A \times B)$ genau dann, wenn $(a,b)(x,y) = (x,y)(a,b)$ für alle $(x,y) \in A \times B$, i.e. wenn $(ax,by) = (xa,yb)$ für alle $(x,y) \in A \times B$, i.e. wenn $ax = xa$ für alle $x \in A$ und $by = yb$ für alle $y \in B$, i.e. wenn $a \in \mathrm{Z}(A)$ und $b \in \mathrm{Z}(B)$.

Cf. Lemma 84.

Aufgabe 28

Annahme, es gibt einen Isomorphismus $f : B\mathrm{e}_{1,1}^r \xrightarrow{\sim} B\mathrm{e}_{1,1}^s$ von B-Moduln. Es ist $\mathrm{e}_{1,1}^r \neq 0$. Andererseits ist

$$f(\mathrm{e}_{1,1}^r) \;=\; f(\mathrm{e}_{1,1}^r \mathrm{e}_{1,1}^r) \;=\; \mathrm{e}_{1,1}^r \underbrace{f(\mathrm{e}_{1,1}^r)}_{\in B\mathrm{e}_{1,1}^s} \;=\; 0\,,$$

da $r \neq s$. Wir haben einen *Widerspruch.*

Aufgabe 29

(1) Sei $r \in \mathbf{Z}_{\geqslant 0}$ und seien $a_i \in A$ für $i \in [1,r]$ so gewählt, daß $A = {}_{\mathbf{Z}}\langle a_1\,,\ldots,a_r\rangle$.

Wir haben die surjektive $\mathbf{Z}$-lineare Abbildung $f := \mathbf{Z}^{\oplus r} \to A$, $(\lambda_i)_i \mapsto \sum_i \lambda_i a_i$.

Da mit f auch $f|^B_{f^{-1}(B)} : f^{-1}(B) \to B$ surjektiv ist, genügt es zu zeigen, daß $f^{-1}(B)$ von $\leqslant r$ Elementen erzeugt ist.

Somit dürfen wir annehmen, daß $A = \mathbf{Z}^{\oplus r}$.

Induktion über $r \geqslant 0$. Klar für $r = 0$.

Sei $r \geqslant 1$. Sei die Aussage bekannt für $r-1$. Betrachte $\pi : \mathbf{Z}^{\oplus r} \to \mathbf{Z}$, $(z_i)_i \mapsto z_r$.

Es ist $\pi(B) = m\mathbf{Z}$ für ein $m \in \mathbf{Z}$, da in $\mathbf{Z}$ jedes Ideal von einem Element erzeugt wird ($\mathbf{Z}$ ist Hauptidealbereich).

Es ist $\operatorname{Kern}\pi \simeq \mathbf{Z}^{\oplus(r-1)}$. Nach Induktionsvoraussetzung ist jede Untergruppe von $\operatorname{Kern}\pi$ von $\leqslant r-1$ Elementen erzeugt. Insbesondere ist also $\operatorname{Kern}(\pi|^{\pi(B)}_B) = (\operatorname{Kern}\pi) \cap B \subseteq \operatorname{Kern}\pi$ von $\leqslant r-1$ Elementen erzeugt.

Es bleibt also folgende Aussage zu zeigen.

Sei $u : X \to Y$ eine surjektive $\mathbf{Z}$-lineare Abbildung zwischen abelschen Gruppen. Sei Y von ℓ Elementen erzeugt für ein $\ell \in \mathbf{Z}_{\geqslant 0}$. Sei $\operatorname{Kern} u$ von k Elementen erzeugt für ein $k \in \mathbf{Z}_{\geqslant 0}$. Dann, so müssen wir zeigen, ist X von $k+\ell$ Elementen erzeugt.

Sei $Y = {}_{\mathbf{Z}}\langle y_1\,,\ldots,y_\ell\rangle$ mit $y_i \in Y$ für $i \in [1,\ell]$.

Wähle $x_i \in X$ mit $u(x_i) = y_i$ für $i \in [1,\ell]$.

Sei $\operatorname{Kern} u = {}_{\mathbf{Z}}\langle x_{\ell+1}\,,\ldots,x_{\ell+k}\rangle$ mit $x_i \in X$ für $i \in [\ell+1,\ell+k]$.

Wir *behaupten,* daß $X = {}_{\mathbf{Z}}\langle x_1\,,\ldots,x_{k+\ell}\rangle$.

Sei $x \in X$ gegeben. Schreibe $u(x) = \sum_{i\in[1,\ell]} \lambda_i\, y_i$ mit $\lambda_i \in \mathbf{Z}$ für $i \in [1,\ell]$ geeignet.

Es wird $u(x - \sum_{i\in[1,\ell]} \lambda_i\, x_i) = u(x) - \sum_{i\in[1,\ell]} \lambda_i\, u(x_i) = u(x) - \sum_{i\in[1,\ell]} \lambda_i\, y_i = 0$.

Schreibe $x - \sum_{i\in[1,\ell]} \lambda_i\, x_i = \sum_{i\in[\ell+1,\ell+k]} \lambda_i\, x_i$ mit $\lambda_i \in \mathbf{Z}$ für $i \in [\ell+1,\ell+k]$ geeignet.

Es wird $x = (\sum_{i\in[1,\ell]} \lambda_i\, x_i) + (\sum_{i\in[\ell+1,\ell+k]} \lambda_i\, x_i) = \sum_{i\in[1,\ell+k]} \lambda_i\, x_i$.

Dies zeigt die *Behauptung.*

(2) Es ist $1 \in \mathbf{Z} \subseteq \mathcal{O}$.

Seien z, $w \in \mathcal{O}$ gegeben.

Sei $f(X) = \sum_{i\in[0,m]} a_i X^i \in \mathbf{Z}[X]$ mit $a_m = 1$ und $f(z) = 0$. Insbesondere ist $z^m \in {}_{\mathbf{Z}}\langle z^0, \ldots, z^{m-1}\rangle$.

Sei $g(X) = \sum_{i\in[0,n]} b_i X^i \in \mathbf{Z}[X]$ mit $b_n = 1$ und $g(w) = 0$. Insbesondere ist $w^n \in {}_{\mathbf{Z}}\langle w^0, \ldots, w^{n-1}\rangle$.

Beachte, daß m, $n \geqslant 1$ ist.

Sei $\mathbf{Z}[z,w] := \{\, u(z,w) \,:\, u(X,Y) \in \mathbf{Z}[X,Y] \,\} \subseteq \mathbf{C}$.

Es ist $\mathbf{Z}[z,w]$ ein Teilring von $\mathbf{C}$, als Bild des Ringmorphismus $\mathbf{Z}[X,Y] \to \mathbf{C}$, $X \mapsto z$, $Y \mapsto w$.

Insbesondere sind $z - w$, $zw \in \mathbf{Z}[z,w]$. Also genügt es zu zeigen, daß $\mathbf{Z}[z,w] \overset{!}{\subseteq} \mathcal{O}$.

Wir *behaupten,* daß $\mathbf{Z}[z,w] \overset{!}{=} {}_{\mathbf{Z}}\langle\, z^i w^j \,:\, i \in [0,m-1],\ j \in [0,n-1] \,\rangle$ ist.

Sei $\ell \in \mathbf{Z}_{\geqslant 0}$ gegeben. Wir wollen zeigen, daß $w^\ell \overset{!}{\in} {}_{\mathbf{Z}}\langle\, w^j \,:\, j \in [0,n-1]\rangle$ ist.

Induktion nach $\ell \geqslant 0$.

Falls $\ell < n$ ist, so ist nichts zu zeigen.

Falls $\ell \geqslant n$ ist, so folgt aus $w^n \in {}_{\mathbf{Z}}\langle w^0, \ldots, w^{n-1}\rangle$, daß

$$w^\ell \ \in\ {}_{\mathbf{Z}}\langle w^{\ell-n}, \ldots, w^{\ell-1}\rangle \ \overset{\text{I.V.}}{\subseteq}\ {}_{\mathbf{Z}}\langle\, w^j \,:\, j \in [0,n-1]\rangle\ .$$

ist.

Seien k, $\ell \in \mathbf{Z}_{\geqslant 0}$ gegeben. Wir haben zu zeigen, daß

$$z^k w^\ell \ \overset{!}{\in}\ {}_{\mathbf{Z}}\langle\, z^i w^j \,:\, i \in [0,m-1],\ j \in [0,n-1]\rangle$$

ist.

Nach voriger Aussage dürfen wir $\ell \in [0,n-1]$ annehmen.

Wir führen nun eine Induktion nach $k \geqslant 0$.

Falls $k < m$ ist, so ist nichts zu zeigen.

Falls $k \geqslant m$ ist, so folgt aus $z^m \in {}_{\mathbf{Z}}\langle z^0, \ldots, z^{m-1}\rangle$, daß

$$z^k w^\ell \ \in\ {}_{\mathbf{Z}}\langle z^{k-m} w^\ell, \ldots, z^{k-1} w^\ell\rangle \ \overset{\text{I.V.}}{\subseteq}\ {}_{\mathbf{Z}}\langle\, z^i w^j \,:\, i \in [0,m-1],\ j \in [0,n-1]\rangle$$

ist. Dies zeigt die *Behauptung.*

Sei nun $\xi \in \mathbf{Z}[z,w]$ gegeben. Es ist $\mathbf{Z}[\xi] := \{\, f(\xi) \,:\, f(X) \in \mathbf{Z}[X] \,\} \subseteq \mathbf{Z}[z,w]$ nach (1) und der eben gezeigten Behauptung eine endlich erzeugte abelsche Gruppe. Also hat die Kette

$$\mathbf{z}\langle\xi^0\rangle \ \subseteq\ \mathbf{z}\langle\xi^0, \xi^1\rangle \ \subseteq\ \mathbf{z}\langle\xi^0, \xi^1, \xi^2\rangle \ \subseteq\ \cdots\ ,$$

deren Vereinigung ganz $\mathbf{Z}[\xi]$ ist, spätestens ab dann nur noch Glieder gleich $\mathbf{Z}[\xi]$, wenn alle gewählten Erzeuger von $\mathbf{Z}[\xi]$ im betrachteten Kettenglied enthalten sind.

Insbesondere gibt es ein $k \in \mathbf{Z}_{\geqslant 1}$ mit $\xi^k \in {}_{\mathbf{Z}}\langle\xi^0, \ldots, \xi^{k-1}\rangle$.

Dann aber gibt es $\lambda_i \in \mathbf{Z}$ für $i \in [0,k-1]$ mit $\xi^k = \sum_{i\in[0,k-1]} \lambda_i\, \xi^i$. Folglich ist $\xi \in \mathcal{O}$.

Alternativ, ist $\mathbf{Z}[\xi]$ als endlich erzeugte abelsche Gruppe bekannt, so können wird $\mathbf{Z}[\xi] = \mathbf{z}\langle h_1(\xi), \ldots, h_v(\xi)\rangle$ schreiben, wobei $v \in \mathbf{Z}_{\geqslant 0}$ und $h_i(X) \in \mathbf{Z}[X]$ für $i \in [1,v]$. Sei $M := \max\{\, \deg h_i \,:\, i \in [1,v] \,\}$. Es ist $\xi^{M+1} = \sum_{i\in[1,v]} c_i h_i(\xi)$ für gewisse $c_i \in \mathbf{Z}$ für $i \in [1,v]$. Da $H(X) := X^{M+1} - \sum_{i\in[1,v]} c_i h_i(X) \in \mathbf{Z}[X]$ normiert ist und $H(\xi) = 0$ ist, folgt $\xi \in \mathcal{O}$.

(3) Sei $q \in \mathbf{Q}$ gegeben mit $f(q) = 0$ für $f(X) = \sum_{i\in[0,m]} \lambda_i X^i \in \mathbf{Z}[X]$, wobei $m \in \mathbf{Z}_{\geqslant 1}$ und $\lambda_m = 1$.

Wir haben zu zeigen, daß $q \stackrel{!}{\in} \mathbf{Z}$.

Annahme, nicht. Schreibe $q = \frac{a}{b}$ mit $a, b \in \mathbf{Z} \setminus \{0\}$ teilerfremd, und mit $b \notin \{-1, +1\}$.

Aus

$$\sum_{i\in[0,m]} \lambda_i \, (\tfrac{a}{b})^i \;=\; 0$$

folgt

$$0 \;=\; \sum_{i\in[0,m]} \lambda_i a^i b^{m-i} \;\equiv_b\; \lambda_m a^m \;=\; a^m \;\not\equiv_b\; 0\,,$$

und wir haben einen *Widerspruch.*

Aufgabe 30

Schreibe $n := \chi(1)$.

Zu zeigen ist $\operatorname{Kern}\rho \stackrel{!}{=} \{\, g \in G \,:\, \chi(g) = n \,\}$.

Sei $g \in G$.

Zu $\stackrel{!}{\subseteq}$. Ist $\rho(g) = \mathrm{id}_V$, so ist $\chi(g) = \chi_\rho(g) = \operatorname{tr}\rho(g) = \operatorname{tr}\mathrm{id}_V = \dim_{\mathbf{C}} V = n$.

Zu $\stackrel{!}{\supseteq}$. Schreibe $k := |\langle g\rangle|$ und $\zeta := \zeta_k$.

Es ist $\chi(g) = \sum_{j\in[0,k-1]} x_j\,\zeta^j$ mit $x_j \in \mathbf{Z}_{\geqslant 0}$ so, daß $\sum_{j\in[0,k-1]} x_j = n$, wobei ζ^k ein Eigenwert von $\rho(g)$ von (algebraischer wie geometrischer) Multiplizität x_j ist, wobei Multiplizität 0 heiße, daß ζ^k kein Eigenwert ist. Cf. Aufgabe 25.(1) und Lösung dazu.

Es ist $\operatorname{Re}(\zeta^j) = \cos(2\pi j/k) < 1$ für $j \in [1, k-1]$.

Ist $\chi(g) = n$, dann ist

$$x_0 + \sum_{j\in[1,k-1]} x_j \;=\; n \;=\; \operatorname{Re} n \;=\; \operatorname{Re}\chi(g) \;=\; \operatorname{Re}(\sum_{j\in[0,k-1]} x_j\,\zeta^j) \;=\; x_0 + \sum_{j\in[1,k-1]} x_j \operatorname{Re}(\zeta^j)\,,$$

also

$$0 \;=\; \sum_{j\in[1,k-1]} x_j(1 - \operatorname{Re}(\zeta^j))\,.$$

Da darin stets $x_j \geqslant 0$ und $(1 - \operatorname{Re}\zeta^j) > 0$ ist, folgt, daß $x_j = 0$ für $j \in [1, k-1]$ und also $x_0 = n$ ist.

Somit ist 1 der einzige Eigenwert von $\rho(g)$. Da $\rho(g)$ diagonalisierbar ist, folgt $\rho(g) = \mathrm{id}_V$, i.e. $g \in \operatorname{Kern}\rho$; cf. Lösung zu Aufgabe 25.(1).

Aufgabe 31

Vorbemerkung. Sei C eine R-Algebra. Seien ${}_CX$ und ${}_CY$ gegeben.

Es ist $\operatorname{Hom}_C(X, Y)$ bekanntermaßen eine abelsche Gruppe via $(f + \tilde f)(x) := f(x) + \tilde f(x)$ für $f, \tilde f \in \operatorname{Hom}_C(X, Y)$ und $x \in X$.

Es wird $\operatorname{Hom}_C(X, Y)$ zu einem R-Modul via $(rf)(x) := r(f(x))$ für $r \in R$, $f \in \operatorname{Hom}_C(X, Y)$ und $x \in X$.

Verifizieren wir dies. Seien $r, \tilde r \in R$, $f, \tilde f \in \operatorname{Hom}_C(X, Y)$, $c, \tilde c \in C$, $x, \tilde x \in X$ gegeben.

Es ist rf wieder C-linear, da

$$(rf)(c\,x + \tilde c\,\tilde x) \;=\; r(f(c\,x + \tilde c\,\tilde x)) \;=\; r(cf(x) + \tilde c f(\tilde x)) \;=\; c\,rf(x) + \tilde c\,rf(\tilde x) \;=\; c(rf)(x) + \tilde c(rf)(\tilde x)\,.$$

Es ist

$$\begin{aligned}(1\cdot f)(x) &= 1\cdot f(x)\\ &= f(x)\\ ((r\tilde r)f)(x) &= (r\tilde r)f(x)\\ &= r(\tilde r f(x))\\ &= r(\tilde r f)(x)\\ &= (r(\tilde r f))(x)\\ ((r+\tilde r)(f+\tilde f))(x) &= (r+\tilde r)(f+\tilde f)(x)\\ &= (r+\tilde r)(f(x)+\tilde f(x))\\ &= rf(x)+\tilde r f(x)+r\tilde f(x)+\tilde r\tilde f(x)\\ &= (rf)(x)+(\tilde r f)(x)+(r\tilde f)(x)+(\tilde r\tilde f)(x)\\ &= (rf+\tilde r f+r\tilde f+\tilde r\tilde f)(x)\ ,\end{aligned}$$

und also

$$\begin{aligned}1\cdot f &= f\\ (r\tilde r)f &= r(\tilde r f)\\ (r+\tilde r)(f+\tilde f) &= rf+\tilde r f+r\tilde f+\tilde r\tilde f\ .\end{aligned}$$

(1) Es soll $\mathrm{Hom}_A(M,P)$ zu einem B-Linksmodul werden vermöge

$$(b\cdot f)(m) := f(mb)$$

für $b\in B$, $f\in\mathrm{Hom}_A(M,P)$ und $m\in M$.
Verifizieren wir dies.
Bekanntermaßen ist $\mathrm{Hom}_A(M,P)$ eine abelsche Gruppe; cf. Vorbemerkung.
Seien ferner $b,\tilde b\in B$, $f,\tilde f\in\mathrm{Hom}_A(M,P)$, $a,\tilde a\in A$, $m,\tilde m\in M$ gegeben.
Es ist bf wieder A-linear, da

$$\begin{aligned}(bf)(am+\tilde a\tilde m) &= f((am+\tilde a\tilde m)b)\\ &= f(amb+\tilde a\tilde m b)\\ &= f(amb)+f(\tilde a\tilde m b)\\ &= af(mb)+\tilde a f(\tilde m b)\\ &= a(bf)(m)+\tilde a(bf)(\tilde m)\ .\end{aligned}$$

Es ist

$$\begin{aligned}(1\cdot f)(m) &= f(m\cdot 1)\\ &= f(m)\\ ((b\tilde b)f)(m) &= f(m(b\tilde b))\\ &= f((mb)\tilde b)\\ &= (\tilde b f)(mb)\\ &= (b(\tilde b f))(m)\\ ((b+\tilde b)(f+\tilde f))(m) &= (f+\tilde f)(m(b+\tilde b))\\ &= (f+\tilde f)(mb+m\tilde b)\\ &= f(mb+m\tilde b)+\tilde f(mb+m\tilde b)\\ &= f(mb)+f(m\tilde b)+\tilde f(mb)+\tilde f(m\tilde b)\\ &= (bf)(m)+(\tilde b f)(m)+(b\tilde f)(m)+(\tilde b\tilde f)(m)\\ &= (bf+\tilde b f+b\tilde f+\tilde b\tilde f)(m)\ ,\end{aligned}$$

und also

$$\begin{aligned}1\cdot f &= f\\ (b\tilde b)f &= b(\tilde b f)\\ (b+\tilde b)(f+\tilde f) &= bf+\tilde b f+b\tilde f+\tilde b\tilde f\ .\end{aligned}$$

(2) *Wohldefiniertheit von* Φ.

Gegeben sei $f \in \mathrm{Hom}_A(M \underset{B}{\otimes} N, P)$.

Zu zeigen ist die A-Linearität der Abbildung $M \to P$, $m \mapsto f(m \otimes n)$ für $n \in N$ und die B-Linearität der Abbildung $N \to \mathrm{Hom}_A(M,P)$, $n \mapsto (m \mapsto f(m \otimes n))$.

Es ist

$$\begin{aligned} am + \tilde{a}\tilde{m} &\mapsto f((am + \tilde{a}\tilde{m}) \otimes n) \\ &= f((am) \otimes n + (\tilde{a}\tilde{m}) \otimes n) \\ &= f(a(m \otimes n) + \tilde{a}(\tilde{m} \otimes n)) \\ &= af(m \otimes n) + \tilde{a}f(\tilde{m} \otimes n) \end{aligned}$$

für $a, \tilde{a} \in A$ und $m, \tilde{m} \in M$.

Ferner ist

$$\begin{aligned} bn + \tilde{b}\tilde{n} &\mapsto (m \mapsto f(m \otimes (bn + \tilde{b}\tilde{n}))) \\ &= (m \mapsto f(m \otimes bn + m \otimes \tilde{b}\tilde{n})) \\ &= (m \mapsto f(mb \otimes n + m\tilde{b} \otimes \tilde{n})) \\ &= (m \mapsto f(mb \otimes n) + f(m\tilde{b} \otimes \tilde{n})) \\ &= (m \mapsto f(mb \otimes n)) + (m \mapsto f(m\tilde{b} \otimes \tilde{n})) \\ &\overset{(1)}{=} b(m \mapsto f(m \otimes n)) + \tilde{b}(m \mapsto f(m \otimes \tilde{n})) \end{aligned}$$

für $b, \tilde{b} \in B$ und $n, \tilde{n} \in N$.

R-Linearität von Φ.

Die R-Modulstruktur von $\mathrm{Hom}_A(M \underset{B}{\otimes} N, P)$ und von $\mathrm{Hom}_B(N, \mathrm{Hom}_A(M,P))$ sei wie in der Vorbemerkung.

Seien $r, \tilde{r} \in R$ und $f, \tilde{f} \in \mathrm{Hom}_A(M \underset{B}{\otimes} N, P)$ gegeben. Es wird

$$\begin{aligned} \Phi(rf + \tilde{r}\tilde{f}) &= \big(n \mapsto (m \mapsto (rf + \tilde{r}\tilde{f})(m \otimes n))\big) \\ &= \big(n \mapsto (m \mapsto rf(m \otimes n) + \tilde{r}\tilde{f}(m \otimes n))\big) \\ &= \big(n \mapsto (m \mapsto rf(m \otimes n)) + (m \mapsto \tilde{r}\tilde{f}(m \otimes n))\big) \\ &= \big(n \mapsto (m \mapsto rf(m \otimes n))\big) + \big(n \mapsto (m \mapsto \tilde{r}\tilde{f}(m \otimes n))\big) \\ &= \big(n \mapsto r(m \mapsto f(m \otimes n))\big) + \big(n \mapsto \tilde{r}(m \mapsto \tilde{f}(m \otimes n))\big) \\ &= r\big(n \mapsto (m \mapsto f(m \otimes n))\big) + \tilde{r}\big(n \mapsto (m \mapsto \tilde{f}(m \otimes n))\big) \\ &= r\Phi(f) + \tilde{r}\Phi(\tilde{f}) \; . \end{aligned}$$

Wohldefiniertheit von Ψ.

Gegeben sei $g \in \mathrm{Hom}_B(N, \mathrm{Hom}_A(M,P))$.

Zu zeigen ist die B-Bilinearität von $M \times N \longrightarrow P$, $(m,n) \longmapsto (g(n))(m)$ sowie die A-Linearität der dann resultierenden Abbildung $M \underset{B}{\otimes} N \longrightarrow P$, $m \otimes n \longmapsto (g(n))(m)$.

Es ist

$$\begin{aligned} (g(bn))(m) &= (bg(n))(m) \\ &= (g(n))(mb) \end{aligned}$$

für $m \in M$, $n \in N$ und $b \in B$, sowie

$$\begin{aligned} (g(n + \tilde{n}))(m + \tilde{m}) &= (g(n) + g(\tilde{n}))(m + \tilde{m}) \\ &= (g(n))(m + \tilde{m}) + (g(\tilde{n}))(m + \tilde{m}) \\ &= (g(n))(m) + (g(n))(\tilde{m}) + (g(\tilde{n}))(m) + (g(\tilde{n}))(\tilde{m}) \end{aligned}$$

für $m, \tilde{m} \in M$ und $n, \tilde{n} \in N$.

Ferner ist

$$\begin{array}{rl} & a(\sum_{(m,n)} z_{(m,n)}\, m\otimes n) + \tilde{a}(\sum_{(m,n)} \tilde{z}_{(m,n)}\, m\otimes n) \\ = & \sum_{(m,n)}(z_{(m,n)}(am)\otimes n + \tilde{z}_{(m,n)}(\tilde{a}m)\otimes n) \\ \longmapsto & \sum_{(m,n)}(z_{(m,n)}(g(n))(am) + \tilde{z}_{(m,n)}(g(n))(\tilde{a}m)) \\ = & \sum_{(m,n)}(z_{(m,n)}a(g(n))(m) + \tilde{z}_{(m,n)}\tilde{a}(g(n))(m)) \\ = & a(\sum_{(m,n)} z_{(m,n)}(g(n))(m)) + \tilde{a}(\sum_{(m,n)} \tilde{z}_{(m,n)}(g(n))(m))\ . \end{array}$$

wobei $a,\, \tilde{a} \in A$ und $z_{(m,n)}\,,\, \tilde{z}_{(m,n)} \in \mathbf{Z}$ für $(m,n) \in M \times N$.

Gegenseitige Inversion von Φ und Ψ.

Zum einen wird

$$\begin{array}{rcl} \Psi(\Phi(f)) & = & \Psi\big(n \mapsto (m \mapsto f(m\otimes n))\big) \\ & = & \big(m\otimes n \mapsto (m \mapsto f(m\otimes n))(m)\big) \\ & = & \big(m\otimes n \mapsto f(m\otimes n)\big) \\ & = & f \end{array}$$

für $f \in \mathrm{Hom}_A(M \underset{B}{\otimes} N,\, P)$.

Zum anderen wird

$$\begin{array}{rcl} \Phi(\Psi(g)) & = & \Phi\big(m\otimes n \mapsto (g(n))(m)\big) \\ & = & \big(n \mapsto (m \mapsto \big(m\otimes n \mapsto (g(n))(m)\big)(m\otimes n))\big) \\ & = & \big(n \mapsto (m \mapsto (g(n))(m))\big) \\ & = & \big(n \mapsto g(n)\big) \\ & = & g \end{array}$$

für $g \in \mathrm{Hom}_B(N,\, \mathrm{Hom}_A(M,P))$.

Die R-Linearität von $\Psi = \Phi^-$ folgt nun aus der von Φ.

> Die Aussage von Aufgabe 31.(2) kennt man auch als "Adjunktion von Tensor und Hom", symbolisch geschrieben $M \underset{B}{\otimes} - \ \dashv\ \mathrm{Hom}_A(M,-)$.
>
> Vorsicht! (Hinweis von Simon Klenk.)
>
> Es ist $\mathrm{Hom}_A(M,P)$ ein B-Modul, also auch, via definierendem Morphismus $R \to A$, ein R-Modul. Schreibe diese Operation $r * f$ für $r \in R$ und $f \in \mathrm{Hom}_A(M,P)$. Es ist also $(r*f)(m) = f(m\cdot r)$ für $m \in M$.
>
> Es ist $\mathrm{Hom}_A(M,P)$ aber auch ein R-Modul wie oben angegeben. Wir schreiben diese Operation weiterhin $r \cdot f$ für $r \in R$ und $f \in \mathrm{Hom}_A(M,P)$. Es ist also $(r\cdot f)(m) = r \cdot f(m)$ für $m \in M$.
>
> Ist nun $r\cdot m = m \cdot r$ für alle $r \in R$ und $m \in M$, dann ist stets $f(m\cdot r) = f(r\cdot m) = r\cdot f(m)$, da f als A-lineare Abbildung insbesondere R-linear ist. Also ist diesenfalls $r * f = r \cdot f$.
>
> Im allgemeinen ist aber $r * f \neq r \cdot f$. Sei hierzu etwa $R = A = B = M = P := \mathbf{C}$. Sei $a\cdot m\cdot b := am\bar{b}$, letzteres Produkt gebildet im Körper $\mathbf{C}$. Sei $f = \mathrm{id}$, $m = 1$ und $r = \mathrm{i}$. Zum einen ist $(r*f)(m) = f(m\cdot r) = \mathrm{id}(1\cdot \mathrm{i}) = \bar{\mathrm{i}} = -\mathrm{i}$. Zum anderen ist $(r\cdot f)(m) = r\cdot f(m) = \mathrm{i}\cdot \mathrm{id}(1) = \mathrm{i}$.

(3) Wir haben zu zeigen, daß

$$\begin{array}{rcl} P|_B & \longleftrightarrow & \mathrm{Hom}_A(A,P) \\ p & \longmapsto & (a \mapsto ap) \\ u(1) & \longleftarrow\!\shortmid & u \end{array}$$

sich invertierende B-lineare Abbildungen sind.

Wohldefiniertheit von $\longmapsto$.

Sei $p \in P$. Es ist $A \twoheadrightarrow P$, $a \mapsto ap$ eine A-lineare Abbildung, da

$$(xa + \tilde{x}\tilde{a}) \mapsto (xa + \tilde{x}\tilde{a})p \ = \ x(ap) + \tilde{x}(\tilde{a}p)$$

für $x,\, \tilde{x},\, a,\, \tilde{a} \in A$.

B-Linearität von $\longmapsto$.

Es wird

$$\begin{array}{rcl} bp+\tilde{b}\tilde{p} & \longmapsto & (a \mapsto a(bp+\tilde{b}\tilde{p})) \\ & = & (a \mapsto abp + a\tilde{b}\tilde{p}) \\ & = & (a \mapsto abp) + (a \mapsto a\tilde{b}\tilde{p}) \\ & \overset{(1)}{=} & b(a \mapsto ap) + \tilde{b}(a \mapsto a\tilde{p}) \end{array}$$

für $b, \tilde{b} \in B$ und $p, \tilde{p} \in P$.

Gegenseitige Inversion.

Zum einen wird $p \longmapsto (a \mapsto ap) \longmapsto (a \mapsto ap)(1) = p$ für $p \in P$.

Zum anderen wird $u \longmapsto u(1) \longmapsto (a \mapsto au(1) = u(a)) = u$.

Aufgabe 32

Da $6 \cdot (\mathbf{Z} \times \mathbf{Z}^{2\times 2} \times \mathbf{Z}) \subseteq \omega(\mathbf{Z}\mathrm{S}_3)$, ist $\mathrm{Z}(\omega(\mathbf{Z}\mathrm{S}_3)) = \omega(\mathbf{Z}\mathrm{S}_3) \cap \mathrm{Z}(\mathbf{Z} \times \mathbf{Z}^{2\times 2} \times \mathbf{Z})$.

Unter Verwendung der Lösung zu Aufgabe 18.(1) ergibt sich

$$\omega(\mathbf{Z}\mathrm{S}_3) \cap \mathrm{Z}(\mathbf{Z} \times \mathbf{Z}^{2\times 2} \times \mathbf{Z}) \;=\; \left\{ (a, \left(\begin{smallmatrix} b & 0 \\ 0 & b \end{smallmatrix}\right), c) \in \mathbf{Z} \times \mathbf{Z}^{2\times 2} \times \mathbf{Z} \,:\, a \equiv_3 b,\; b \equiv_3 c,\; a \equiv_2 c \right\} .$$

Es folgt

$$\mathrm{Z}(\mathbf{Z}\mathrm{S}_3) \xrightarrow[\sim]{\omega_{\mathrm{Z}}|^{\omega_{\mathrm{Z}}(\mathrm{Z}(\mathbf{Z}\mathrm{S}_3))}_{\mathrm{Z}(\mathbf{Z}\mathrm{S}_3)}} \omega_{\mathrm{Z}}(\mathrm{Z}(\mathbf{Z}\mathrm{S}_3)) \;=\; \{(a,b,c) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \,:\, a \equiv_3 b \equiv_3 c,\; a \equiv_2 c\} \;\subseteq\; \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} .$$

Aufgabe 33

(1) Die Aussage ist falsch. Es hat e.g. S_3 einen irreduziblen Charakter $\chi := (\begin{smallmatrix} 2 & 0 & -1 \end{smallmatrix})$; cf. Beispiel 86.(1). Multipliziert mit der Klassenfunktion $\varphi := (\begin{smallmatrix} 0 & 0 & 1 \end{smallmatrix})$ erhalten wir die Klassenfunktion $\chi \cdot \varphi = (\begin{smallmatrix} 0 & 0 & -1 \end{smallmatrix})$. Diese ist kein Charakter, da ${}_{\mathrm{S}_3}(\chi \cdot \varphi\,,\, \chi) = \frac{1}{3} \notin \mathbf{Z}$.

(2) Die Aussage ist richtig.

Wegen $\psi(1) = 1$ ist $\psi|^{\mathrm{GL}_1(\mathbf{C})} : G \longrightarrow \mathrm{GL}_1(\mathbf{C})$ ein Gruppenmorphismus; cf. Beispiel 73.(6).

Also ist $\psi(g)^- = \psi(g^-) \overset{\text{A. 25.(2)}}{=} \overline{\psi(g)}$ für $g \in G$.

Es folgt

$$\begin{array}{rcl} {}_G(\chi \cdot \psi,\, \chi \cdot \psi) & = & \frac{1}{|G|} \sum_g \chi(g) \cdot \psi(g) \cdot \overline{\chi(g) \cdot \psi(g)} \\ & = & \frac{1}{|G|} \sum_g \chi(g)\, \overline{\chi(g)}\, \psi(g)\psi(g)^- \\ & = & \frac{1}{|G|} \sum_g \chi(g)\, \overline{\chi(g)} \\ & = & {}_G(\chi, \chi) \\ & \overset{\text{B. 94.(2)}}{=} & 1\,, \end{array}$$

und also ist $\chi \cdot \psi$ irreduzibel; cf. Bemerkung 94.(2).

Cf. Beispiel 111.

(3) Die Aussage ist falsch.

Schreibe $\mathrm{C}_2 = \langle\, a \,:\, a^2 \,\rangle$.

Betrachte den Gruppenmorphismus $f : \mathrm{C}_2 \longrightarrow \mathrm{S}_3\,,\, a \longmapsto (1,2)$.

Wir verwenden die Bezeichnungen von Beispiel 86.(1) für $\mathrm{X}(\mathrm{S}_3)$, und die von Beispiel 86.(2) für $\mathrm{X}(\mathrm{C}_2)$.

Es ist $\chi_3 = \left(\begin{smallmatrix} 2 & 0 & -1 \end{smallmatrix}\right)$ ein irreduzibler Charakter von S_3.

Es wird $(\chi_3 \circ f)(1) = \chi_3(\mathrm{id}) = 2$ und $(\chi_3 \circ f)(a) = \chi_3((1,2)) = 0$.

Somit ist $\chi_3 \circ f = \left(\begin{smallmatrix} 2 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & -1 \end{smallmatrix}\right)$ nicht irreduzibel; cf. Beispiel 86.(2).

(4) Die Aussage ist richtig.

Über Charaktere.

Wir wollen zeigen, daß ${}_H(\chi \circ f, \chi \circ f) \stackrel{!}{=} 1$ ist; cf. Bemerkung 94.(2).

Beachte, daß die Fasern von $H \xrightarrow{f} G$ alle die gleiche Länge $|H|/|G|$ haben, da für $g \in G$ und $h \in H$ mit $f(h) = g$ sich $f^{-1}(\{g\}) = h \cdot \operatorname{Kern} f$ ergibt, und da $|H|/|\operatorname{Kern} f| = |H/\operatorname{Kern} f| = |G|$.

Somit wird

$$\begin{aligned}
{}_H(\chi \circ f, \chi \circ f) &= |H|^{-1} \textstyle\sum_{h \in H} \chi(f(h)) \overline{\chi(f(h))} \\
&= |H|^{-1} \textstyle\sum_{g \in G} \sum_{h \in f^{-1}(\{g\})} \chi(f(h)) \overline{\chi(f(h))} \\
&= |H|^{-1} \textstyle\sum_{g \in G} \sum_{h \in f^{-1}(\{g\})} \chi(g) \overline{\chi(g)} \\
&= |H|^{-1} \textstyle\sum_{g \in G} |f^{-1}(\{g\})| \, \chi(g) \overline{\chi(g)} \\
&= |H|^{-1} \textstyle\sum_{g \in G} (|H|/|G|) \chi(g) \overline{\chi(g)} \\
&= |G|^{-1} \textstyle\sum_{g \in G} \chi(g) \overline{\chi(g)} \\
&= {}_G(\chi, \chi) \\
&= 1 \, .
\end{aligned}$$

Über Moduln.

Sei $\chi = \chi_V$ für einen einfachen $\mathbf{C}G$-Modul V; cf. Definition 76.

Sei $\rho : G \longrightarrow \mathrm{GL}(V)$ die zugehörige Darstellung; cf. Lemma 44.(2).

Es ist $\rho \circ f : H \longrightarrow \mathrm{GL}(V)$ eine Darstellung von H auf V.

Schreiben wir $V\rfloor_f$ für den zugehörigen $\mathbf{C}H$-Modul. I.e. als $\mathbf{C}$-Vektorraum ist $V\rfloor_f = V$, und es operiert $h \in H$ via $h \cdot v = (\rho(f(h)))(v) = f(h)v$ für $v \in V$.

Es ist $(\chi \circ f)(h) = \operatorname{tr} \rho(f(h))$ für $h \in H$, und folglich ist $\chi \circ f = \chi_{V\rfloor_f}$.

Somit ist zu zeigen, daß $V\rfloor_f$ ein einfacher $\mathbf{C}H$-Modul ist.

Da V einfach über $\mathbf{C}G$ ist, ist $V \neq 0$ und somit $V\rfloor_f \neq 0$.

Sei $W \subseteq V = V\rfloor_f$ ein $\mathbf{C}H$-Teilmodul.

Können wir zeigen, daß $W \subseteq V$ ein $\mathbf{C}G$-Teilmodul ist, so folgt aus der Einfachheit von V, daß $W = 0$ oder $W = V$, und wir sind fertig.

Es ist $W \subseteq V$ ein $\mathbf{C}$-Teilraum. Bleibt zu zeigen, daß $gW \stackrel{!}{\subseteq} W$ für $g \in G$.

Sei $g \in G$. Da f surjektiv ist, gibt es ein $h \in H$ mit $f(h) = g$. Es wird

$$gw \;=\; f(h)w \;=\; h \cdot w \;\in\; W$$

für $w \in W$, da $W \subseteq V$ ein $\mathbf{C}H$-Teilmodul ist.

Aufgabe 34

(1) Schreibe für $(z^s)_s \in \prod_{s\in[1,t]} \mathbf{C}^{n_s\times n_s}$ zunächst

$$\omega'\big(z^1\,,\,\ldots\,,\,z^t\big) \;:=\; \textstyle\sum_{g\in G}\Big(\frac{1}{|G|}\sum_{s\in[1,t]} n_s\,\mathrm{tr}\,\big(\omega^s(g^-)\,z^s\big)\Big)g \;\in\; \mathbf{C}G\,.$$

Wir wollen $\omega' \stackrel{!}{=} \omega^-$ zeigen. Da wir bereits wissen, daß ω ein Isomorphismus ist, genügt es, $\omega'\circ\omega \stackrel{!}{=} \mathrm{id}_{\mathbf{C}G}$ zu zeigen. Dank $\mathbf{C}$-Linearität von ω und ω' genügt es zu zeigen, daß $(\omega'\circ\omega)(h) = h$ für $h\in G$. In der Tat wird

$$\begin{aligned}
(\omega'\circ\omega)(h) &= \textstyle\sum_{g\in G}\Big(\frac{1}{|G|}\sum_{s\in[1,t]} n_s\,\mathrm{tr}\,\big(\omega^s(g^-)\,\omega^s(h)\big)\Big)g\\
&= \textstyle\sum_{g\in G}\Big(\frac{1}{|G|}\sum_{s\in[1,t]} n_s\,\mathrm{tr}\,\omega^s(g^-h)\Big)g\\
&= \textstyle\sum_{g\in G}\Big(\frac{1}{|G|}\sum_{s\in[1,t]} n_s\chi_s(g^-h)\Big)g\\
&\stackrel{\text{L. 87}}{=} \textstyle\sum_{g\in G}\partial_{g^-h,1}\,g\\
&= h\,.
\end{aligned}$$

(2) Sei $q\in[1,t]$. Es wird

$$\begin{aligned}
\varepsilon_q &\stackrel{\text{Def.}}{=} \omega^-\big((\partial_{q,s}\mathrm{E}_{n_s})_s\big)\\
&= \textstyle\sum_{g\in G}\Big(\frac{1}{|G|}\sum_{s\in[1,t]} n_s\,\mathrm{tr}\,\big(\omega^s(g^-)\,\partial_{q,s}\mathrm{E}_{n_s}\big)\Big)g\\
&= \textstyle\sum_{g\in G}\Big(\frac{1}{|G|}\,n_q\,\mathrm{tr}\,\big(\omega^q(g^-)\big)\Big)g\\
&= \textstyle\frac{1}{|G|}\sum_{g\in G} n_q\chi_q(g^-)g\,,
\end{aligned}$$

wie auch in Lemma 89.

(3) Sei $q\in[1,t]$. Seien $a,\,b\,\in\,[1,n_q]$. Es wird

$$\begin{aligned}
\mathrm{e}^q_{a,b} &= \omega\Big(\omega^-(\mathrm{e}^q_{a,b})\Big)\\
&= \omega\Big(\textstyle\sum_{g\in G}\Big(\frac{1}{|G|}\,n_q\,\mathrm{tr}\,\big(\omega^q(g^-)\,\mathrm{e}_{a,b}\big)\Big)g\Big)\\
&= \omega\Big(\textstyle\sum_{g\in G}\Big(\frac{1}{|G|}\,n_q\,\omega^q_{b,a}(g^-)\Big)g\Big)\\
&= \Big(\textstyle\sum_{g\in G}\frac{1}{|G|}\,n_q\,\omega^q_{b,a}(g^-)\,\omega^s(g)\Big)_s\\
&= \Big(\big(\textstyle\sum_{g\in G}\frac{1}{|G|}\,n_q\,\omega^q_{b,a}(g^-)\,\omega^s_{i,j}(g)\big)_{i,j}\Big)_s\,.
\end{aligned}$$

In anderen Worten, für $q,\,s\,\in\,[1,t]$, $a,\,b\,\in\,[1,n_q]$ und $i,\,j\,\in\,[1,n_s]$ ist

$$\sum_{g\in G}\omega^q_{b,a}(g^-)\,\omega^s_{i,j}(g) \;=\; 0$$

falls $q\neq s$, und

$$\sum_{g\in G}\omega^q_{b,a}(g^-)\,\omega^q_{i,j}(g) \;=\; \frac{|G|}{n_q}\,\partial_{i,b}\,\partial_{j,a}\,.$$

Da sich nach Gleichsetzen von a und b sowie von i und j und jeweiliger Summation wieder die horizontale Orthogonalität ergibt, ist dies also eine Art "verfeinerte horizontale Orthogonalität"; allerdings abhängig von der Wahl von ω, im Gegensatz zur horizontalen Orthogonalität aus Satz 90.(1).

Aufgabe 35

Betrachte G als G-Menge via Konjugation; cf. Beispiel 2.(6).

Dies liefert den $\mathbf{C}G$-Modul $\mathbf{C}G$ mit der Konjugationsoperation. Sei $\psi := \chi_{\mathbf{C}G}$ der zugehörige Charakter.

Für $g \in G$ wird

$$\psi(g) \overset{\text{B. 73.(3)}}{=} |\{\, x \in G \,:\, {}^g x = x \,\}| \;=\; |\{\, x \in G \,:\, gx = xg \,\}| \;=\; |\{\, x \in G \,:\, {}^x g = g \,\}| \;=\; |\mathrm{C}_G(g)| \,.$$

Somit wird

$$\mathbf{Z}_{\geqslant 0} \overset{\text{B. 95.(1)}}{\ni} {}_G(\chi, \psi) \;=\; \tfrac{1}{|G|} \textstyle\sum_{s \in [1,t]} |{}^G g_s|\, \chi(g_s)\, \overline{\psi(g_s)} \;=\; \tfrac{1}{|G|} \textstyle\sum_{s \in [1,t]} |{}^G g_s|\, \chi(g_s)\, |\mathrm{C}_G(g_s)| \overset{\text{L. 5}}{=} \textstyle\sum_{s \in [1,t]} \chi(g_s) \,.$$

Aufgabe 36

(1) *Über Charaktere.*

Vorbemerkung. Für φ, φ', $\varphi'' \in \mathrm{Kf}(G)$ ist

$${}_G(\varphi \cdot \varphi', \varphi'') \;=\; \tfrac{1}{|G|} \textstyle\sum_{g \in G} \varphi(g)\, \varphi'(g)\, \overline{\varphi''(g)} \;=\; {}_G(\varphi,\, \bar{\varphi}' \cdot \varphi'') \,.$$

Dank Bemerkung 94.(1), genügt es zu zeigen, daß für jeden irreduziblen Charakter τ von G gilt, daß

$${}_G\big((\psi \cdot (\chi\downarrow_H^G))\uparrow_H^G, \tau\big) \;\overset{!}{=}\; {}_G\big((\psi\uparrow_H^G) \cdot \chi\,, \tau\big)$$

ist. In der Tat wird

$$\begin{aligned}
{}_G\big((\psi \cdot (\chi\downarrow_H^G))\uparrow_H^G, \tau\big) &\overset{\text{L. 120}}{=} {}_H\big(\psi \cdot (\chi\downarrow_H^G), \tau\downarrow_H^G\big) \\
&= {}_H\big(\psi, \overline{(\chi\downarrow_H^G)} \cdot (\tau\downarrow_H^G)\big) \\
&= {}_H\big(\psi, (\bar{\chi} \cdot \tau)\downarrow_H^G\big) \\
&\overset{\text{L. 120}}{=} {}_G\big(\psi\uparrow_H^G, \bar{\chi} \cdot \tau\big) \\
&= {}_G\big((\psi\uparrow_H^G) \cdot \chi\,, \tau\big) \,.
\end{aligned}$$

Alternativ können wir Lemma 117 verwenden und erhalten für $g \in G$

$$\begin{aligned}
(\psi \cdot (\chi\downarrow_H^G))\uparrow_H^G(g) &= |H|^{-1} \textstyle\sum_{x \in G,\ {}^x g \in H} (\psi \cdot (\chi\downarrow_H^G))({}^x g) \\
&= |H|^{-1} \textstyle\sum_{x \in G,\ {}^x g \in H} \psi({}^x g) \cdot \chi({}^x g) \\
&= |H|^{-1} \textstyle\sum_{x \in G,\ {}^x g \in H} \psi({}^x g) \cdot \chi(g) \\
&= \psi\uparrow_H^G(g) \cdot \chi(g) \\
&= ((\psi\uparrow_H^G) \cdot \chi)(g) \,.
\end{aligned}$$

Über Moduln.

Beachte zunächst, daß

$$(\psi \cdot (\chi\downarrow_H^G))\uparrow_H^G \;=\; \chi_{N \otimes M}\uparrow_H^G \;=\; \chi_{\mathbf{C}G \underset{\mathbf{C}H}{\otimes} (N \otimes M)}$$

und

$$(\psi\uparrow_H^G) \cdot \chi \;=\; (\chi_N\uparrow_H^G) \cdot \chi_M \;=\; \chi_{(\mathbf{C}G \underset{\mathbf{C}H}{\otimes} N) \otimes M}$$

ist. Wir haben zu zeigen, daß eben diese zugehörigen $\mathbf{C}G$-Moduln isomorph sind; cf. Bemerkung 95.(2).

Wir wollen zunächst folgende $\mathbf{C}H$-lineare Abbildung konstruieren.

$$\begin{array}{ccccccc} N & \otimes & M & \xrightarrow{f_0} & (\mathbf{C}G & \underset{\mathbf{C}H}{\otimes} & N) \otimes M \\ n & \otimes & m & \longmapsto & (1 & \otimes & n) \otimes m \end{array}$$

Es ist $(1 \otimes n) \otimes m$ additiv in m und n. Ferner wird für $z \in \mathbf{C}$ auch

$$(1 \otimes nz) \otimes m \;=\; (1 \otimes n)z \otimes m = (1 \otimes n) \otimes zm \;.$$

Folglich ist f_0 wohldefiniert und $\mathbf{Z}$-linear.

Auf $\mathbf{Z}$-linearen Erzeugern erkennt man, daß f_0 auch $\mathbf{C}$-linear ist, denn es wird

$$\begin{array}{rcl} f_0(z(n \otimes m)) & = & f_0(zn \otimes m) \\ & = & (1 \otimes zn) \otimes m \\ & = & (z \otimes n) \otimes m \\ & = & (z(1 \otimes n)) \otimes m \\ & = & z((1 \otimes n) \otimes m) \\ & = & z f_0(n \otimes m) \end{array}$$

für $z \in \mathbf{C}$, wobei $m \in M$ und $n \in N$.

Schließlich erkennt man auf $\mathbf{Z}$-linearen Erzeugern, daß f_0 insgesamt $\mathbf{C}H$-linear ist, denn es wird

$$\begin{array}{rcl} f_0(h(n \otimes m)) & = & f_0(hn \otimes hm) \\ & = & (1 \otimes hn) \otimes hm \\ & = & (h \otimes n) \otimes hm \\ & = & h(1 \otimes n) \otimes hm \\ & = & h((1 \otimes n) \otimes m) \\ & = & h f_0(n \otimes m) \end{array}$$

für $h \in H$, wobei $n \in N$ und $m \in M$.

Dies liefert via Aufgabe 31.(2, 3) die $\mathbf{C}G$-lineare Abbildung

$$\begin{array}{ccccccc} \mathbf{C}G & \underset{\mathbf{C}H}{\otimes} & (N & \otimes & M) & \xrightarrow{f} & (\mathbf{C}G \underset{\mathbf{C}H}{\otimes} N) \otimes M \\ g & \otimes & (n & \otimes & m) & \longmapsto & (g \otimes n) \otimes gm \;, \end{array}$$

da $g \otimes (n \otimes m)$ in der Tat abgebildet wird auf

$$g f_0(n \otimes m) \;=\; g((1 \otimes n) \otimes m) \;=\; g(1 \otimes n) \otimes gm \;=\; (g \otimes n) \otimes gm \;.$$

> Vorsicht, es hat f mit dem Assoziativitätsisomorphismus aus der Lösung zu Aufgabe 26.(4) nichts zu tun.

Bleibt zu zeigen, daß f bijektiv ist.

Sei $G = \bigsqcup_{k \in [1,\ell]} x_k H$.

Sei $(\, n_j \,:\, j \in [1,v] \,)$ eine $\mathbf{C}$-lineare Basis von N. Sei $(\, m_i \,:\, i \in [1,u] \,)$ eine $\mathbf{C}$-lineare Basis von M. Dann ist

$$\big(\, x_k \otimes (n_j \otimes m_i) \,:\, k \in [1,\ell],\, j \in [1,v],\; i \in [1,u] \,\big)$$

eine $\mathbf{C}$-lineare Basis von $\mathbf{C}G \underset{\mathbf{C}H}{\otimes} (N \otimes M)$; cf. Beweis zu Lemma 110 und Beweis zu Lemma 117. Diese wird auf das Tupel

$$\big(\, (x_k \otimes n_j) \otimes x_k m_i \,:\, k \in [1,\ell],\, j \in [1,v],\; i \in [1,u] \,\big)$$

abgebildet. Da für jedes $k \in [1,\ell]$ das Tupel $(\, x_k m_i \,:\, i \in [1,u]\,)$ eine $\mathbf{C}$-lineare Basis von M und $(\, x_k \otimes n_j \,:\, k \in [1,\ell],\ j \in [1,v]\,)$ eine $\mathbf{C}$-lineare Basis von $\mathbf{C}G \underset{\mathbf{C}H}{\otimes} N$ ist, ist jenes Bildtupel eine $\mathbf{C}$-lineare Basis von $(\mathbf{C}G \underset{\mathbf{C}H}{\otimes} N) \otimes M$.

Somit ist f bijektiv.

(2) *Über Charaktere.*

Es ist

$$((\chi \cdot \chi') \cdot \chi'')(g) \;=\; (\chi(g) \cdot \chi'(g)) \cdot \chi''(g) \;=\; \chi(g) \cdot (\chi'(g) \cdot \chi''(g)) \;=\; (\chi \cdot (\chi' \cdot \chi''))(g)$$

für $g \in G$.

Über Moduln.

Beachte zunächst, daß

$$(\chi \cdot \chi') \cdot \chi'' \;=\; (\chi_M \cdot \chi_{M'}) \cdot \chi_{M''} \;=\; \chi_{M \otimes M'} \cdot \chi_{M''} \;=\; \chi_{(M \otimes M') \otimes M''}$$

und

$$\chi \cdot (\chi' \cdot \chi'') \;=\; \chi_M \cdot (\chi_{M'} \cdot \chi_{M''}) \;=\; \chi_M \cdot \chi_{M' \otimes M''} \;=\; \chi_{M \otimes (M' \otimes M'')}$$

ist. Wir haben zu zeigen, daß eben diese zugehörigen $\mathbf{C}G$-Moduln isomorph sind; cf. Bemerkung 95.(2).

Wir verfügen über die bijektive $\mathbf{C}$-lineare Abbildung

$$\begin{array}{ccccccccc} M & \otimes & (M' & \otimes & M'') & \xrightarrow{\;f\;} & (M & \otimes & M') & \otimes & M'' \\ m & \otimes & (m' & \otimes & m'') & \longmapsto & (m & \otimes & m') & \otimes & m'' \,; \end{array}$$

cf. Aufgabe 26.(4) und Lösung davon.

Wir haben zu zeigen, daß diese Abbildung $\mathbf{C}G$-linear ist. Es genügt, dies auf $\mathbf{Z}$-linearen Erzeugern zu zeigen. Es wird

$$\begin{array}{rcl} f(g(m \otimes (m' \otimes m''))) & = & f(gm \otimes g(m' \otimes m'')) \\ & = & f(gm \otimes (gm' \otimes gm'')) \\ & = & (gm \otimes gm') \otimes gm'' \\ & = & g(m \otimes m') \otimes gm'' \\ & = & g((m \otimes m') \otimes m'') \\ & = & gf(m \otimes (m' \otimes m''))\,, \end{array}$$

wobei $g \in G$, $m \in M$, $m' \in M'$, $m'' \in M''$.

(3) *Über Charaktere.*

Es ist

$$\overline{(\chi \cdot \chi')}(g) \;=\; \overline{(\chi \cdot \chi')(g)} \;=\; \overline{\chi(g) \cdot \chi'(g)} \;=\; \overline{\chi(g)} \cdot \overline{\chi'(g)} \;=\; \bar\chi(g) \cdot \bar\chi'(g) \;=\; (\bar\chi \cdot \bar\chi')(g)$$

für $g \in G$.

Über Moduln.

Beachte zunächst, daß

$$\overline{\chi \cdot \chi'} \;=\; \overline{\chi_M \cdot \chi_{M'}} \;=\; \bar\chi_{M \otimes M'} \;=\; \chi_{(M \otimes M')^*}$$

und

$$\bar\chi \cdot \bar\chi' \;=\; \bar\chi_M \cdot \bar\chi_{M'} \;=\; \chi_{M^*} \cdot \chi_{M'^*} \;=\; \chi_{M^* \otimes M'^*}$$

ist. Wir haben zu zeigen, daß eben diese zugehörigen $\mathbf{C}G$-Moduln isomorph sind; cf. Bemerkung 95.(2).

Wir wollen folgende $\mathbf{C}G$-lineare Abbildung konstruieren und als bijektiv nachweisen.

$$\begin{array}{ccccc} M^* & \otimes & M'^* & \xrightarrow{f} & (M \otimes M')^* \\ \lambda & \otimes & \lambda' & \longmapsto & (m \otimes m' \mapsto \lambda(m) \cdot \lambda'(m')) \end{array}$$

Es ist $(m \otimes m' \mapsto \lambda(m) \cdot \lambda'(m'))$ additiv in λ und in λ'. Für $z \in \mathbf{C}$ wird ferner

$$(\lambda z)(m) \cdot \lambda'(m') \;=\; (z\lambda)(m) \cdot \lambda'(m') \;=\; z \cdot \lambda(m) \cdot \lambda'(m') \;=\; \lambda(m) \cdot (z\lambda')(m')$$

für $m \in M$ und $m' \in M'$, weswegen die entsprechenden Abbildungen aus $M \otimes M'$ übereinstimmen.
Also ist f eine wohldefinierte $\mathbf{Z}$-lineare Abbildung.
Zeigen wir, daß f auch $\mathbf{C}G$-linear ist. Für $z \in \mathbf{C}$, $g \in G$, $\lambda \in M^*$ und $\lambda' \in M'^*$ wird

$$\begin{array}{rcl} f(z(\lambda \otimes \lambda')) & = & f(z\lambda \otimes \lambda') \\ & = & (m \otimes m' \mapsto (z\lambda)(m) \cdot \lambda'(m')) \\ & = & (m \otimes m' \mapsto z\lambda(m) \cdot \lambda'(m')) \\ & = & z(m \otimes m' \mapsto \lambda(m) \cdot \lambda'(m')) \end{array}$$

und

$$\begin{array}{rcl} f(g(\lambda \otimes \lambda')) & = & f(g\lambda \otimes g\lambda') \\ & = & (m \otimes m' \mapsto (g\lambda)(m) \cdot (g\lambda')(m')) \\ & = & (m \otimes m' \mapsto \lambda(g^- m) \cdot \lambda'(g^- m')) \\ & = & g(m \otimes m' \mapsto \lambda(m) \cdot \lambda'(m')) \;, \end{array}$$

beachte hierzu, daß $g^-(m \otimes m') = g^- m \otimes g^- m'$ ist, sowie cf. Lemma 106.
Zeigen wir, daß f bijektiv ist.
Sei $(m_1, \ldots, m_u)$ eine $\mathbf{C}$-lineare Basis von M. Sei $(\lambda_1, \ldots, \lambda_u)$ die dazu duale Basis von M^*.
Sei $(m'_1, \ldots, m'_{u'})$ eine $\mathbf{C}$-lineare Basis von M'. Sei $(\lambda'_1, \ldots, \lambda'_{u'})$ die dazu duale Basis von M'^*.
Es ist $(\, \lambda_i \otimes \lambda'_j \,:\, i \in [1,u],\ j \in [1,u'] \,)$ eine $\mathbf{C}$-lineare Basis von $M^* \otimes M'^*$; cf. Beweis zu Lemma 110.
Diese wird unter f abgebildet auf

$$(\, (m \otimes m' \mapsto \lambda_i(m) \cdot \lambda'_j(m')) \,:\, i \in [1,u],\ j \in [1,u'] \,) \;.$$

Es ist $(\, m_i \otimes m'_j \,:\, i \in [1,u],\ j \in [1,u'] \,)$ eine $\mathbf{C}$-lineare Basis von $M \otimes M'$; cf. Beweis zu Lemma 110.
Zu dieser ist unser Bildtupel eine duale Basis von $(M \otimes M')^*$, da sich

$$(m \otimes m' \mapsto \lambda_i(m) \cdot \lambda'_j(m'))(m_{\tilde{i}} \otimes m'_{\tilde{j}}) \;=\; \lambda_i(m_{\tilde{i}}) \cdot \lambda_j(m'_{\tilde{j}}) \;=\; \partial_{i,\tilde{i}}\, \partial_{j,\tilde{j}} \;=\; \partial_{(i,j),(\tilde{i},\tilde{j})}$$

ergibt für $i, \tilde{i} \in [1,u]$ und $j, \tilde{j} \in [1,u']$.
Also ist f bijektiv.

Argumente über Moduln lassen sich bei Bedarf besser verallgemeinern als Argumente über Charaktere. Daher legt man Wert auf diese Möglichkeit.

Aufgabe 37

(1) Wir zerlegen $\mathrm{S}_4 = \mathrm{S}_3\,\mathrm{id} \sqcup \mathrm{S}_3(1,4) \sqcup \mathrm{S}_3(2,4) \sqcup \mathrm{S}_3(3,4)$.

Dies sieht man e.g. wie folgt. Es ist $\mathrm{S}_4/\mathrm{S}_3 \to [1,4]$, $\sigma\mathrm{S}_3 \mapsto \sigma(4)$ ein Isomorphismus von S_4-Mengen; cf. Lemma 5. Unter dieser bijektiven Abbildung kommt $\mathrm{id}\,\mathrm{S}_3$ auf 4, $(1,4)$ auf 1, $(2,4)$ auf 2 und $(3,4)$ auf 3. Schließlich bilden die Inversen einer Menge von Linksnebenklassenvertretern eine Menge von Rechtsnebenklassenvertretern.

Schreibe dementsprechend $\rho_1 := \mathrm{id}$, $\rho_2 := (1,4)$, $\rho_3 := (2,4)$, $\rho_4 := (3,4)$.

Wir haben die Konjugationsklassenrepräsentanten id, $(1,2)$, $(1,2,3)$ in S_3 aus Beispiel 93.(1).

Wir haben die Konjugationsklassenrepräsentanten id, $(1,2)$, $(1,2,3)$, $(1,2,3,4)$ und $(1,2)(3,4)$ in S_4. Die Konjugationsklassenlängen sind 1, 6, 8, 6, 3, respektive.

Es ist $\chi_1 = (1\ 1\ 1)$. Mit Lemma 117 wird

$$\begin{aligned}
\chi_1\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}(\mathrm{id}) &= \tfrac{|\mathrm{S}_4|}{|\mathrm{S}_3|}\,\chi_1(\mathrm{id}) = 4\\
\chi_1\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2)\in\mathrm{S}_3} \chi_1({}^{\rho_j}(1,2)) = 1+0+0+1 = 2\\
\chi_1\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2,3)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2,3)\in\mathrm{S}_3} \chi_1({}^{\rho_j}(1,2,3)) = 1+0+0+0 = 1\\
\chi_1\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2,3,4)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2,3,4)\in\mathrm{S}_3} \chi_1({}^{\rho_j}(1,2,3,4)) = 0+0+0+0 = 0\\
\chi_1\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2)(3,4)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2)(3,4)\in\mathrm{S}_3} \chi_1({}^{\rho_j}(1,2)(3,4)) = 0+0+0+0 = 0\,.
\end{aligned}$$

So ergibt sich $\chi_1\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4} = (4\ 2\ 1\ 0\ 0)$.

Es ist $\chi_2 = (1\ {-1}\ 1)$. Mit Lemma 117 wird

$$\begin{aligned}
\chi_2\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}(\mathrm{id}) &= \tfrac{|\mathrm{S}_4|}{|\mathrm{S}_3|}\,\chi_2(\mathrm{id}) = 4\\
\chi_2\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2)\in\mathrm{S}_3} \chi_2({}^{\rho_j}(1,2)) = -1+0+0+(-1) = -2\\
\chi_2\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2,3)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2,3)\in\mathrm{S}_3} \chi_2({}^{\rho_j}(1,2,3)) = 1+0+0+0 = 1\\
\chi_2\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2,3,4)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2,3,4)\in\mathrm{S}_3} \chi_2({}^{\rho_j}(1,2,3,4)) = 0+0+0+0 = 0\\
\chi_2\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2)(3,4)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2)(3,4)\in\mathrm{S}_3} \chi_2({}^{\rho_j}(1,2)(3,4)) = 0+0+0+0 = 0\,.
\end{aligned}$$

So ergibt sich $\chi_2\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4} = (4\ {-2}\ 1\ 0\ 0)$.

Es ist $\chi_3 = (2\ 0\ {-1})$. Mit Lemma 117 wird

$$\begin{aligned}
\chi_3\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}(\mathrm{id}) &= \tfrac{|\mathrm{S}_4|}{|\mathrm{S}_3|}\,\chi_3(\mathrm{id}) = 8\\
\chi_3\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2)\in\mathrm{S}_3} \chi_3({}^{\rho_j}(1,2)) = 0+0+0+0 = 0\\
\chi_3\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2,3)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2,3)\in\mathrm{S}_3} \chi_3({}^{\rho_j}(1,2,3)) = -1+0+0+0 = -1\\
\chi_3\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2,3,4)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2,3,4)\in\mathrm{S}_3} \chi_3({}^{\rho_j}(1,2,3,4)) = 0+0+0+0 = 0\\
\chi_3\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4}((1,2)(3,4)) &= \textstyle\sum_{j\in[1,4],\ \rho_j(1,2)(3,4)\in\mathrm{S}_3} \chi_3({}^{\rho_j}(1,2)(3,4)) = 0+0+0+0 = 0\,.
\end{aligned}$$

So ergibt sich $\chi_3\big\uparrow_{\mathrm{S}_3}^{\mathrm{S}_4} = (8\ 0\ {-1}\ 0\ 0)$.

(2) Wir haben den Gruppenmorphismus

$$\begin{array}{rcl}
\mathrm{S}_4 & \xrightarrow{\ f\ } & \mathrm{S}_3\\
(1,2) & \longmapsto & (1,2)\\
(2,3) & \longmapsto & (2,3)\\
(3,4) & \longmapsto & (1,2)
\end{array}$$

da $(1,2)^2 = \mathrm{id}$, $(2,3)^2 = \mathrm{id}$, $(1,2)^2 = \mathrm{id}$, $((1,2)\circ(2,3))^3 = \mathrm{id}$, $((2,3)\circ(1,2))^3 = \mathrm{id}$, $((1,2)\circ(1,2))^2 = \mathrm{id}$; cf. Aufgabe 9, Satz 24.

Es ist f surjektiv, da $\mathrm{S}_3 = \langle(1,2),\,(2,3)\rangle$.

Es wird

$$\begin{array}{rcl} \mathrm{S}_4 & \xrightarrow{f} & \mathrm{S}_3 \\ \mathrm{id} & \longmapsto & \mathrm{id} \\ (1,2) & \longmapsto & (1,2) \\ (1,2,3) & \longmapsto & (1,2,3) \\ (1,2,3,4) & \longmapsto & (1,3) \\ (1,2)(3,4) & \longmapsto & \mathrm{id} \end{array}$$

Da $\chi_3 = (\begin{smallmatrix} 2 & 0 & -1 \end{smallmatrix})$ ist, wird $\chi_3 \circ f = (\begin{smallmatrix} 2 & 0 & -1 & 0 & 2 \end{smallmatrix})$.

Nach Aufgabe 33.(4) ist $\chi_3 \circ f$ ein irreduzibler Charakter von S_4.

(3) Zur Unterscheidung schreiben wir nun die irreduziblen Charaktere von S_3 als $\chi_{3,i}$, wobei $i \in [1,3]$, die von S_4 als $\chi_{4,i}$, wobei $i \in [1,5]$.

Wir haben $\chi_{4,1} = (\begin{smallmatrix} 1 & 1 & 1 & 1 & 1 \end{smallmatrix})$ (trivialer Charakter).

Wir haben $\chi_{4,2} = (\begin{smallmatrix} 1 & -1 & 1 & -1 & 1 \end{smallmatrix})$ (zur Signumsdarstellung).

Diese beiden Charaktere χ_1^4 und χ_2^4 von S_4 sind in der Tat irreduzibel, da die zugehörigen Darstellungen eindimensional und damit einfach sind. Cf. Beispiel 39.(3).

Mit (1) ergibt sich

$$\mathrm{S}_4(\chi_{3,1}|_{\mathrm{S}_3}^{\mathrm{S}_4}, \chi_{4,1}) \;=\; \tfrac{1}{24}(1\cdot 4\cdot 1 + 6\cdot 2\cdot 1 + 8\cdot 1\cdot 1 + 6\cdot 0\cdot 1 + 3\cdot 0\cdot 1) \;=\; 1\,.$$

Also ist auch $\chi_{4,3} := \chi_{3,1}|_{\mathrm{S}_3}^{\mathrm{S}_4} - 1\cdot\chi_{4,1} = (\begin{smallmatrix} 3 & 1 & 0 & -1 & -1 \end{smallmatrix})$ noch ein Charakter von S_4; cf. Bemerkung 94.(1). Dieser ist in der Tat irreduzibel, da

$$\mathrm{S}_4(\chi_{4,3}, \chi_{4,3}) \;=\; \tfrac{1}{24}(1\cdot 3\cdot 3 + 6\cdot 1\cdot 1 + 8\cdot 0\cdot 0 + 6\cdot(-1)\cdot(-1) + 3\cdot(-1)\cdot(-1)) \;=\; 1\,;$$

cf. Bemerkung 94.(2).

Erstere Rechnung läßt sich noch zu

$$\mathrm{S}_4(\chi_{3,1}|_{\mathrm{S}_3}^{\mathrm{S}_4}, \chi_{4,1}) \overset{\text{L.1}20}{=} \mathrm{S}_3(\chi_{3,1}, \chi_{4,1}|_{\mathrm{S}_3}^{\mathrm{S}_4}) \;=\; \tfrac{1}{6}(1\cdot 1\cdot 1 + 3\cdot 1\cdot 1 + 2\cdot 1\cdot 1) \;=\; 1\,.$$

vereinfachen. Oder, ohne weitere Rechnung, es ist $\chi_{4,1}|_{\mathrm{S}_3}^{\mathrm{S}_4} = \chi_{3,1}$ irreduzibel, also ist das Resultat gleich 1 dank Bemerkung 94.(2).

Ferner ist $\chi_{4,4} := \chi_{4,3}\cdot\chi_{4,2} = (\begin{smallmatrix} 3 & 1 & 0 & -1 & -1 \end{smallmatrix})\cdot(\begin{smallmatrix} 1 & -1 & 1 & -1 & 1 \end{smallmatrix}) = (\begin{smallmatrix} 3 & -1 & 0 & 1 & -1 \end{smallmatrix})$ ein irreduzibler Charakter von S_4; cf. Aufgabe 33.(2).

Schließlich haben wir mit $\chi_{4,5} := \chi_{3,3} \circ f = (\begin{smallmatrix} 2 & 0 & -1 & 0 & 2 \end{smallmatrix})$ aus (2) gerade 5 paarweise verschiedene irreduzible Charaktere von S_4 gefunden, wie uns von der Anzahl der Konjugationsklassen vorgegeben war.

Somit ist

$$\mathrm{X}(\mathrm{S}_4) \;=\; \begin{array}{c} \\ \chi_{4,1} \\ \chi_{4,2} \\ \chi_{4,3} \\ \chi_{4,4} \\ \chi_{4,5} \end{array} \begin{array}{c} \begin{array}{ccccc} \mathrm{id} & (1,2) & (1,2,3) & (1,2,3,4) & (1,2)(3,4) \\ 1 & 6 & 8 & 6 & 3 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 3 & 1 & 0 & -1 & -1 \\ 3 & -1 & 0 & 1 & -1 \\ 2 & 0 & -1 & 0 & 2 \end{bmatrix} \end{array},$$

wobei direkt unter den Konjugationsklassenrepräsentanten die Länge ihrer Konjugationsklassen notiert wurde.

Hier noch ein alternativer Weg, um ohne (2) auf $\chi_{4,5}$ zu kommen.

Aus (1) haben wir noch den von $\chi_{3,3} = (\begin{smallmatrix}2&0&-1\end{smallmatrix})$ induzierten Charakter $\chi_{3,3}\uparrow_{S_3}^{S_4} = (\begin{smallmatrix}8&0&-1&0&0\end{smallmatrix})$.

Es ist $_{S_4}(\chi_{3,3}\uparrow_{S_3}^{S_4}, \chi_{4,3}) \overset{L.120}{=} {}_{S_3}(\chi_{3,3}, \chi_{4,3}\downarrow_{S_3}^{S_4}) = \frac{1}{6}(1\cdot 2\cdot 3 + 3\cdot 0\cdot 1 + 2\cdot(-1)\cdot 0) = 1$.

Es ist $_{S_4}(\chi_{3,3}\uparrow_{S_3}^{S_4}, \chi_{4,4}) \overset{L.120}{=} {}_{S_3}(\chi_{3,3}, \chi_{4,4}\downarrow_{S_3}^{S_4}) = \frac{1}{6}(1\cdot 2\cdot 3 + 3\cdot 0\cdot(-1) + 2\cdot(-1)\cdot 0) = 1$.

Also ist auch $\chi_{4,5} := \chi_{3,3}\uparrow_{S_3}^{S_4} - \chi_{4,3} - \chi_{4,4} = (\begin{smallmatrix}8&0&-1&0&0\end{smallmatrix}) - (\begin{smallmatrix}3&1&0&-1&-1\end{smallmatrix}) - (\begin{smallmatrix}3&-1&0&1&-1\end{smallmatrix}) = (\begin{smallmatrix}2&0&-1&0&2\end{smallmatrix})$ ein Charakter von S_4; cf. Bemerkung 94.(1). Dank

$$_{S_4}(\chi_{4,5}, \chi_{4,5}) = \tfrac{1}{24}(1\cdot 2\cdot 2 + 6\cdot 0\cdot 0 + 8\cdot(-1)\cdot(-1) + 6\cdot 0\cdot 0 + 3\cdot 2\cdot 2) = 1$$

ist $\chi_{4,5}$ in der Tat irreduzibel; cf. Bemerkung 94.(2).

Aufgabe 38

(1) Schreibe $H := C_G(m)$.

Lösung über Moduln.

Sei $\mathbf{C}$ der triviale $\mathbf{C}H$-Modul. Es genügt zu zeigen, daß $\mathbf{C}M$ und $\mathbf{C}G \underset{\mathbf{C}C_G(m)}{\otimes} \mathbf{C}$ isomorphe $\mathbf{C}G$-Moduln sind; cf. Bemerkung 74, Definition 116.

Wir haben die $\mathbf{C}H$-lineare Abbildung $\mathbf{C} \longrightarrow M$, $1 \longmapsto m$, da $hm = m$ für $h \in H$.

Aufgabe 31.(2, 4) macht hieraus die $\mathbf{C}G$-lineare Abbildung

$$\begin{array}{ccccc} \mathbf{C}G & \underset{\mathbf{C}H}{\otimes} & \mathbf{C} & \longrightarrow & \mathbf{C}M \\ g & \otimes & 1 & \longmapsto & gm\,, \end{array}$$

deren Existenz man auch direkt einsehen kann.

Da M transitiv ist, ist diese Abbildung surjektiv. Da zudem

$$\dim_{\mathbf{C}}(\mathbf{C}G \underset{\mathbf{C}H}{\otimes} \mathbf{C}) \overset{L.117}{=} |G|/|H| \overset{L.5}{=} |M| = \dim_{\mathbf{C}}(\mathbf{C}M)$$

ist, ist die Abbildung bijektiv.

Lösung über Charaktere.

Sei ψ_1 der triviale Charakter von H. Sei $g \in G$ gegeben.

Es ist $\chi_{\mathbf{C}M}(g) = |\{\, m \in M \,:\, gm = m \,\}|$; cf. Beispiel 73.(3).

Es ist

$$\begin{array}{rcl} \psi_1\uparrow_H^G(g) & \overset{L.117}{=} & \frac{1}{|H|}\sum_{x\in G,\ {}^xg\in H} \psi_1({}^xg) \\ & = & \frac{1}{|H|}\sum_{x\in G,\ {}^xg\in H} 1 \\ & = & \frac{1}{|H|}|\{\, x\in G \,:\, {}^xg \in H\,\}| \\ & = & \frac{1}{|H|}|\{\, x\in G \,:\, gx^-H = x^-H\,\}| \\ & = & \frac{1}{|H|}|\{\, x\in G \,:\, g(xH) = xH\,\}| \\ & = & |\{\, xH \in G/H \,:\, g(xH) = xH\,\}| \\ & \overset{L.5}{=} & |\{\, m\in M \,:\, gm = m\,\}| \\ & = & \chi_{\mathbf{C}M}(g)\,. \end{array}$$

(2) Sei $m \in M$. Sei ψ_1 der triviale Charakter von $H := C_G(m)$. Es wird

$$\begin{array}{rcl} {}_G(\chi_{\mathbf{C}M}, \chi_1) & \overset{(1)}{=} & {}_G(\psi_1\uparrow_H^G, \chi_1) \\ & \overset{L.120}{=} & {}_H(\psi_1, \chi_1\downarrow_H^G) \\ & = & {}_H(\psi_1, \psi_1) \\ & = & 1\,. \end{array}$$

(3) Sowohl die Anzahl der Bahnen als auch der Wert von $\frac{1}{|G|}\sum_{g\in G}|\{\, m\in M\,:\, gm=m\,\}|$ sind additiv bezüglich disjunkter Vereinigungen von G-Mengen. Somit ist o.E. M transitiv; cf. Bemerkung 6.

Zu zeigen ist, daß $1 \stackrel{!}{=} \frac{1}{|G|}\sum_{g\in G}|\{\, m\in M\,:\, gm=m\,\}|$.

Es wird

$$1 \stackrel{(2)}{=} {}_G(\chi_{\mathbf{C}M}\,,\chi_1) \;=\; \tfrac{1}{|G|}\textstyle\sum_{g\in G}\chi_{\mathbf{C}M}(g)\,\underbrace{\overline{\chi_1(g)}}_{=1} \stackrel{\text{B. 73.(3)}}{=} \tfrac{1}{|G|}\textstyle\sum_{g\in G}|\{\, m\in M\,:\, gm=m\,\}|\;.$$

(4) Sei χ_1 der triviale Charakter von G. Es tritt χ_1 mit Multiplizität 1 in $\chi_{\mathbf{C}M}$ auf; cf. Lösung zu (2). Also ist $\varphi := \chi_{\mathbf{C}M} - \chi_1$ ein Charakter von G. Zu zeigen ist, daß φ irreduzibel ist. Zu zeigen ist also, daß ${}_G(\varphi,\varphi) \stackrel{!}{=} 1$; cf. Bemerkung 94.(2).

Es ist

$$\begin{aligned} {}_G(\varphi,\varphi) &= {}_G(\chi_{\mathbf{C}M}-\chi_1\,,\chi_{\mathbf{C}M}-\chi_1)\\ &= {}_G(\chi_{\mathbf{C}M}\,,\chi_{\mathbf{C}M}) - 2\,{}_G(\chi_{\mathbf{C}M}\,,\chi_1) + {}_G(\chi_1\,,\chi_1)\\ &\stackrel{(2)}{=} {}_G(\chi_{\mathbf{C}M}\,,\chi_{\mathbf{C}M}) - 1\;. \end{aligned}$$

Zu zeigen ist also, daß ${}_G(\chi_{\mathbf{C}M}\,,\chi_{\mathbf{C}M}) \stackrel{!}{=} 2$.

Sei $m\in M$ so, daß $M\smallsetminus\{m\}$ eine transitive $H := \mathrm{C}_G(m)$-Menge ist. Sei ψ_1 der triviale Charakter von H. Es wird

$$\begin{aligned} {}_G(\chi_{\mathbf{C}M}\,,\chi_{\mathbf{C}M}) &\stackrel{(1)}{=} {}_G(\psi_1\uparrow^G_H\,,\chi_{\mathbf{C}M})\\ &\stackrel{\text{L. }120}{=} {}_H(\psi_1\,,\chi_{\mathbf{C}M}\downarrow^G_H)\\ &= {}_H(\psi_1\,,(\varphi+\chi_1)\downarrow^G_H)\\ &= {}_H(\psi_1\,,\varphi\downarrow^G_H+\psi_1)\\ &= {}_H(\psi_1\,,\varphi\downarrow^G_H)+1\;. \end{aligned}$$

Zu zeigen ist also, daß ${}_G(\psi_1\,,\varphi\downarrow^G_H) \stackrel{!}{=} 1$.

Es ist $M = \{m\}\sqcup(M\smallsetminus\{m\})$ eine Zerlegung in H-Mengen.

Als $\mathbf{C}H$-Moduln ist also $\mathbf{C}M = \mathbf{C}\{m\}\oplus\mathbf{C}(M\smallsetminus\{m\})$ zerlegt, wobei H auf m und damit auch auf $\mathbf{C}\{m\}$ trivial operiert.

Somit ist auch der zu M gehörige Charakter $\chi_{\mathbf{C}M}\downarrow^G_H$ von H die Summe aus dem trivialen Charakter ψ_1 von H und dem zu $\mathbf{C}(M\smallsetminus\{m\})$ gehörigen Charakter von H; cf. Bemerkung 75.

Nun ist aber der zu M gehörige Charakter $\chi_{\mathbf{C}M}\downarrow^G_H$ auch Summe von ψ_1 und $\varphi\downarrow^G_H$.

Ein Vergleich zeigt, daß $\varphi\downarrow^G_H$ der zu $\mathbf{C}(M\smallsetminus\{m\})$ gehörige Charakter von H ist.

Da nach Voraussetzung $\mathbf{C}(M\smallsetminus\{m\})$ eine transitive H-Menge ist, folgt daher mit (2), daß in der Tat

$${}_G(\psi_1\,,\varphi\downarrow^G_H) \;=\; 1$$

ist.

Sei M eine transitive G-Menge.

Via $g(m,m') := (gm,gm')$ für $g\in G$ und $m,\,m'\in M$ wird $M\times M$ zu einer G-Menge.

Sei $\Delta M := \{\,(m,m)\,:\,m\in M\,\}\subseteq M\times M$. Es ist $M\times M = \Delta M\sqcup(M\times M\smallsetminus\Delta M)$ eine Zerlegung in G-Mengen.

Wir *behaupten,* daß M genau dann doppelt transitiv ist, wenn $M\times M\smallsetminus\Delta M$ transitiv ist.

Sei zum einen $M\times M\smallsetminus\Delta M$ transitiv. Sei $m\in M$. Sind $x,\,x'\in M\smallsetminus\{m\}$ vorgegeben, so gibt es ein $g\in G$ mit $(x',m) = (gx,gm)$. Also ist $g\in\mathrm{C}_G(m)$ mit $gx = x'$ gefunden.

Existiere umgekehrt $m\in M$ so, daß $M\smallsetminus\{m\}$ eine transitive $\mathrm{C}_G(m)$-Menge ist. Wähle $m'\in M\smallsetminus\{m\}$. Sei $(x,x')\in M\times M\smallsetminus\Delta M$ gegeben. Da M transitiv ist, gibt es ein $g\in G$ mit $gm = x$. Da $g^-x'\neq$

$g^- x = m$, gibt es ein $u \in \mathrm{C}_G(m)$ mit $um' = g^- x'$. Es wird $gu(m, m') = (gum, gum') = (gm, gg^- x') = (x, x')$.

Dies zeigt die *Behauptung.*

Diese äquivalente Charakterisierung zeigt, daß die Wahl von m in der Definition der doppelten Transitivität keine Rolle spielt.

Aufgabe 39.

Schreibe $z = x + \mathrm{i}y$ mit $x, y \in \mathbf{R}$. Es wird

$$0 \;=\; |z + r|^2 - (|z| + r)^2 \;=\; ((x + r)^2 + y^2) - (x^2 + y^2 + 2|z|r + r^2) \;=\; 2(x - |z|)r \;,$$

i.e. $x = |z|$.

Es folgt

$$x^2 \;=\; |z|^2 \;=\; x^2 + y^2 \;,$$

also $y = 0$.

Ferner ist $x = |z| \in \mathbf{R}_{\geqslant 0}$.

Insgesamt ist $z = x + \mathrm{i}y \in \mathbf{R}_{\geqslant 0}$.

Alternativ kann man mit Cauchy-Schwarz argumentieren.

Aufgabe 40

(1) Wir wollen zeigen, daß Γ eine linear unabhängige Teilmenge des L-Vektorraums $\mathrm{Hom}_K(L, L)$ ist.

Annahme nicht. Sei $m \in \mathbf{Z}_{\geqslant 1}$ minimal so, daß es $\lambda_i \in L$ und paarweise verschiedene $\gamma_i \in \Gamma$ für $i \in [1, m]$ gibt mit $\sum_{i\in[1,m]} \lambda_i\gamma_i = 0$, aber $\lambda_j \neq 0$ für ein $j \in [1, m]$.

Wegen Minimalität ist $\lambda_i \neq 0$ für alle $i \in [1, m]$.

Da $\gamma_1(1) = 1$ ist, ist $\gamma_1 \neq 0$ und also $m \geqslant 2$.

Es ist $\gamma_1 \neq \gamma_2$. Sei $x \in L$ so gewählt, daß $\gamma_1(x) \neq \gamma_2(x)$.

Es wird

$$\sum_{i\in[1,m]} \lambda_i\gamma_i(z) \;=\; 0$$

für $z \in L$. Also ist

$$\begin{array}{rcccl} 0 & = & \sum_{i\in[1,m]} \lambda_i\gamma_i(xy) & = & \sum_{i\in[1,m]} \lambda_i\gamma_i(x)\gamma_i(y) \\ 0 & = & (\sum_{i\in[1,m]} \lambda_i\gamma_i(y))\gamma_1(x) & = & \sum_{i\in[1,m]} \lambda_i\gamma_1(x)\gamma_i(y) \end{array}$$

für $y \in L$. Als Differenz erhalten wir

$$0 \;=\; \sum_{i\in[2,m]} \lambda_i(\gamma_i(x) - \gamma_1(x))\gamma_i(y) \;=\; 0$$

für $y \in L$, i.e.

$$0 \;=\; \sum_{i\in[2,m]} \lambda_i(\gamma_i(x) - \gamma_1(x))\gamma_i \;=\; 0$$

Da $\lambda_2(\gamma_2(x) - \gamma_1(x)) \neq 0$ ist, ist das ein *Widerspruch* zur angenommenen Minimalität. Also ist Γ linear unabhängig.

Ist nun L endlichdimensional über K, so ist auch $\dim_L \mathrm{Hom}_K(L, L) = \dim_K L =: n$. Denn ist $(x_1, \ldots, x_n)$ eine K-lineare Basis von L, so ist $(\, (x_i \mapsto \partial_{j,i}) \,:\, j \in [1, n]\,)$ eine L-lineare Basis von $\mathrm{Hom}_K(L, L)$. Da Γ eine linear unabhängige Teilmenge des L-Vektorraums ist, folgt $|\Gamma| \leqslant n$.

Diese lineare Unabhängigkeit von Γ ist als *Dedekindsches Lemma* bekannt.

(2) Es wurde $\Phi_n(X) \in \mathbf{Q}(X)$ gebildet.

(i) Um zu zeigen, daß $\Phi_n(X) \in \mathbf{Z}[X]$ liegt und $\Phi_n(X) = \prod_{i\in[1,n-1],\,\mathrm{ggT}(i,n)=1}(X-\zeta^i)$ (gebildet in $\mathbf{C}[X]$) ist für $n \in \mathbf{Z}_{\geqslant 1}$, verwenden wir Induktion nach n.
Sei $n \in \mathbf{Z}_{\geqslant 1}$. Beachte, daß $\zeta_{n/d} = \zeta_n^d = \zeta^d$ für $d \,|\, n$. Es wird

$$\begin{aligned}
\Phi_n(X) &= \frac{X^n-1}{\prod_{d\,|\,n,\ d\neq n}\Phi_d(X)} \\
&= \frac{X^n-1}{\prod_{d\,|\,n,\ d\neq 1}\Phi_{n/d}(X)} \\
&= \frac{\prod_{i\in[0,n-1]}(X-\zeta^i)}{\prod_{d\,|\,n,\ d\neq 1}\prod_{i\in[0,n/d-1],\,\mathrm{ggT}(i,n/d)\,=\,1}(X-\zeta^{id})} \\
&= \frac{\prod_{i\in[0,n-1]}(X-\zeta^i)}{\prod_{d\,|\,n,\ d\neq 1}\prod_{i\in[0,n-1],\,\mathrm{ggT}(i,n)\,=\,d}(X-\zeta^i)} \\
&= \frac{\prod_{i\in[0,n-1]}(X-\zeta^i)}{\prod_{i\in[0,n-1],\,\mathrm{ggT}(i,n)\,\neq\,1}(X-\zeta^i)} \\
&= \prod_{i\in[0,n-1],\,\mathrm{ggT}(i,n)=1}(X-\zeta^i)\ .
\end{aligned}$$

Insbesondere ist $\Phi_n(X) \in \mathbf{C}[X]$. Bleibt zu zeigen, daß $\Phi_n(X) \overset{!}{\in} \mathbf{Z}[X]$ ist.
Annahme, nicht. Schreibe $\Phi_n(X) =: \sum_{k\geqslant 0} z_k\, X^k$. Sei $\hat{k} \geqslant 0$ maximal mit $z_{\hat{k}} \in \mathbf{C} \smallsetminus \mathbf{Z}$.
Schreibe $\prod_{d\,|\,n,\ d\neq n}\Phi_d(X) =: f(X) = \sum_{\ell\geqslant 0} w_\ell\, X^\ell \in \mathbf{Z}[X]$, was nach Induktionsvoraussetzung möglich ist. Sei $\hat{\ell} := \deg f$. Es ist $w_{\hat{\ell}} = 1$.
Es ist der Koeffizient von $X^{\hat{k}+\hat{\ell}}$ in $\Phi_n(X)f(X)$ gleich

$$\textstyle\sum_{\ell\in[0,\hat{\ell}]} z_{\hat{k}+\hat{\ell}-\ell}\, w_\ell \;=\; z_{\hat{k}} + \underbrace{\sum_{\ell\in[0,\hat{\ell}-1]} z_{\hat{k}+\hat{\ell}-\ell}\, w_\ell}_{\in\,\mathbf{Z}} \;\notin\; \mathbf{Z}\ .$$

Aber es ist $\Phi_n(X)f(X) = X^n - 1 \in \mathbf{Z}[X]$. Wir haben einen *Widerspruch.*

(ii) *Vorbemerkung: Gaußsches Lemma.* Sei $a(X) \in \mathbf{Z}[X]$ normiert. Sei $b(X) \in \mathbf{Q}[X]$ ein Teiler von $a(X)$ in $\mathbf{Q}[X]$. Die Nullstellen von $b(X)$ in $\mathbf{C}$ sind auch Nullstellen von $a(X)$, liegen also in $\mathcal{O}$. Es folgt $b(X) \in \mathbf{Q}[X] \cap \mathcal{O}[X] = \mathbf{Z}[X]$; cf. Aufgabe 29.(3).
Wir wollen zeigen, daß $\Phi_n(X)$ in $\mathbf{Q}[X]$ irreduzibel ist.
Annahme, nicht. Sei $\Phi_n(X) = u(X)v(X)$ mit $u,\, v \in \mathbf{Q}[X]$ normiert und $\deg u,\, \deg v \geqslant 1$. Es sind $u(X),\, v(X) \in \mathbf{Z}[X]$; cf. Vorbemerkung.
Sei $\xi \in \mathbf{C}$ eine Nullstelle von $u(X)$. Da ξ auch eine Nullstelle von $\Phi_n(X)$ ist, folgt $\xi = \zeta^i$ für ein $i \in [0, n-1]$ mit $\mathrm{ggT}(i,n) = 1$.
Sei $j \in [0, n-1]$ mit $\mathrm{ggT}(j,n) = 1$. Es gibt ein $a \in \mathbf{Z}$ mit $\mathrm{ggT}(a,n) = 1$ und $ia \equiv_n j$, für welches dann auch $\zeta^{ia} = \zeta^j$ ist.
Können wir also zeigen, daß mit ξ auch ξ^a eine Nullstelle von $u(X)$ ist für alle $a \in \mathbf{Z}$ teilerfremd zu n, so haben wir gezeigt, daß jede Nullstelle von $\Phi_n(X)$ auch Nullstelle von $u(X)$ ist, daß also $u(X) = \Phi_n(X)$ und $v(X) = 1$ ist, und wir sind an einen *Widerspruch* angelangt.
Sei p eine Primzahl teilerfremd zu n. Es genügt zu zeigen, daß mit ξ auch ξ^p eine Nullstelle von $u(X)$ ist.

Annahme, nicht. Dann ist ξ^p eine Nullstelle von $v(X)$, i.e. ξ ist eine Nullstelle von $v(X^p)$. Also ist $(X-\xi)$ ein gemeinsamer Teiler von $u(X)$ und $v(X^p)$ in $\mathbf{C}[X]$. Der Euklidsche Algorithmus in $\mathbf{C}[X]$, ausgeführt innerhalb $\mathbf{Q}[X]$, darf also nicht $\mathrm{ggT}(u(X), v(X^p)) = 1$ liefern. Sei $g(X) := \mathrm{ggT}(u(X), v(X^p)) \in \mathbf{Q}[X]$ (als normiert vereinbart); es ist $\deg g \geqslant 1$. Es ist $g(X) \in \mathbf{Z}[X]$; cf. Vorbemerkung.

Schreibe $u(X) = r(X)\, g(X)$ und $v(X^p) = s(X)\, g(X)$ mit $r(X)$, $s(X) \in \mathbf{Z}[X]$; cf. Vorbemerkung.

Wir bilden alles nach $\mathbf{F}_p[X]$ ab, ohne Änderung der Bezeichnungen.

Sei $\gamma(X) \in \mathbf{F}_p[X]$ ein normierter irreduzibler Teiler von $g(X)$. Dann ist $\gamma(X)$ ein Teiler von $u(X)$ in $\mathbf{F}_p[X]$. Ferner ist $\gamma(X)$ ein Teiler von $v(X^p) = v(X)^p$ in $\mathbf{F}_p[X]$. Also ist $\gamma(X)$ auch ein Teiler von $v(X)$. Insgesamt ist $\gamma(X)^2$ ein Teiler von $u(X)v(X) = \Phi_n(X)$. Somit ist $\gamma(X)^2$ auch ein Teiler von $X^n - 1$. Schreibe $X^n - 1 = \gamma(X)^2\, \delta(X)$ für ein $\delta(X) \in \mathbf{F}_p[X]$. In $\mathbf{F}_p[X]$ wird

$$nX^{n-1} \;=\; (X^n-1)' \;=\; (\gamma(X)^2\, \delta(X))' \;=\; 2\gamma(X)\, \gamma'(X)\, \delta(X) + \gamma(X)^2\, \delta(X)\,.$$

(formale Ableitung in $\mathbf{F}_p[X]$). Da $\gamma(X)$ die rechte Seite teilt, folgt, daß es auch die linke Seite teilt. Da $n \not\equiv_p 0$ ist, folgt $\gamma(X) = X$, und somit $0 = \gamma(0)^2\, \delta(0) = 0^n - 1 = -1$ in $\mathbf{F}_p$. Wir haben einen **Widerspruch.**

(iii) Sei Γ die Menge aller $\mathbf{Q}$-Algebrenmorphismen von $\mathbf{Q}(\zeta)$ nach $\mathbf{Q}(\zeta)$.

Sei $i \in [0, n-1]$ mit $\mathrm{ggT}(i, n) = 1$ gegeben.

Da $\Phi_n(\zeta^i) = 0$ gemäß (1), haben wir einen $\mathbf{Q}$-Algebrenmorphismus

$$\begin{array}{ccc} \mathbf{Q}[X]/(\Phi_n(X)) & \xrightarrow{f_i} & \mathbf{Q}(\zeta) \\ X + (\Phi_n(X)) & \longmapsto & \zeta^i \end{array}$$

Es ist f_i ist surjektiv, da mit ζ^i auch alle anderen Potenzen von ζ im Bild liegen.

Es ist f_i injektiv, da $\Phi_n(X)$ dank (ii) irreduzibel ist und also $\mathbf{Q}[X]/(\Phi_n(X))$ ein Körper ist, und da $\mathbf{Q}(\zeta)$ nicht der Nullring ist.

Es ist $f_i \circ f_1^{-1} : \mathbf{Q}(\zeta) \xrightarrow{\sim} \mathbf{Q}(\zeta)$ ein Isomorphismus von $\mathbf{Q}$-Algebren, der ζ nach ζ^i abbildet.

Also ist $|\Gamma| \geqslant \deg \Phi_n(X)$.

Sei $K := \{\, z \in \mathbf{Q}(\zeta) \,:\, \text{für } \sigma \in \Gamma \text{ ist } \sigma(z) = z \,\}$. Es ist $\mathbf{Q} \subseteq K \subseteq \mathbf{Q}(\zeta)$.

Es ist $K \subseteq \mathbf{Q}(\zeta)$ ein Teilring, da jedes $\sigma \in \Gamma$ ein Ringmorphismus ist.

Wegen $\mathbf{Q} \subseteq K$ ist K eine endlichdimensionale $\mathbf{Q}$-Algebra. Da K zudem ein Integritätsbereich ist, ist K ein Körper.

Es ist $\dim_{\mathbf{Q}} \mathbf{Q}(\zeta) = (\dim_{\mathbf{Q}} K)(\dim_K \mathbf{Q}(\zeta))$, da eine $\mathbf{Q}$-lineare Basis $(\, x_i \,:\, i \in [1,u]\,)$ von K und eine K-lineare Basis $(\, y_j \,:\, j \in [1,v]\,)$ von $\mathbf{Q}(\zeta)$ die $\mathbf{Q}$-lineare Basis $(\, x_i\, y_j \,:\, i \in [1,u],\ j \in [1,v]\,)$ von $\mathbf{Q}(\zeta)$ geben.

Es ist $\dim_{\mathbf{Q}} \mathbf{Q}(\zeta) = \dim_{\mathbf{Q}}(\mathbf{Q}[X]/(\Phi_n(X))) = \deg \Phi_n(X)$.

Es ist $\mathbf{Q}(\zeta)$ eine K-Algebra. Es besteht Γ aus K-Algebrenmorphismen. Also ist $|\Gamma| \leqslant \dim_K \mathbf{Q}(\zeta)$; cf. (1).

Insgesamt ist

$$\deg \Phi_n(X) \;=\; \dim_{\mathbf{Q}} \mathbf{Q}(\zeta) \;=\; (\dim_{\mathbf{Q}} K)(\dim_K \mathbf{Q}(\zeta)) \;\geqslant\; (\dim_{\mathbf{Q}} K)|\Gamma| \geqslant (\dim_{\mathbf{Q}} K)(\deg \Phi_n(X))\,.$$

Es folgt $\dim_{\mathbf{Q}} K = 1$, also $K = \mathbf{Q}$.

Aufgabe 41

(1) Sei $(g,h) \in G \times H$. Sei $\chi = \chi_M$ für einen $\mathbf{C}G$-Modul M. Sei $\psi = \chi_N$ für einen $\mathbf{C}H$-Modul N.
Wir haben die wohldefinierte und $\mathbf{C}$-lineare Abbildung

$$\begin{array}{ccccc} M & \otimes & N & \xrightarrow{\rho((g,h))} & M & \otimes & N \\ m & \otimes & n & \longmapsto & (gm) & \otimes & (hn)\,. \end{array}$$

Es ist $\rho((g,h))\rho((g^-,h^-)) = \mathrm{id}_{M\otimes N}$, und also $\rho((g,h)) \in \mathrm{GL}(M \otimes N)$.
Es ist $\rho((g,h))\rho((\tilde{g},\tilde{h})) = \rho((g\tilde{g},h\tilde{h}))$ für (g,h), $(\tilde{g},\tilde{h}) \in G \times H$, und also

$$\begin{array}{ccccccc} \rho & : & G & \times & H & \longrightarrow & \mathrm{GL}(M \otimes N) \\ & & (g & , & h) & \longmapsto & \big(\rho((g,h)) : m \otimes n \mapsto (gm) \otimes (hn)\big) \end{array}$$

eine Darstellung von $G \times H$.

Nennen wir diese das *äußere Tensorprodukt* von M und N und schreiben den zugehörigen $\mathbf{C}(G \times H)$-Modul $M \boxtimes N$. Als $\mathbf{C}$-Vektorraum ist also $M \boxtimes N = M \otimes N$, und dieser wird ausgestattet mit der zu ρ gehörigen $\mathbf{C}(G \times H)$-Modulstruktur.

Ferner sei $\chi \boxdot \psi := \chi_{M\boxtimes N}$ das *äußere Produkt* von χ und ψ.

Berechnen wir $\chi \boxdot \psi = \chi_{M\boxtimes N}$ ausgehend von χ und ψ.

Sei $(m_1 \ldots, m_k)$ eine $\mathbf{C}$-lineare Basis von M. Sei $(n_1 \ldots, n_\ell)$ eine $\mathbf{C}$-lineare Basis von N.

Es ist $(\, m_i \otimes n_j \,:\, i \in [1,k],\ j \in [1,\ell]\,)$ eine Basis von $M \otimes N$.

Sei $(g,h) \in G \times H$. Sei $i \in [1,k]$. Sei $j \in [1,\ell]$.

Sei $gm_i = \sum_a z_{a,i}\, m_a$ mit $z_{a,i} \in \mathbf{C}$ stets. Sei $hn_j = \sum_b w_{b,j}\, n_b$ mit $w_{b,j} \in \mathbf{C}$ stets.

Es wird

$$(g,h)(m_i \otimes n_j) \;=\; (gm_i) \otimes (hn_j) \;=\; \textstyle\sum_{a,b} z_{a,i}\, w_{b,j}\, m_a \otimes n_b\,.$$

Somit wird der Beitrag des Basiselements $m_i \otimes n_j$ zur Spur von $\rho((g,h))$ gleich $z_{i,i}\, w_{j,j}$. Insgesamt wird

$$(\chi \boxdot \psi)(g,h) = \chi_{M\boxtimes N}(g,h) \;=\; \textstyle\sum_{i,j} z_{i,i}\, w_{j,j} \;=\; (\sum_i z_{i,i})(\sum_j w_{j,j}) \;=\; \chi(g) \cdot \psi(h)\,,$$

wie in der Aufgabenstellung vorgegeben.

> Betrachten wir einmal den Fall $G = H$.
> Wir erhalten den $\mathbf{C}G$-Modul $M \otimes N$ aus dem $\mathbf{C}(G \times G)$-Modul $M \boxtimes N$ durch Restriktion entlang der *Diagonalen* $\Delta : G \to G \times G$, $g \mapsto (g,g)$; cf. Lemma 110.
> Entsprechend erhalten wir $\chi \cdot \psi = (\chi \boxdot \psi) \circ \Delta$; cf. Bemerkung 113.

(2) Es wird

$$\begin{array}{rcl} {}_{G\times H}(\chi \boxdot \psi,\, \tilde{\chi} \boxdot \tilde{\psi}) & = & \sum_{(g,h)} (\chi \boxdot \psi)(g,h)\, \overline{(\tilde{\chi} \boxdot \tilde{\psi})(g,h)} \\ & = & \sum_{(g,h)} \chi(g)\, \psi(h)\, \overline{\tilde{\chi}(g)\, \tilde{\psi}(h)} \\ & = & (\sum_g \chi(g)\, \overline{\tilde{\chi}(g)})(\sum_h \psi(h)\, \overline{\tilde{\psi}(h)}) \\ & = & {}_G(\chi,\chi) \cdot {}_H(\psi,\psi)\,. \end{array}$$

(3) Da das Skalarprodukt auf Charakteren Werte in $\mathbf{Z}_{\geqslant 0}$ annimmt, folgt aus (2), daß genau dann ${}_{G\times H}(\chi \boxdot \psi,\, \chi \boxdot \psi) = 1$ gilt, wenn ${}_G(\chi,\chi) = 1$ und ${}_H(\psi,\psi) = 1$ ist; cf. Bemerkung 95.(1).

Daraus folgt wiederum, daß $\chi \boxdot \psi$ genau dann ein einfacher Charakter von $G \times H$ ist, wenn χ ein einfacher Charakter von G und ψ ein einfacher Charakter von H ist; cf. Bemerkung 94.(2).

(4) Seien $\chi_1 \ \ldots, \chi_t$ die verschiedenen irreduziblen Charaktere von G, und sei $G = \bigsqcup_{s\in[1,t]} {}^{G}g_s$.
Seien $\psi_1 \ \ldots, \psi_v$ die verschiedenen irreduziblen Charaktere von H, und sei $H = \bigsqcup_{u\in[1,v]} {}^{H}h_u$.
Es ist

$$\begin{aligned} G \times H &= (\bigsqcup_{s\in[1,t]} {}^{G}g_s) \times (\bigsqcup_{u\in[1,v]} {}^{H}h_u) \\ &= \bigsqcup_{s\in[1,t],\ u\in[1,v]} ({}^{G}g_s \times {}^{H}h_u) \\ &= \bigsqcup_{s\in[1,t],\ u\in[1,v]} {}^{G\times H}(g_s\,, h_u)\ . \end{aligned}$$

Also gibt es auch $t \cdot v$ verschiedene irreduzible Charaktere von $G \times H$; cf. Lemma 84.
Für $s,\ \tilde{s} \in [1,t]$ und $u,\ \tilde{u} \in [1,v]$ ist

$$ {}_{G\times H}(\chi_s \boxdot \psi_u\,,\ \chi_{\tilde{s}} \boxdot \psi_{\tilde{u}}) \overset{(2)}{=} {}_{G}(\chi_s\,, \chi_{\tilde{s}}) \cdot {}_{H}(\psi_u\,, \psi_{\tilde{u}}) \ = \ \partial_{s,\tilde{s}}\, \partial_{u,\tilde{u}} \ = \ \partial_{(s,u),(\tilde{s},\tilde{u})}\ . $$

Also sind die $t\cdot v$ irreduziblen Charaktere in $(\ \chi_s \boxtimes \psi_u \ :\ s \in [1,t],\ u \in [1,v]\ )$ paarweise verschieden; cf. (3). Somit taucht jeder irreduzible Charakter von $G \times H$ in dieser Liste auf.

(5) Schreibe $\zeta := \zeta_3$.
Die Charaktertafel von S_3 ist gegeben durch

$$\mathrm{X}(\mathrm{S}_3) \ = \ \begin{array}{c} \\ \\ \chi_1 \\ \chi_2 \\ \chi_3 \end{array} \begin{array}{c} \begin{array}{ccc} \mathrm{id} & (1,2) & (1,2,3) \\ 1 & 3 & 2 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & 0 & -1 \end{bmatrix} \end{array} ,$$

wobei direkt unter den Konjugationsklassenrepräsentanten die Länge ihrer Konjugationsklassen notiert wurde; cf. Beispiel 93.(1).
Die Charaktertafel von $\mathrm{C}_3 = \langle\, a \ :\ a^3 \,\rangle$ ist gegeben durch

$$\mathrm{X}(\mathrm{C}_3) \ = \ \begin{array}{c} \\ \\ \psi_1 \\ \psi_2 \\ \psi_3 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & a & a^2 \\ 1 & 1 & 1 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{bmatrix} \end{array} ,$$

wobei direkt unter den Konjugationsklassenrepräsentanten die Länge ihrer Konjugationsklassen notiert wurde; cf. Beispiel 93.(2).
Gemäß (4) und Lösung dazu ergibt sich folgende Charaktertafel von $\mathrm{S}_3 \times \mathrm{C}_3$.

$$\mathrm{X}(\mathrm{S}_3{\times}\mathrm{C}_3) \ = \ \begin{array}{c} \\ \chi_1 \boxtimes \psi_1 \\ \chi_2 \boxtimes \psi_1 \\ \chi_3 \boxtimes \psi_1 \\ \chi_1 \boxtimes \psi_2 \\ \chi_2 \boxtimes \psi_2 \\ \chi_3 \boxtimes \psi_2 \\ \chi_1 \boxtimes \psi_3 \\ \chi_2 \boxtimes \psi_3 \\ \chi_3 \boxtimes \psi_3 \end{array} \begin{array}{c} \begin{array}{ccccccccc} {\scriptstyle (\mathrm{id},1)} & {\scriptstyle ((1,2),1)} & {\scriptstyle ((1,2,3),1)} & {\scriptstyle (\mathrm{id},a)} & {\scriptstyle ((1,2),a)} & {\scriptstyle ((1,2,3),a)} & {\scriptstyle (\mathrm{id},a^2)} & {\scriptstyle ((1,2),a^2)} & {\scriptstyle ((1,2,3),a^2)} \\ 1 & 3 & 2 & 1 & 3 & 2 & 1 & 3 & 2 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 2 & 0 & -1 & 2 & 0 & -1 & 2 & 0 & -1 \\ 1 & 1 & 1 & \zeta & \zeta & \zeta & \zeta^2 & \zeta^2 & \zeta^2 \\ 1 & -1 & 1 & \zeta & -\zeta & \zeta & \zeta^2 & -\zeta^2 & \zeta^2 \\ 2 & 0 & -1 & 2\zeta & 0 & -\zeta & 2\zeta^2 & 0 & -\zeta^2 \\ 1 & 1 & 1 & \zeta^2 & \zeta^2 & \zeta^2 & \zeta & \zeta & \zeta \\ 1 & -1 & 1 & \zeta^2 & -\zeta^2 & \zeta^2 & \zeta & -\zeta & \zeta \\ 2 & 0 & -1 & 2\zeta^2 & 0 & -\zeta^2 & 2\zeta & 0 & -\zeta \end{bmatrix} \end{array} ,$$

wobei direkt unter den Konjugationsklassenrepräsentanten die Länge ihrer Konjugationsklassen notiert wurde.

Aufgabe 42

(1) Es ist $\mathrm{S}^2M \subseteq M \otimes M$ ein $\mathbf{C}G$-Teilmodul, da für $m,\, m' \in M$ und $g \in G$ der $\mathbf{C}$-lineare Erzeuger $m \otimes m' + m' \otimes m$ von S^2M unter Multiplikation mit g auf

$$g(m \otimes m' + m' \otimes m) \;=\; (gm) \otimes (gm') + (gm') \otimes (gm) \;\in\; \mathrm{S}^2M$$

abgebildet wird.

Es ist $\Lambda^2M \subseteq M \otimes M$ ein $\mathbf{C}G$-Teilmodul, da für $m,\, m' \in M$ und $g \in G$ der $\mathbf{C}$-lineare Erzeuger $m \otimes m' - m' \otimes m$ von Λ^2M unter Multiplikation mit g auf

$$g(m \otimes m' - m' \otimes m) \;=\; (gm) \otimes (gm') - (gm') \otimes (gm) \;\in\; \mathrm{S}^2M$$

abgebildet wird.

Es ist $M \otimes M = \mathrm{S}^2M + \Lambda^2M$, da für $m,\, m' \in M$ der $\mathbf{C}$-lineare Erzeuger $m \otimes m'$ von $M \otimes M$ in der rechten Seite enthalten ist wegen

$$m \otimes m' \;=\; \underbrace{\tfrac{1}{2}(m \otimes m' + m' \otimes m)}_{\in \mathrm{S}^2M} + \underbrace{\tfrac{1}{2}(m \otimes m' - m' \otimes m)}_{\in \Lambda^2M} \;\in\; \mathrm{S}^2M + \Lambda^2M\,.$$

Sei $(m_1, \ldots, m_k)$ eine $\mathbf{C}$-lineare Basis von M.

Es erzeugt $(\, m_i \otimes m_j + m_j \otimes m_i \,:\, 1 \leqslant i \leqslant j \leqslant k\,)$ auf $\mathbf{C}$-lineare Weise S^2M. Denn für $m = \sum_i z_i\, m_i$ und $m' = \sum_i z'_i\, m_i$ mit $z_i\,,\, z'_i \in \mathbf{C}$ für $i \in [1,k]$ wird

$$\begin{aligned} m \otimes m' + m' \otimes m &= (\textstyle\sum_i z_i\, m_i) \otimes (\sum_j z'_j\, m_j) + (\sum_j z'_j\, m_j) \otimes (\sum_i z_i\, m_i) \\ &= \textstyle\sum_{i,j} z_i\, z'_j (m_i \otimes m_j + m_j \otimes m_i)\,. \end{aligned}$$

Es erzeugt $(\, m_i \otimes m_j - m_j \otimes m_i \,:\, 1 \leqslant i < j \leqslant k\,)$ auf $\mathbf{C}$-lineare Weise Λ^2M. Denn für $m = \sum_i z_i\, m_i$ und $m' = \sum_i z'_i\, m_i$ mit $z_i\,,\, z'_i \in \mathbf{C}$ für $i \in [1,k]$ wird

$$\begin{aligned} m \otimes m' - m' \otimes m &= (\textstyle\sum_i z_i\, m_i) \otimes (\sum_j z'_j\, m_j) - (\sum_j z'_j\, m_j) \otimes (\sum_i z_i\, m_i) \\ &= \textstyle\sum_{i,j} z_i\, z'_j (m_i \otimes m_j - m_j \otimes m_i) \\ &= \textstyle\sum_{i \neq j} z_i\, z'_j (m_i \otimes m_j - m_j \otimes m_i)\,. \end{aligned}$$

Also ist

$$k^2 \;=\; \dim_{\mathbf{C}}(M \otimes M) \;\leqslant\; \underbrace{\dim_{\mathbf{C}} \mathrm{S}^2M}_{\leqslant \frac{k(k+1)}{2}} + \underbrace{\dim_{\mathbf{C}} \Lambda^2M}_{\leqslant \frac{k(k-1)}{2}} \;\leqslant\; k^2\,.$$

Somit stehen überall Gleichheiten. Insbesondere ist

$$(\, m_i \otimes m_j + m_j \otimes m_i \,:\, 1 \leqslant i \leqslant j \leqslant k\,)$$

eine $\mathbf{C}$-lineare Basis von S^2M, es ist

$$(\, m_i \otimes m_j - m_j \otimes m_i \,:\, 1 \leqslant i < j \leqslant k\,)$$

eine $\mathbf{C}$-lineare Basis von Λ^2M und es ist die Summe $\mathrm{S}^2M + \Lambda^2M$ direkt.

Sei $g \in G$. Schreibe $gm_a = \sum_b w_{b,a}\, m_b$ für $a \in [1,k]$, wobei $w_{b,a} \in \mathbf{C}$ stets.

Berechnen wir $\chi_{\mathrm{S}^2M}(g)$. Sei $1 \leqslant i \leqslant j \leqslant k$ gegeben. Es wird

$$g(m_i \otimes m_j + m_j \otimes m_i) \;=\; \sum_{a,b} w_{a,i}\, w_{b,j} (m_a \otimes m_b + m_b \otimes m_a)\,.$$

Der Beitrag zur Spur des Basiselements $m_i \otimes m_j + m_j \otimes m_i$ ist also gleich $w_{i,i}\, w_{j,j} + w_{i,j}\, w_{j,i}$, falls $i < j$, und $w_{i,i}^2$, falls $i = j$.
Insgesamt wird

$$\begin{aligned}
\chi_{\mathrm{S}^2 M}(g) &= (\textstyle\sum_{i<j} w_{i,i}\, w_{j,j} + w_{i,j}\, w_{j,i}) + (\sum_i w_{i,i}^2) \\
&= \tfrac{1}{2}(\textstyle\sum_i w_{i,i})(\sum_j w_{j,j}) + (\sum_{i<j} w_{i,j}\, w_{j,i}) + \tfrac{1}{2}(\sum_i w_{i,i}^2) \\
&= \tfrac{1}{2}(\textstyle\sum_i w_{i,i})(\sum_j w_{j,j}) + \tfrac{1}{2}(\sum_{i,j} w_{i,j}\, w_{j,i}) \\
&= \tfrac{1}{2}\big((\operatorname{tr} \rho_M(g))^2 + \operatorname{tr}(\rho_M(g)^2)\big) \\
&= \tfrac{1}{2}\big((\operatorname{tr} \rho_M(g))^2 + \operatorname{tr}(\rho_M(g^2))\big) \\
&= \tfrac{1}{2}\big(\chi_M(g)^2 + \chi_M(g^2)\big)\ .
\end{aligned}$$

Berechnen wir $\chi_{\Lambda^2 M}(g)$. Sei $1 \leqslant i < j \leqslant k$ gegeben. Es wird

$$g(m_i \otimes m_j - m_j \otimes m_i) \;=\; \sum_{a,b} w_{a,i}\, w_{b,j}(m_a \otimes m_b - m_b \otimes m_a)\ .$$

Der Beitrag zur Spur des Basiselements $m_i \otimes m_j - m_j \otimes m_i$ ist also gleich $w_{i,i}\, w_{j,j} - w_{i,j}\, w_{j,i}$.
Insgesamt wird

$$\begin{aligned}
\chi_{\Lambda^2 M}(g) &= (\textstyle\sum_{i<j} w_{i,i}\, w_{j,j} - w_{i,j}\, w_{j,i}) \\
&= \tfrac{1}{2}(\textstyle\sum_i w_{i,i})(\sum_j w_{j,j}) - (\sum_{i<j} w_{i,j}\, w_{j,i}) - \tfrac{1}{2}(\sum_i w_{i,i}^2) \\
&= \tfrac{1}{2}(\textstyle\sum_i w_{i,i})(\sum_j w_{j,j}) - \tfrac{1}{2}(\sum_{i,j} w_{i,j}\, w_{j,i}) \\
&= \tfrac{1}{2}\big((\operatorname{tr} \rho_M(g))^2 - \operatorname{tr}(\rho_M(g)^2)\big) \\
&= \tfrac{1}{2}\big((\operatorname{tr} \rho_M(g))^2 - \operatorname{tr}(\rho_M(g^2))\big) \\
&= \tfrac{1}{2}\big(\chi_M(g)^2 - \chi_M(g^2)\big)\ .
\end{aligned}$$

Probe. Es ist für $g \in G$ in der Tat

$$\chi_M(g)^2 \;=\; \chi_{M\otimes M}(g) \;=\; \chi_{\mathrm{S}^2 M}(g) + \chi_{\Lambda^2 M}(g) \;=\; \tfrac{1}{2}\big(\chi_M(g)^2 + \rho_M(g^2)\big) + \tfrac{1}{2}\big(\chi_M(g)^2 - \rho_M(g^2)\big)\ .$$

Alternative. Wir können auch Eigenwerte zur Berechnung von $\chi_{\mathrm{S}^2 M}(g)$ und $\chi_{\Lambda^2 M}(g)$ verwenden. Sei $(m_1\,, \ldots,\, m_k)$ eine $\mathbf{C}$-lineare Basis von M aus Eigenvektoren von $\rho_M(g)$; cf. Lösung zu Aufgabe 25.(1). Sei $g m_i = \xi_i m_i$ mit $\xi_i \in \mathbf{C}$ für $i \in [1, k]$. Also ist $g^2 m_i = \xi_i^2 m_i$ mit $\xi_i \in \mathbf{C}$ für $i \in [1, k]$. Insbesondere ist $\chi_M(g) = \sum_{i\in[1,k]} \xi_i$ und $\chi_M(g^2) = \sum_{i\in[1,k]} \xi_i^2$.
Es ist

$$g(m_i{\otimes}m_j{+}m_j{\otimes}m_i) \;=\; g m_i{\otimes}g m_j{+}g m_j{\otimes}g m_i \;=\; \xi_i m_i{\otimes}\xi_j m_j{+}\xi_j m_j{\otimes}\xi_i m_i \;=\; \xi_i\xi_j(m_i{\otimes}m_j{+}m_j{\otimes}m_i)$$

für $1 \leqslant i \leqslant j \leqslant k$. Also ist

$$\begin{aligned}
\chi_{\mathrm{S}^2 M}(g) &= \textstyle\sum_{1\leqslant i\leqslant j\leqslant k} \xi_i\xi_j \\
&= \tfrac{1}{2}\big((\textstyle\sum_{i\in[1,k]} \xi_i)^2 + (\sum_{i\in[1,k]} \xi_i^2)\big) \\
&= \tfrac{1}{2}\big(\chi_M(g)^2 + \chi_M(g^2)\big)\ .
\end{aligned}$$

Es ist

$$g(m_i{\otimes}m_j{-}m_j{\otimes}m_i) \;=\; g m_i{\otimes}g m_j{-}g m_j{\otimes}g m_i \;=\; \xi_i m_i{\otimes}\xi_j m_j{-}\xi_j m_j{\otimes}\xi_i m_i \;=\; \xi_i\xi_j(m_i{\otimes}m_j{-}m_j{\otimes}m_i)$$

für $1 \leqslant i \leqslant j \leqslant k$. Also ist

$$\begin{aligned}
\chi_{\Lambda^2 M}(g) &= \textstyle\sum_{1\leqslant i<j\leqslant k} \xi_i\xi_j \\
&= \tfrac{1}{2}\big((\textstyle\sum_{i\in[1,k]} \xi_i)^2 - (\sum_{i\in[1,k]} \xi_i^2)\big) \\
&= \tfrac{1}{2}\big(\chi_M(g)^2 - \chi_M(g^2)\big)\ .
\end{aligned}$$

(2) Die Charaktertafel von S_4 ist gegeben durch

$$X(\mathrm{S}_4) \;=\; \begin{array}{c} \\ \chi_{4,1} \\ \chi_{4,2} \\ \chi_{4,3} \\ \chi_{4,4} \\ \chi_{4,5} \end{array} \begin{array}{c} \begin{array}{ccccc} \mathrm{id} & (1,2) & (1,2,3) & (1,2,3,4) & (1,2)(3,4) \\ 1 & 6 & 8 & 6 & 3 \end{array} \\ \left[\begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 3 & 1 & 0 & -1 & -1 \\ 3 & -1 & 0 & 1 & -1 \\ 2 & 0 & -1 & 0 & 2 \end{array}\right] \end{array},$$

wobei direkt unter den Konjugationsklassenrepräsentanten die Länge ihrer Konjugationsklassen notiert wurde; cf. Lösung zu Aufgabe 37.(3).

Wir ordnen die Konjugationsklassenrepräsentanten von S_5 in der folgenden Reihenfolge, darunter die Konjugationsklassenlängen.

id	$(1,2)$	$(1,2,3)$	$(1,2,3,4)$	$(1,2,3,4,5)$	$(1,2)(3,4)$	$(1,2,3)(4,5)$
1	10	20	30	24	15	20

Wir schreiben Charaktere dementsprechend als Zeilenvektoren.

Es sind $\chi_{5,1} := (1\ 1\ 1\ 1\ 1\ 1\ 1)$ und $\chi_{5,2} := (1\ {-1}\ 1\ {-1}\ 1\ 1\ {-1})$ irreduzible Charaktere von S_5; cf. Beispiel 39.(3).

Wir arbeiten mit dem Skalarprodukt; cf. Bemerkung 94.

Zum Induzieren verwenden wir

$$\mathrm{S}_5 \;=\; \mathrm{S}_4\,\mathrm{id} \sqcup \mathrm{S}_4(1,5) \sqcup \mathrm{S}_4(2,5) \sqcup \mathrm{S}_4(3,5) \sqcup \mathrm{S}_4(4,5)\ ;$$

cf. Lemma 117.

Es ist $\chi_{4,1}\big|_{\mathrm{S}_4}^{\mathrm{S}_5} = (5\,3\,2\,1\,0\,1\,0)$. Dieser Charakter enthält $\chi_{5,1}$ einmal. Folglich ist $\chi_{5,3} := \chi_{4,1}\big|_{\mathrm{S}_4}^{\mathrm{S}_5} - \chi_{5,1} = (4\ 2\ 1\ 0\ {-1}\ 0\ {-1})$ ein Charakter. Dieser ist irreduzibel.

Sei $\chi_{5,4} := \chi_{5,3} \cdot \chi_{5,2} = (4\ {-2}\ 1\ 0\ {-1}\ 0\ 1)$. Dieser Charakter ist irreduzibel; cf. auch Aufgabe 33.(2).

Sei $\chi_{5,5} := \Lambda^2\chi_{5,3} = (6\ 0\ 0\ 0\ 1\ {-2}\ 0)$; cf. (1). Dieser Charakter ist irreduzibel.

Es ist $\chi_{4,3}\big|_{\mathrm{S}_4}^{\mathrm{S}_5} = (15\ 3\ 0\ {-1}\ 0\ {-1}\ 0)$. Dieser Charakter enthält $\chi_{5,3}$ und $\chi_{5,5}$ je einmal. Folglich ist $\chi_{5,6} := \chi_{4,3}\big|_{\mathrm{S}_4}^{\mathrm{S}_5} - \chi_{5,3} - \chi_{5,5} = (5\ 1\ {-1}\ {-1}\ 0\ 1\ 1)$ ein Charakter. Dieser ist irreduzibel.

Sei $\chi_{5,7} := \chi_{5,6} \cdot \chi_{5,2} = (5\ {-1}\ {-1}\ 1\ 0\ 1\ {-1})$. Dieser Charakter ist irreduzibel; cf. auch Aufgabe 33.(2).

Insgesamt ergibt sich die Charaktertafel der S_5 zu

$$X(\mathrm{S}_5) \;=\; \begin{array}{c} \\ \chi_{5,1} \\ \chi_{5,2} \\ \chi_{5,3} \\ \chi_{5,4} \\ \chi_{5,5} \\ \chi_{5,6} \\ \chi_{5,7} \end{array} \begin{array}{c} \begin{array}{ccccccc} \mathrm{id} & (1,2) & (1,2,3) & (1,2,3,4) & (1,2,3,4,5) & (1,2)(3,4) & (1,2,3)(4,5) \\ 1 & 10 & 20 & 30 & 24 & 15 & 20 \end{array} \\ \left[\begin{array}{ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 4 & 2 & 1 & 0 & -1 & 0 & -1 \\ 4 & -2 & 1 & 0 & -1 & 0 & 1 \\ 6 & 0 & 0 & 0 & 1 & -2 & 0 \\ 5 & 1 & -1 & -1 & 0 & 1 & 1 \\ 5 & -1 & -1 & 1 & 0 & 1 & -1 \end{array}\right] \end{array},$$

wobei direkt unter den Konjugationsklassenrepräsentanten die Länge ihrer Konjugationsklassen notiert wurde.

Aufgabe 43

(1) Ist $z \in \mathrm{Z}(G)$, so ist $M \to M$, $m \mapsto zm$ ein $\mathbf{C}G$-linearer Endomorphismus von M. Nach Schurs Lemma ist dieser Endomorphismus also durch eine Multiplikation mit einem Element aus $\mathbf{C}$ gegeben; cf. Lemma 66.(4), Lemma 69. In anderen Worten, es ist

$$\rho_M(\mathrm{Z}(G)) \leqslant \mathrm{Z}(\mathrm{GL}(M)) = \{ \lambda \cdot \mathrm{id}_M : \lambda \in \mathrm{GL}_1(\mathbf{C}) \} .$$

Abermals in anderen Worten, es gibt einen Gruppenmorphismus $\mu : \mathrm{Z}(G) \to \mathrm{GL}_1(\mathbf{C})$ mit $\rho_M(z) = \mu(z) \cdot \mathrm{id}_M$ für $z \in \mathrm{Z}(G)$.

Sei $k \in \mathbf{Z}_{\geqslant 1}$. Schreibe $G^{\times k} := \underbrace{G \times \cdots \times G}_{k \text{ Faktoren}}$ und $M^{\boxtimes k} := \underbrace{M \boxtimes \cdots \boxtimes M}_{k \text{ Faktoren}}$.

Gemäß Aufgabe 41.(L. z. 1, 3) ist $M^{\boxtimes k}$ ein einfacher $\mathbf{C}(G^{\times k})$-Modul.

Wir haben den surjektiven Gruppenmorphismus $\mathrm{Z}(G)^{\times k} \to \mathrm{Z}(G)$, $(z_i)_i \mapsto z_1 \cdots z_k$ und dessen Kern $C := \{ (z_i)_i \in \mathrm{Z}(G)^{\times k} : z_1 \cdots z_k = 1 \} \trianglelefteqslant G^{\times k}$. Es ist $|C| = |\mathrm{Z}(G)|^{k-1}$.

Ist $(z_i)_i = (z_1, \ldots, z_k) \in C$, so ist

$$\begin{aligned}(z_1, \ldots, z_k)(m_1 \otimes \cdots \otimes m_k) &= z_1 m_1 \otimes \cdots \otimes z_k m_k \\ &= \mu(z_1) m_1 \otimes \cdots \otimes \mu(z_k) m_k \\ &= \mu(z_1) \cdots \mu(z_k)(m_1 \otimes \cdots \otimes m_k) \\ &= \mu(z_1 \cdots z_k)(m_1 \otimes \cdots \otimes m_k) \\ &= m_1 \otimes \cdots \otimes m_k\end{aligned}$$

für $m_i \in M$ für $i \in [1, k]$.

Also gibt es den $\mathbf{C}(G^{\times k}/C)$-Modul $M^{\boxtimes k}$ mit der Operation

$$(g_i)_i C(m_1 \otimes \cdots \otimes m_k) = g_1 m_1 \otimes \cdots \otimes g_k m_k$$

für $(g_i)_i \in G^{\times k}$ und $m_i \in M$ für $i \in [1, k]$. Da $\mathbf{C}(G^{\times k}) \to \mathbf{C}(G^{\times k}/C)$, $g \mapsto gC$ surjektiv ist, ist dieser ebenfalls einfach; cf. Lösung zu Aufgabe 33.(4).

Somit ist $\dim_{\mathbf{C}}(M^{\boxtimes k}) = (\dim_{\mathbf{C}} M)^k$ ein Teiler von $|G^{\times k}/C| = |G|^k/|\mathrm{Z}(C)|^{k-1}$; cf. Satz 102.

Da dies für jedes $k \in \mathbf{Z}_{\geqslant 1}$ zutrifft, folgt, daß $\dim_{\mathbf{C}} M$ ein Teiler von $|G|/|\mathrm{Z}(C)|$ ist. Denn sei p eine Primzahl. Für $a \in \mathbf{Z}$ schreiben wir $\mathrm{v}_p(a) := \max\{ i \in \mathbf{Z}_{\geqslant 0} ; p^i \text{ teilt } a \}$. Es ist $k\,\mathrm{v}_p(\dim_{\mathbf{C}} M) = \mathrm{v}_p((\dim_{\mathbf{C}} M)^k) \leqslant \mathrm{v}_p(|G|^k/|\mathrm{Z}(C)|^{k-1}) = k(\mathrm{v}_p(|G|) - \mathrm{v}_p(|\mathrm{Z}(G)|)) + \mathrm{v}_p(|\mathrm{Z}(G)|)$ und also $\mathrm{v}_p(\dim_{\mathbf{C}} M) \leqslant \mathrm{v}_p(|G|) - \mathrm{v}_p(|\mathrm{Z}(G)|) + k^{-1}\,\mathrm{v}_p(|\mathrm{Z}(G)|)$ für $k \in \mathbf{Z}_{\geqslant 1}$. Es folgt $\mathrm{v}_p(\dim_{\mathbf{C}} M) \leqslant \mathrm{v}_p(|G|) - \mathrm{v}_p(|\mathrm{Z}(G)|)$.

(2) Sei $1_{\mathrm{Z}(\mathbf{C}N)} = \varepsilon_1 + \cdots + \varepsilon_k$ die orthogonale Zerlegung in primitive Idempotente in $\mathrm{Z}(\mathbf{C}N)$; cf. Aufgabe 22.

Gebe es kein $i \in [1, k]$ mit $\varepsilon_i M = M$.

Es ist $1 \cdot M = (\varepsilon_1 + \cdots + \varepsilon_k)M \neq 0$. Da also nicht alle ε_i das M annullieren können, ist o.E. $0 \subset \varepsilon_1 M \subset M$.

Für $g \in G$ ist $\mathrm{Z}(\mathbf{C}N) \to \mathrm{Z}(\mathbf{C}N)$, $\xi \mapsto g\xi g^-$ ein $\mathbf{C}$-Algebrenautomorphismus; folglich ist $g\varepsilon_i g^-$ ein primitives Idempotent von $\mathrm{Z}(\mathbf{C}N)$ für $i \in [1, k]$. Definiere $g \cdot i$ durch $g\varepsilon_i =: \varepsilon_{g \cdot i}$ für $g \in G$ und $i \in [1, k]$. Dies macht $[1, k]$ zu einer G-Menge.

Sei $H := \{ g \in G : g\varepsilon_1 M = \varepsilon_1 M \} = \mathrm{C}_G(\{1\})$.

Es ist $N \leqslant H$, da ε_1 zentral in $\mathbf{C}N$ ist. Dank $N \trianglelefteqslant G$ ist auch $N \trianglelefteqslant H$.

Es ist $\varepsilon_1 M \subset M$ ein $\mathbf{C}H$-Teilmodul.

Es ist $H < G$, da M ein einfacher $\mathbf{C}G$-Modul ist und also $\varepsilon_1 M$ kein $\mathbf{C}G$-Teilmodul von M sein kann.

Wir behaupten, daß $\varepsilon_1 M$ ein einfacher $\mathbf{C}H$-Modul ist. *Annahme,* nicht. Sei $0 \subset X \subset \varepsilon_1 M$ ein $\mathbf{C}H$-Teilmodul. Es ist $0 \subset \hat{X} := \sum_{g\in G} gX \subseteq M$ ein $\mathbf{C}G$-Teilmodul. Schreibe $G = \bigsqcup_{j\in[1,\ell]} g_j H$. Es ist $\hat{X} = \sum_{j\in[1,\ell]} g_j X$. Es ist $g_j X \subset g_j \varepsilon_1 M = g_j \varepsilon_1 g_j^- M = \varepsilon_{g_j\cdot 1} M$ für $g \in G$. Es ist $g_j \cdot 1 \neq g_{j'} \cdot 1$ für $j, j' \in [1,\ell]$ mit $j \neq j'$. Also ist $\hat{X} \subset M$. *Widerspruch* zur Einfachheit von M. Dies zeigt die Behauptung.

Es bleibt zu zeigen, daß als $\mathbf{C}G$-Moduln

$$M \overset{!}{\simeq} (\varepsilon_1 M)\big\uparrow_H^G$$

ist, da wir dann für ψ den Charakter zu $\varepsilon_1 M$ von H nehmen können.

Zur $\mathbf{C}H$-linearen Inklusionsabbildung $\varepsilon_1 M \to M$ gehört mit Aufgabe 31.(2,3) die $\mathbf{C}G$-lineare Abbildung

$$\begin{array}{ccccc} \mathbf{C}G & \underset{\mathbf{C}H}{\otimes} & \varepsilon_1 M & \longrightarrow & M \\ g & \otimes & \varepsilon_1 m & \longmapsto & g\varepsilon_1 m \end{array}$$

Da M einfach ist und das Bild dieser $\mathbf{C}G$-linearen Abbildung ungleich 0 ist, ist diese surjektiv.

Bleibt zu zeigen, daß

$$\dim_{\mathbf{C}} \mathbf{C}G \underset{\mathbf{C}H}{\otimes} \varepsilon_1 M \overset{!}{=} \dim_{\mathbf{C}} M \,.$$

Aber es ist, mit obigen Bezeichnungen, $M = \widehat{\varepsilon_1 M} = \bigoplus_j g_j \varepsilon_1 M$ wegen der Einfachheit von M. Somit ist

$$\dim_{\mathbf{C}} M \;=\; \dim_{\mathbf{C}} \widehat{\varepsilon_1 M} \;=\; \textstyle\sum_j \dim_{\mathbf{C}} \varepsilon_1 M \;=\; \frac{|G|}{|H|} \dim_{\mathbf{C}} \varepsilon_1 M \overset{\text{L.117}}{=} \dim_{\mathbf{C}} \mathbf{C}G \underset{\mathbf{C}H}{\otimes} \varepsilon_1 M \,.$$

(3) Nehmen wir mit Induktion über $|G|$ an, die Aussage sei gezeigt für alle Gruppen von Ordnung kleiner als $|G|$.

Sei $1_{\mathrm{Z}(\mathbf{C}A)} = 1_{\mathbf{C}A} = \varepsilon_1 + \cdots + \varepsilon_k$ die orthogonale Zerlegung in primitive Idempotente in $\mathrm{Z}(\mathbf{C}A) = \mathbf{C}A$; cf. Aufgabe 22.

Fall: es gibt ein $j \in [1,k]$ mit $\varepsilon_j M = M$.

Beachte, daß $\mathbf{C}A \simeq \mathbf{C}^{\times k}$, da $\mathbf{C}A$ kommutativ ist; cf. Satz 67. Also ist jeder einfache $\mathbf{C}A$-Modul isomorph zu $\mathbf{C}A\varepsilon_i$ für ein $i \in [1,k]$; cf. Lemma 81. Insbesondere sind diese einfachen Moduln alle eindimensional.

Es ist $M \simeq \bigoplus_{u\in[1,v]} \mathbf{C}A\varepsilon_{i(u)}$ für $v := \dim_{\mathbf{C}} M$ und $i(u) \in [1,k]$ für $u \in [1,v]$; cf. Bemerkung 77.

Da $M = \varepsilon_j M$ ist, ist auch

$$\textstyle\bigoplus_{u\in[1,v]} \mathbf{C}A\varepsilon_{i(u)} \;=\; \varepsilon_j \bigoplus_{u\in[1,v]} \mathbf{C}A\varepsilon_{i(u)} \;=\; \bigoplus_{u\in[1,v]} \mathbf{C}A\varepsilon_j\varepsilon_{i(u)} \;=\; \bigoplus_{u\in[1,v],\, i(u)=j} \mathbf{C}A\varepsilon_j \,.$$

Es folgt, daß $i(u) = j$ für alle $u \in [1,v]$ und daß $M \simeq (\mathbf{C}A\varepsilon_j)^{\oplus v}$.

Sei $a \in A$. Es ist $\mathbf{C}A\varepsilon_j \to \mathbf{C}A\varepsilon_j\,,\ \xi \mapsto a\xi$ eine $\mathbf{C}A$-lineare Abbildung, und somit gleich $\lambda\,\mathrm{id}_{\mathbf{C}A\varepsilon_j}$ für ein $\lambda \in \mathbf{C}$; cf. Lemma 66.(4). Unser Isomorphismus zeigt, daß auch $M \to M$, $m \longmapsto am$ gleich $\lambda\,\mathrm{id}_M$ ist.

Also ist $\rho_M(A) \leqslant \mathrm{Z}(\mathrm{GL}(M)) \cap \rho_M(G) \leqslant \mathrm{Z}(\rho_M(G))$.

Da M auch ein einfacher $\mathbf{C}(\rho_M(G))$-Modul ist, folgt mit (1), daß $\chi(1)$ ein Teiler von $|\rho_M(G)|/|\mathrm{Z}(\rho_M(G))|$ und damit von $|\rho_M(G)|/|\rho_M(A)|$ ist.

Ist $K := \mathrm{Kern}\,\rho_M \trianglelefteqslant G$, so wird $\rho_M(G) \simeq G/K$ und $\rho_M(A) \simeq A/(A\cap K) \simeq AK/K$, letzteres mittels $a(A\cap K) \mapsto aK$.

Also ist $|\rho_M(G)|/|\rho_M(A)| = |G/K|/|AK/K| = |G|/|AK|$ ein Teiler von $|G|/|A|$.

Insgesamt ist $\chi(1)$ als Teiler von $\frac{|G|}{|A|}$ nachgewiesen.

Fall: es gibt kein $j \in [1,k]$ mit $\varepsilon_j M = M$.
Gemäß (2) gibt es eine Untergruppe $A \trianglelefteq H < G$ und einen irreduziblen Charakter ψ von H mit $\chi = \psi\uparrow_H^G$.
Nach Induktionsvoraussetzung ist $\psi(1)$ ein Teiler von $\frac{|H|}{|A|}$. Also ist $\chi(1) = \psi\uparrow_H^G(1) \overset{\text{L. }120}{=} \frac{|G|}{|H|}\,\psi(1)$ ein Teiler von $\frac{|G|}{|H|} \cdot \frac{|H|}{|A|} = \frac{|G|}{|A|}$.

Aufgabe 44

Sei χ ein irreduzibler Charakter von G. Es ist zu zeigen, daß $\chi(1) \overset{!}{\leqslant} m_H \frac{|G|}{|H|}$. Es ist also zu zeigen, daß

$$\chi(1) \overset{!}{\leqslant} \psi(1)\frac{|G|}{|H|}$$

für einen irreduziblen Charakter ψ von G.

Sei ψ ein irreduzibler Charakter von H mit ${}_H(\psi, \chi\downarrow_H^G) \geqslant 1$, existent, da $\chi\downarrow_H^G \neq 0$ ist; cf. Bemerkung 94.(1).

Also ist

$$\psi(1)\frac{|G|}{|H|} \overset{\text{L. }117}{=} \psi\uparrow_H^G(1) \overset{\text{B. }94.(1)}{\geqslant} {}_G(\psi\uparrow_H^G, \chi)\,\chi(1) \overset{\text{L. }120}{=} {}_H(\psi, \chi\downarrow_H^G)\,\chi(1) \geqslant \chi(1)\,.$$

Aufgabe 45

Sei $g \in G$. Es wird

$$\begin{aligned}
(\psi \circ r|_H^{H/N})\uparrow_H^G(g) &\overset{\text{L. }117}{=} \tfrac{1}{|H|}\textstyle\sum_{x\in G,\ {}^xg\in H}(\psi \circ r|_H^{H/N})({}^xg) \\
&= \tfrac{1}{|H|}\textstyle\sum_{x\in G,\ {}^xg\in H}\psi({}^xgN) \\
&= \tfrac{|N|}{|H|}\textstyle\sum_{xN\in G/N,\ {}^xgN\in H/N}\psi({}^xgN) \\
&= \tfrac{1}{|H/N|}\textstyle\sum_{xN\in G/N,\ {}^{xN}gN\in H/N}\psi({}^{xN}gN) \\
&\overset{\text{L. }117}{=} \psi\uparrow_{H/N}^{G/N}(gN) \\
&= (\psi\uparrow_{H/N}^{G/N} \circ r)(g)\,.
\end{aligned}$$

Aufgabe 46

Wir induzieren irreduzible Charaktere von zyklischen Untergruppen nach S_4. Wir verwenden die Notation der Lösung zu Aufgabe 37.(3), was die Konjugationsklassenrepräsentanten id, $(1,2)$, $(1,2,3)$, $(1,2,3,4)$, $(1,2)(3,4)$ von S_4 und ihre Charaktertafel angeht.

Wir haben die zyklische Untergruppe $I := \langle(1,2,3,4)\rangle \leqslant \mathrm{S}_4$. Ihre Konjugationsklassen sind repräsentiert von id, $(1,2,3,4)$, $(1,3)(2,4)$, $(1,4,3,2)$. Dieser Reihenfolge entsprechend notieren wir Charaktere als Zeilenvektoren; cf. Beispiel 86.(2). Es wird

$$\begin{aligned}
(1\ 1\ 1\ 1)\uparrow_I^{\mathrm{S}_4} &= (6\ 0\ 0\ 2\ 2) &=:\ \psi_1 \\
(1\ {-1}\ 1\ {-1})\uparrow_I^{\mathrm{S}_4} &= (6\ 0\ 0\ {-2}\ 2) &=:\ \psi_2 \\
(1\ \zeta_4\ {-1}\ {-\zeta_4})\uparrow_I^{\mathrm{S}_4} &= (6\ 0\ 0\ 0\ {-2}) &=:\ \psi_3\,.
\end{aligned}$$

Wir haben die zyklische Untergruppe $J := \langle(1,2,3)\rangle \leqslant \mathrm{S}_4$. Ihre Konjugationsklassen sind repräsentiert von id, $(1,2,3)$, $(1,3,2)$. Dieser Reihenfolge entsprechend notieren wir Charaktere als Zeilenvektoren; cf. Beispiel 86.(2). Es wird

$$(1\ \zeta_3\ \zeta_3^2)\uparrow_J^{\mathrm{S}_4} = (8\ 0\ {-1}\ 0\ 0) =:\ \psi_4\,.$$

Wir haben die zyklische Untergruppe $K := \langle (1,2) \rangle \leqslant \mathrm{S}_4$. Ihre Konjugationsklassen sind repräsentiert von id, $(1,2)$. Dieser Reihenfolge entsprechend notieren wir Charaktere als Zeilenvektoren; cf. Beispiel 86.(2). Es wird

$$(1\ 1)\uparrow_K^{\mathrm{S}_4} \ = \ (12\ 2\ 0\ 0\ 0) \ =: \ \psi_5 \ .$$

Somit ist, in der Notation der Lösung von Aufgabe 37.(3),

$$\begin{array}{rcll} \chi_{4,1} & = & (1\ 1\ 1\ 1\ 1) & = \ \frac{1}{2}\psi_1 - \psi_4 + \frac{1}{2}\psi_5 \\ \chi_{4,2} & = & (1\ {-1}\ 1\ {-1}\ 1) & = \ \frac{1}{2}\psi_1 + \psi_2 + \psi_3 - \psi_4 - \frac{1}{2}\psi_5 \\ \chi_{4,3} & = & (3\ 1\ 0\ {-1}\ {-1}) & = \ -\frac{1}{2}\psi_1 + \frac{1}{2}\psi_5 \\ \chi_{4,4} & = & (3\ {-1}\ 0\ 1\ {-1}) & = \ \frac{1}{2}\psi_1 + \psi_3 - \frac{1}{2}\psi_5 \\ \chi_{4,5} & = & (2\ 0\ {-1}\ 0\ 2) & = \ -\psi_3 + \psi_4 \ . \end{array}$$

Eine Darstellung wie verlangt ergibt sich hieraus durch Multiplikation mit 24.

Cf. Beispiel 163, wo der Satz 161 von Brauer für $G = \mathrm{S}_4$ betrachtet wird.

Aufgabe 47

(1) Sei X ein einfacher $\mathbf{C}G$-Modul mit $\chi_X = \chi$. Sei Y ein einfacher $\mathbf{C}N$-Teilmodul von X mit $\chi_Y = \psi$.
Es ist $\sum_{g\in G} gY$ ein $\mathbf{C}G$-Teilmodul von X ungleich 0. Also ist $X = \sum_{g\in G} gY$.
Es ist $gY \subseteq X$ ein einfacher $\mathbf{C}N$-Teilmodul mit Charakter ${}^g\psi$.
Für $g \in G$ ist $gY \simeq Y$ als $\mathbf{C}N$-Moduln genau dann, wenn ${}^g\psi = \psi$, i.e. wenn $g \in T$. Es ist

$$Z \ := \ \textstyle\sum_{t\in T} tY$$

ein $\mathbf{C}T$-Teilmodul von X. Sei

$$\varphi \ := \ \chi_Z$$

der zugehörige Charakter von T.
Sei $M \subseteq T$ eine maximale Teilmenge so, daß die Summe $\sum_{t\in M} tY$ direkt ist.
Annahme, es ist $\bigoplus_{t\in M} tY \subset Z$. Dann gibt es ein $t' \in T$ mit $t'Y \not\subseteq \bigoplus_{t\in M} tY$. Da $t'Y$ ein einfacher $\mathbf{C}N$-Modul ist, folgt $t'Y \cap (\bigoplus_{t\in M} tY) = 0$ und also, daß die Summe $\sum_{t\in M\cup\{t'\}} tY$ direkt ist. Das ist ein *Widerspruch* zur Maximalität von M.
Also ist $Z = \bigoplus_{t\in M} tY$.
Entsprechend ist $rZ = \bigoplus_{t\in M} rtY$ für $r \in R$.
Schreibe

$$e' \ := \ |M| \ .$$

Es ist

$$\varphi\rfloor_N^T \ = \ e'\psi \ .$$

Es ist $X = \sum_{g\in G} gY = \sum_{r\in R} rZ$. Letztere Summe ist direkt, da für $r, r' \in R$ mit $r \neq r'$ die nicht zueinander isomorphen einfachen $\mathbf{C}N$-Moduln rY und $r'Y$ von verschiedenen primitiven Idempotenten von $\mathrm{Z}(\mathbf{C}N)$ nicht annulliert werden; cf. Bemerkung 52. Also ist

$$X \ = \ \textstyle\bigoplus_{r\in R} rZ \ .$$

Zusammen erhalten wir folgende Gleichheit von Charakteren von N.

$$\chi\rfloor_N^G \ = \ \textstyle\sum_{r\in R} \chi_{rZ} \ = \ \sum_{r\in R} {}^r(\chi_Z) \ = \ e' \sum_{r\in R} {}^r\psi$$

Insbesondere ist

$$e' \;=\; {}_N(\psi, e' \textstyle\sum_{r\in R} {}^r\psi) \;=\; {}_N(\psi, \chi\rfloor_N^G) \;=\; e\,.$$

Ferner liefert die $\mathbf{C}T$-lineare Inklusionsabbildung $Z \longrightarrow X$ die $\mathbf{C}G$-lineare Abbildung

$$\begin{array}{ccccc} \mathbf{C}G & \underset{\mathbf{C}T}{\otimes} & Z & \xrightarrow{\;f\;} & X \\ g & \otimes & z & \longmapsto & gz\,; \end{array}$$

cf. Aufgabe 31.(2, 3).

Es ist f surjektiv, da $\sum_{g\in G} gY = X$ im Bild von f enthalten ist; cf. oben.

Es ist f injektiv, da

$$\dim_{\mathbf{C}}(\mathbf{C}G \underset{\mathbf{C}T}{\otimes} Z) \overset{\text{L. }117}{=} \tfrac{|G|}{|T|} \dim_{\mathbf{C}} Z \;=\; \dim_{\mathbf{C}} \textstyle\bigoplus_{r\in R} rZ \;=\; \dim_{\mathbf{C}} X\,;$$

Also ist f ein $\mathbf{C}G$-linearer Isomorphismus. Es folgt $\chi = \varphi\rfloor_T^G$.

Cf. Beispiel 126. Die dort an ψ gestellte Bedingung läuft auf $T = N$ hinaus, was wegen $\varphi\rfloor_N^T = e\psi$ auch $e = 1$ erzwingt. Cf. auch Vorbemerkung 3 in (2) unten.

Es ist (1) Bestandteil der *Clifford-Theorie.*

(2) *Vorbemerkung* 1. Für $g \in G \smallsetminus N$ ist $\psi\uparrow_N^G(g) = 0$, denn

$$\psi\uparrow_N^G(g) \overset{\text{L. }117}{=} \frac{1}{|N|} \sum_{h\in G,\ {}^hg\in N} \psi({}^hg) \;=\; 0\,.$$

Vorbemerkung 2. Für $x \in G$ ist $({}^x\psi)\uparrow_N^G = \psi\uparrow_N^G$. Denn bei $g \in G \smallsetminus N$ werden beide Seiten null nach Vorbemerkung 1, und bei $n \in N$ wird

$$({}^x\psi)\uparrow_N^G(n) \overset{\text{L. }117}{=} \tfrac{1}{|N|} \textstyle\sum_{h\in G} ({}^x\psi)({}^hn) \;=\; \tfrac{1}{|N|} \sum_{h\in G} \psi({}^{x^-h}n) \overset{\tilde h = x^-h}{=} \tfrac{1}{|N|} \sum_{\tilde h\in G} \psi({}^{\tilde h}n) \overset{\text{L. }117}{=} \psi\uparrow_N^G(n)\,.$$

Vorbemerkung 3. Falls $\chi(g) = 0$ ist für $g \in G \smallsetminus N$ und falls $e \neq 0$ ist, dann ist

$$\begin{array}{rcl} 1 & \overset{\text{B. }94.(2)}{=} & {}_G(\chi, \chi) \\ & = & \frac{1}{|G|} \sum_{g\in G} \chi(g)\, \overline{\chi(g)} \\ & = & \frac{1}{|G|} \sum_{n\in N} \chi(n)\, \overline{\chi(n)} \\ & = & \frac{|N|}{|G|}\, {}_N(\chi\rfloor_N^G\,, \chi\rfloor_N^G) \\ & \overset{(1)}{=} & \frac{|N|}{|G|} \cdot e \sum_{r\in R} {}_N({}^r\psi\,, \chi\rfloor_N^G) \\ & \overset{\text{L. }120}{=} & \frac{|N|}{|G|} \cdot e \sum_{r\in R} {}_N(({}^r\psi)\uparrow_N^G, \chi) \\ & = & \frac{|N|}{|G|} \cdot e \sum_{r\in R} {}_N(\psi\uparrow_N^G, \chi) \\ & \overset{\text{L. }120}{=} & \frac{|N|}{|G|} \cdot e \sum_{r\in R} {}_N(\psi\,, \chi\rfloor_N^G) \\ & = & \frac{|N|}{|G|} \cdot |R| \cdot e^2 \\ & = & \frac{|N|}{|T|} \cdot e^2\,, \end{array}$$

mithin

$$e^2 \;=\; \frac{|T|}{|N|}\,.$$

Sei nun $e = 1$ und $\chi(g) = 0$ für $g \in G \smallsetminus N$. Mit Vorbemerkung 3 ist $T = N$. Mit (1) wird also $\varphi = \varphi\restriction_N^T = e \cdot \psi = \psi$ und somit $\psi\restriction_N^G = \varphi\restriction_T^G = \chi$.

Sei umgekehrt $\chi = \psi\restriction_N^G$. Dann ist $\psi\restriction_N^G(g) = 0$ für $g \in G \smallsetminus N$ nach Vorbemerkung 1. Ferner ist

$$e \;=\; {}_G(\psi\restriction_N^G, \chi) \;=\; {}_G(\chi, \chi) \;=\; 1\,.$$

Aufgabe 48

Sei $r : G \to G/N$, $g \mapsto gN$ die Restklassenabbildung.

Seien $\chi_1, \ldots, \chi_t$ die verschiedenen irreduziblen Charaktere von G.

Sei $A := \{\, s \in [1,t] \,:\, N \leqslant \operatorname{Kern}\chi_s \,\}$. Sei $B := \{\, s \in [1,t] \,:\, N \not\leqslant \operatorname{Kern}\chi_s \,\}$. Also $[1,t] = A \sqcup B$.

Sei $s \in A$. Es gibt es genau einen Charakter $\check{\chi}_s$ von G/N mit $\check{\chi}_s \circ r = \chi_s$, und dieser ist irreduzibel. Denn ist $\rho_s : G \longrightarrow \mathrm{GL}(V)$ eine zu χ_s gehörige Darstellung von G, so ist N in deren Kern enthalten, cf. Aufgabe 30. Somit gibt es eine Darstellung $\check{\rho}_s : G/N \to \mathrm{GL}(V)$ mit $\rho_s = \check{\rho}_s \circ r$. Ist $\check{\chi}_s$ der Charakter zu $\check{\rho}_s$, so folgt $\check{\chi}_s \circ r = \chi_s$. Die Eindeutigkeit folgt aus der Surjektivität von r. Da $\mathbf{C}G \to \mathbf{C}(G/N)$, $g \mapsto gN$ ein surjektiver $\mathbf{C}$-Algebrenmorphismus ist, folgt aus der Einfachheit des zu ρ_s gehörigen $\mathbf{C}G$-Moduls V die Einfachheit des zu $\check{\rho}_s$ gehörigen $\mathbf{C}(G/N)$-Moduls V und damit die Irreduzibilität von $\check{\chi}_s$.

Ferner durchläuft $\check{\chi}_s$ alle irreduziblen Charaktere von G/N, wenn s durch A läuft. Denn jeder irreduzible Charakter von G/N gibt umgekehrt wieder einen irreduziblen Charakter von G durch Komposition mit r; cf. Aufgabe 33.(4).

Sei $x \in G$ mit $\mathrm{C}_G(x) \cap N = 1$ gegeben.

Zu zeigen ist, daß $\chi_s(x) \stackrel{!}{=} 0$ ist für $s \in B$. Es genügt hierzu, $\sum_{s\in B} |\chi_s(x)|^2 \stackrel{!}{=} 0$ zu zeigen.

Zu zeigen ist ferner, daß $\mathrm{C}_G(x) \stackrel{!}{\simeq} \mathrm{C}_{G/N}(xN)$ ist.

Es ist

$$\textstyle\sum_{s\in A\sqcup B} |\chi_s(x)|^2 \;\stackrel{\text{S. 90.(2)}}{=}\; |\mathrm{C}_G(x)|\,.$$

Es ist

$$\textstyle\sum_{s\in A} |\chi_s(x)|^2 \;=\; \sum_{s\in A} |\check{\chi}_s(xN)|^2 \;\stackrel{\text{S. 90.(2)}}{=}\; |\mathrm{C}_{G/N}(xN)|\,.$$

Also ist

$$\textstyle\sum_{s\in B} |\chi_s(x)|^2 \;=\; (\sum_{s\in A\sqcup B} |\chi_s(x)|^2) - (\sum_{s\in A} |\chi_s(x)|^2) \;=\; |\mathrm{C}_G(x)| - |\mathrm{C}_{G/N}(xN)|\,.$$

Wir haben den Gruppenmorphismus

$$r\restriction_{\mathrm{C}_G(x)}^{\mathrm{C}_{G/N}(xN)} \;:\; \mathrm{C}_G(x) \longrightarrow \mathrm{C}_{G/N}(xN)\,,\; g \longmapsto gN\,,$$

da für $g \in G$ aus ${}^g x = x$ auch ${}^{(gN)}(xN) = xN$ folgt.

Dieser hat den Kern $\mathrm{C}_G(x) \cap N = 1$, ist also injektiv. Es folgt $|\mathrm{C}_G(x)| \leqslant |\mathrm{C}_{G/N}(xN)|$.

Für $\mathrm{C}_G(x) \stackrel{!}{\simeq} \mathrm{C}_{G/N}(xN)$ bleibt $|\mathrm{C}_G(x)| \stackrel{!}{=} |\mathrm{C}_{G/N}(xN)|$ zu zeigen.

Aber es wird

$$0 \;\leqslant\; \textstyle\sum_{s\in B} |\chi_s(x)|^2 \;=\; |\mathrm{C}_G(x)| - |\mathrm{C}_{G/N}(xN)| \;\leqslant\; 0\,.$$

Somit stehen links wie rechts Gleichheitszeichen, und alles ist gezeigt.

Aufgabe 49

Wir werden kommentarlos die Orthonormalität der irreduziblen Charaktere bezüglich des Skalarproduktes aus Bemerkung 92, die Induktionsformel aus Lemma 117 und die Frobenius-Reziprozität aus Lemma 120 verwenden.

Für $M \subseteq G$ schreiben wir $\dot{M} := M \smallsetminus \{1\}$.

Sofort ist $N \cap H = \{1\}$, da für $n \in \dot{N}$ auch $\{n\} \cap H \subseteq {}^G n \cap H = \emptyset$ ist.

Seien $\psi_1 , \ldots , \psi_v$ die irreduziblen Charaktere von H, mit ψ_1 trivial. Falls $H = 1$ ist, dann ist $v = 1$.

Sei

$$\alpha_u \ := \ \psi_u(1)\, \psi_1 - \psi_u \ \in \ \mathrm{V}(H)$$

für $u \in [2, v]$; cf. Definition 134. Es ist $\alpha_u(1) = 0$ stets.

Seien $\chi_1 , \ldots , \chi_t$ die irreduziblen Charaktere von G, mit χ_1 trivial.

Behauptung 1. Sei $\alpha \in \mathrm{V}(H)$. Ist $h \in \dot{H}$, dann ist $\alpha\uparrow_H^G(h) = \alpha(h)$.

Für $g \in G$ folgt aus ${}^g h \in H$, daß ${}^g H \cap H \neq 1$, nach Voraussetzung an H also $g \in H$ ist.

Da $\mathrm{V}(H) \subseteq \mathrm{Kf}(H)$ ist, wird somit

$$\begin{aligned} \alpha\uparrow_H^G(h) &= |H|^{-1} \textstyle\sum_{g \in G,\ {}^g h \in H} \alpha({}^g h) \\ &= |H|^{-1} \textstyle\sum_{g \in H} \alpha({}^g h) \\ &= |H|^{-1} \textstyle\sum_{g \in H} \alpha(h) \\ &= \alpha(h) \, . \end{aligned}$$

Dies zeigt *Behauptung* 1.

Behauptung 2. Sei $\alpha \in \mathrm{V}(H)$. Sei $n \in N$. Es ist $\alpha\uparrow_H^G(n) = 0$.

Es wird

$$\alpha\uparrow_H^G(n) \ = \ |H|^{-1} \sum_{g \in G,\ {}^g n \in H} \alpha({}^g n) \ = \ 0 \, ,$$

da ${}^g n \notin H$ nach Definition von N. Dies zeigt *Behauptung* 2.

Behauptung 3. Es ist $|N||H| = |G|$. Für $\alpha \in \mathrm{V}(H)$ mit $\alpha(1) = 0$ ist ${}_G(\alpha\uparrow_H^G , \alpha\uparrow_H^G) = {}_H(\alpha, \alpha)$.

Schreibe $G = \bigsqcup_{r \in R} rH$ für ein $R \subseteq G$. Nach Voraussetzung an H ist $H = \mathrm{N}_G(H)$ oder $H = 1$. Daher ist

$$G \ = \ \{1\} \sqcup \dot{N} \sqcup \bigsqcup\nolimits_{r \in R} {}^r\dot{H} \, .$$

Folglich ist

$$|G| = 1 + (|N| - 1) + \tfrac{|G|}{|H|}(|H| - 1) \ = \ |N| + |G| - \tfrac{|G|}{|H|} \, ,$$

i.e. $|N| = \frac{|G|}{|H|}$.

Ferner wird

$$\begin{aligned}
{}_G(\alpha\uparrow_H^G, \alpha\uparrow_H^G) &= |G|^{-1} \textstyle\sum_{g\in G} |\alpha\uparrow_H^G(g)|^2 \\
&= |G|^{-1}\big(|\alpha\uparrow_H^G(1)|^2 + (\textstyle\sum_{n\in\dot N} |\alpha\uparrow_H^G(n)|^2) + (\sum_{r\in R}\sum_{h\in\dot H} |\alpha\uparrow_H^G({}^r h)|^2)\big) \\
&= |G|^{-1}\big(|G||H|^{-1}\alpha(1)|^2 + (\textstyle\sum_{n\in\dot N} |\alpha\uparrow_H^G(n)|^2) + (\sum_{r\in R}\sum_{h\in\dot H} |\alpha\uparrow_H^G(h)|^2)\big) \\
&\overset{\text{Beh. } 1,2}{=} |G|^{-1}\big(0 + 0 + (\textstyle\sum_{r\in R}\sum_{h\in\dot H} |\alpha(h)|^2)\big) \\
&= |H|^{-1} \textstyle\sum_{h\in\dot H} |\alpha(h)|^2 \\
&= |H|^{-1} \textstyle\sum_{h\in H} |\alpha(h)|^2 \\
&= {}_H(\alpha,\alpha)\ .
\end{aligned}$$

Dies zeigt *Behauptung* 3.

Behauptung 4. Für $u \in [2,v]$ gibt es einen nichttrivialen irreduziblen Charakter χ von G mit $\alpha_u\uparrow_H^G = \psi_u(1)\,\chi_1 - \chi$. Wir können (und werden) dann die nichttrivialen irreduziblen Charaktere von G so umsortieren, daß $\alpha_u\uparrow_H^G = \psi_u(1)\,\chi_1 - \chi_u$ ist für $u \in [2,v]$.

Sei $u \in [2,v]$. Schreibe $\alpha_u\uparrow_H^G = \sum_{s\in[1,t]} z_s\chi_s$ mit $z_s \in \mathbf{Z}$. Es ist

$$z_1 \;=\; {}_G(\alpha_u\uparrow_H^G, \chi_1) \;=\; {}_H(\alpha_u, \chi_1\downarrow_H^G) \;=\; {}_H(\psi_u(1)\,\psi_1 - \psi_u, \psi_1) \;=\; \psi_u(1)\ .$$

Also wird zum einen

$${}_G(\alpha_u\uparrow_N^G, \alpha_u\uparrow_N^G) \overset{\text{Beh. } 3}{=} {}_G(\alpha_u, \alpha_u) \;=\; {}_H(\psi_u(1)\,\psi_1 - \psi_u, \psi_u(1)\,\psi_1 - \psi_u) \;=\; \psi_u(1)^2 + 1 \;=\; z_1^2 + 1\ ,$$

und zum anderen

$${}_G(\alpha_u\uparrow_N^G, \alpha_u\uparrow_N^G) \;=\; {}_G(\textstyle\sum_{s\in[1,t]} z_s\chi_s, \sum_{\tilde s\in[1,t]} z_{\tilde s}\chi_{\tilde s}) \;=\; \sum_{s\in[1,t]} z_s^2\ .$$

Ein Vergleich zeigt, daß $\sum_{s\in[2,t]} z_s^2 = 1$ ist, daß es also ein $s_0 \in [2,t]$ mit $z_s = \pm\partial_{s,s_0}$ für $s \in [2,t]$ gibt.

Wäre nun $z_{s_0} = 1$, dann wäre $\alpha_u\uparrow_H^G$ ein Charakter von G. Dies trifft aber wegen $\alpha_u\uparrow_H^G(1) = |G||H|^{-1}\alpha_u(1) = 0$ nicht zu. Also ist $z_s = -\partial_{s,s_0}$ für $s \in [2,t]$.

Für $u, \tilde u \in [2,v]$ mit $u \neq \tilde u$ ist auch $\alpha_u\uparrow_H^G \neq \alpha_{\tilde u}\uparrow_H^G$, da $\alpha_u \neq \alpha_{\tilde u}$ ist und da $\alpha_u\uparrow_H^G(h) = \alpha_u(h)$ ist für $h \in \dot H$ nach Behauptung 1, genauso für $\tilde u$.

Somit können wir die nichttrivialen irreduziblen Charaktere von G ohne Einschränkung so sortieren, daß $\alpha_u\uparrow_H^G = \psi_u(1)\,\chi_1 - \chi_u$ ist für $u \in [2,v]$, wie behauptet. Dies zeigt *Behauptung* 4.

Behauptung 5. Sei $u \in [2,v]$. Sei $g \in G$. Genau dann ist $\chi_u(g) = \psi_u(1)$, wenn $\alpha_u\uparrow_H^G(g) = 0$ ist.

In der Tat wird

$$\alpha_u\uparrow_H^G(g) \overset{\text{Beh. } 4}{=} \psi_u(1)\,\chi_1(g) - \chi_u(g) \;=\; \psi_u(1) - \chi_u(g)\ .$$

Dies zeigt *Behauptung* 5.

Behauptung 6. Sei $u \in [2,v]$. Es ist $\chi_u(1) = \psi_u(1)$. Für $g \in G$ ist genau dann $\chi_u(g) = \chi_u(1)$, wenn $\alpha_u\uparrow_H^G(g) = 0$ ist.

Es ist $\alpha_u\uparrow_H^G(1) = |G||H|^{-1}\alpha_u(1) = 0$. Dank Behauptung 5 ist also $\chi_u(1) = \psi_u(1)$.

Eine abermalige Anwendung von Behauptung 5 zeigt daher vollends die *Behauptung* 6.

Behauptung 7. Es ist $N = \tilde N := \bigcap_{u\in[2,v]} \operatorname{Kern}\chi_u \trianglelefteq G$. Es ist $NH = G$.

Zu $N \overset{!}{\leqslant} \tilde{N}$. Sei $n \in N$. Sei $u \in [2,v]$. Wir haben $\chi_u(n) \overset{!}{=} \chi_u(1)$ zu zeigen. Mit Behauptung 2 ist $\alpha_u\uparrow_H^G(n) = 0$, sodaß mit Behauptung 6 in der Tat $\chi_u(n) = \chi_u(1)$ folgt.

Sei

$$\varphi \;:=\; \chi_1 + \textstyle\sum_{u\in[2,v]} \chi_u(1)\,\chi_u \;.$$

Für $\tilde{n} \in \tilde{N}$ wird

$$\varphi(\tilde{n}) \;=\; \chi_1(\tilde{n}) + \textstyle\sum_{u\in[2,v]} \chi_u(1)\,\chi_u(\tilde{n}) \;=\; 1 + \textstyle\sum_{u\in[2,v]} \chi_u(1)\,\chi_u(1) \overset{\text{B. }6}{=} \sum_{u\in[1,v]} \psi_u(1)^2 \overset{\text{S. }90.(2)}{=} |H| \;.$$

Für $u \in [2,v]$ und $h \in \dot{H}$ wird

$$\chi_u(h) \overset{\text{Beh. }4}{=} \psi_u(1)\,\chi_1(h) - \alpha_u\uparrow_H^G(h) \overset{\text{Beh. }1}{=} \psi_u(1)\,\psi_1(h) - \alpha_u(h) \;=\; \psi_u(h) \;.$$

Für $h \in \dot{H}$ wird also

$$\varphi(h) \;=\; \chi_1(h) + \textstyle\sum_{u\in[2,v]} \chi_u(1)\,\chi_u(h) \;=\; 1 + \textstyle\sum_{u\in[2,v]} \chi_u(1)\,\chi_u(h) \overset{\text{Beh. }6}{=} \sum_{u\in[1,v]} \psi_u(1)\,\psi_u(h) \overset{\text{S. }90.(2)}{=} 0 \;.$$

Es folgt, daß $\tilde{N} \cap H = 1$ ist.

Also ist

$$\tfrac{|G|}{|N|} \overset{\text{Beh. }3}{=} |H| \;=\; \tfrac{|H|}{|\tilde{N}\cap H|} \overset{\text{B. }32}{=} \tfrac{|\tilde{N}H|}{|\tilde{N}|} \;\leqslant\; \tfrac{|\tilde{N}H|}{|N|} \;\leqslant\; \tfrac{|G|}{|N|} \;.$$

Folglich stehen überall Gleichheiten. Es folgt $|N| = |\tilde{N}|$, wegen $N \leqslant \tilde{N}$ mithin $N = \tilde{N}$. Weiter folgt $|\tilde{N}H| = |G|$, also $NH = \tilde{N}H = G$. Dies zeigt *Behauptung* 7.

Behauptung 8. Für $n \in \dot{N}$ ist $\mathrm{C}_G(n) \leqslant N$.

Sei $g \in \mathrm{C}_G(n)$ gegeben. Zu zeigen ist $g \overset{!}{\in} N$.

Da $G \overset{\text{Beh. }7}{=} NH$ ist, können wir $g = mh$ mit $m \in N$ und $h \in H$ schreiben. Zu zeigen ist $h \overset{!}{=} 1$.

Annahme, es ist $h \neq 1$. Es ist ${}^N h \subseteq Nh$, da $N \overset{\text{Beh. }7}{\trianglelefteq} G$.

Es ist $\mathrm{C}_G(h) \leqslant H$, da aus ${}^x h = h$ folgt, daß ${}^x H \cap H \neq 1$ und somit $x \in H$ ist.

Insbesondere ist $\mathrm{C}_N(h) = N \cap \mathrm{C}_G(h) \leqslant N \cap H \overset{\text{Beh. }7}{=} 1$. Also wird

$$|{}^N h| \overset{\text{L. }5}{=} \tfrac{|N|}{|\mathrm{C}_N(h)|} \;=\; |N| \;,$$

und somit ${}^N h = Nh$. Schreibe demgemäß $g = mh = \tilde{m}h\tilde{m}^-$ für ein $\tilde{m} \in N$.

Nun ist

$$n \;=\; gng^- \;=\; \tilde{m}h\tilde{m}^- n \tilde{m} h^- \tilde{m}^- \;,$$

also

$$(\tilde{m}^- n \tilde{m})h = h(\tilde{m}^- n \tilde{m}) \;,$$

und somit $\tilde{m}^- n \tilde{m} \in \mathrm{C}_N(h) = 1$. Aber da $n \neq 1$, ist auch $\tilde{m}^- n \tilde{m} \neq 1$, und wir haben einen *Widerspruch.* Dies zeigt *Behauptung* 8.

Behauptung 9. Es ist $\mathrm{ggT}(|N|, |H|) = 1$.

Sei p ein Primteiler von $|N|$. Wir haben zu zeigen, daß p kein Teiler von $|H|$ ist.

Sei $Q \leqslant N$ eine p-Sylowgruppe. Sei P eine p-Sylowgruppe von G mit $Q \leqslant P$. Cf. Sätze 13 und 15.

Wir haben zu zeigen, daß $Q \overset{!}{=} P$. Denn dann ist p kein Teiler von $|G|/|Q|$, und, da $|Q|$ ein Teiler von $|N|$ ist, also auch kein Teiler von

$$|G|/|N| \overset{\text{Beh. 7}}{=} |NH|/|N| \overset{\text{B. 32}}{=} |H|/|N \cap H| \;=\; |H| \,.$$

Wegen der Maximalität von Q genügt es zu zeigen, daß $P \overset{!}{\leqslant} N$ ist.

Da p ein Primteiler von N ist, ist $1 < Q \leqslant P$. Also ist auch $\mathrm{Z}(P) \neq 1$; cf. Aufgabe 6. Wähle ein $z \in \mathrm{Z}(P)$ mit $z \neq 1$. Wähle ein $q \in Q$ mit $q \neq 1$. Da $q \in P \cap N$ liegt, wird

$$z \;\in\; \mathrm{C}_G(q) \overset{\text{Beh. 8}}{\leqslant} N \,.$$

Somit ist

$$P \;\leqslant\; \mathrm{C}_G(z) \overset{\text{Beh. 8}}{\leqslant} N \,.$$

Dies zeigt *Behauptung* 9.

Ist $1 < H < G$, dann heißt solch eine Gruppe G auch eine *Frobeniusgruppe*. Die Aussage $N \trianglelefteqslant G$ ist ein Satz von Frobenius, für welchen es meines Wissens zur Zeit (2011) keinen Beweis ohne Charaktertheorie gibt; cf. **[2]** und mathoverflow.net/questions/63142/.

Aufgabe 50

Die Aussage ist falsch.

Sei $G = \mathrm{C}_6$, erzeugt von einem Element c von Ordnung 6. Schreibe $U := \langle c^3 \rangle \leqslant G$ und $V := \langle c^2 \rangle \leqslant G$. Es ist

$$M \;=\; \{\, 1,\, U,\, V \,\} \,.$$

Sei φ ein Charakter von U. Da U und G abelsch sind, wird mit Korollar 118

$$\varphi\big\uparrow_U^G(c) \;=\; \sum_{u \,\in\, U} \frac{|\mathrm{C}_G(u)|}{|\mathrm{C}_H(u)|} \cdot \partial_{G_u \,, G_c} \cdot \varphi(u) \;=\; \sum_{u \,\in\, U} \frac{|G|}{|U|} \cdot \partial_{u,c} \cdot \varphi(u) \;=\; 0 \,.$$

Genauso wird auch $\varphi\big\uparrow_V^G(c) = 0$ für jeden Charakter φ von V; sowie $\varphi\big\uparrow_1^G(c) = 0$ für jeden Charakter φ von 1.

Somit ist der triviale Charakter χ_1 von G nicht $\mathbf{Z}$-Linearkombination aus von Untergruppen aus M nach G induzierten Charakteren, da ja $\chi_1(c) = 1$.

Cf. Satz 161. Beachte, daß M eine Teilmenge der fastzyklischen Untergruppen von G ist.

Aufgabe 51

Sei $R \subseteq G$ so, daß $G = \bigsqcup_{x \in R} xU$ ist. Sei $S \subseteq H$ so, daß $H = \bigsqcup_{y \in S} yV$ ist.

Dann ist $G \times H = \bigsqcup_{(x,y) \in R \times S} (x,y)(U \times V)$.

Für $(g,h) \in G \times H$ wird

$$\begin{aligned}
(\varphi \boxdot \psi)\restriction_{U\times V}^{G\times H}\big((g,h)\big) &= \sum_{(x,y)\,\in\, R\times S,\ {}^{(x,y)}(g,h)\,\in\, U\times V} (\varphi \boxdot \psi)({}^{(x,y)}(g,h)) \\
&= \sum_{x\,\in\, R,\ {}^{x}g\,\in\, U} \ \sum_{y\,\in\, S,\ {}^{y}h\,\in\, V} \varphi({}^{x}g)\cdot\psi({}^{y}h) \\
&= \big(\sum_{x\,\in\, R,\ {}^{x}g\,\in\, U} \varphi({}^{x}g)\big)\cdot\big(\sum_{y\,\in\, S,\ {}^{y}h\,\in\, V} \psi({}^{y}h)\big) \\
&= \varphi\restriction_U^G(g)\cdot\psi\restriction_V^H(h) \\
&= (\varphi\restriction_U^G \boxdot \psi\restriction_V^H)\big((g,h)\big)\ .
\end{aligned}$$

Aufgabe 52

Wir wollen das Problem von G auf A_5 **reduzieren.**

Es ist $|G| = (4^2-1)(4^2-4) = 2^2\cdot 3^2\cdot 5 = 180$.

Seien $\ell_1 := \langle\binom{1}{0}\rangle$, $\ell_2 := \langle\binom{1}{1}\rangle$, $\ell_3 := \langle\binom{1}{\alpha}\rangle$, $\ell_4 := \langle\binom{1}{\alpha^2}\rangle$, $\ell_5 := \langle\binom{0}{1}\rangle$.

Die Menge $\{\,\ell_i\,:\,i\in[1,5]\,\}$ der Geraden, also der eindimensionalen Teilräume, von $\mathbf{F}_4^2$ wird eine G-Menge unter Verwendung der Tatsache, daß für $g\in G$, also für einen Isomorphismus g von $\mathbf{F}_4^2$ nach $\mathbf{F}_4^2$, auch das Bild einer Geraden unter diesem Isomorphismus g wieder eine Gerade ist.

Definieren wir $\sigma(g)\in \mathrm{S}_5$ durch wir $\ell_{\sigma(g)(i)} := g\ell_i$ für $i\in[1,5]$, so erhalten wir einen Gruppenmorphismus

$$\begin{array}{ccc} G & \xrightarrow{\ \sigma\ } & \mathrm{S}_5 \\ g & \longmapsto & \sigma(g)\ . \end{array}$$

Denn in der Tat ist

$$\ell_{\sigma(gh)(i)} \;=\; gh\ell_i \;=\; g\ell_{\sigma(h)(i)} \;=\; \ell_{\sigma(g)\sigma(g)(i)}$$

für $i\in[1,5]$ und $g,\,h\,\in\,G$, und also $\sigma(gh)=\sigma(g)\circ\sigma(h)$ für $g,\,h\,\in\,G$.

Cf. Aufgabe 8.(2).

Wir wollen den Kern von σ berechnen. Es ist $g\in\operatorname{Kern}\sigma$ genau dann, wenn $\sigma\ell_i=\ell_i$ für alle $i\in[1,5]$. Also ist $\{\,s\cdot \mathrm{E}_2\,:\,s\in\mathrm{U}(\mathbf{F}_4)\,\}\leqslant\operatorname{Kern}\sigma$. Wir wollen hierin die Gleichheit zeigen. Sei $\sigma(g)=1$. Schreibe $g=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ mit $a,\,b,\,c,\,d\,\in\,\mathbf{F}_4$. Aus $g\ell_1=\ell_1$ folgt $c=0$. Aus $g\ell_5=\ell_5$ folgt $b=0$. Aus $g\ell_2=\ell_2$ folgt nun $a=d$.

Folglich ist $I:=\sigma(G)\leqslant\mathrm{S}_5$ eine Untergruppe der Ordnung 60. Da $\mathrm{S}_5 = I\sqcup\tau I = I\sqcup I\tau$ für $\tau\in\mathrm{S}_5\smallsetminus I$, ist $\tau I = I\tau$ für $\tau\in\mathrm{S}_5$, folglich $I\trianglelefteqslant\mathrm{S}_5$. Da $\mathrm{A}_5/(I\cap\mathrm{A}_5)\xrightarrow{\sim} I\mathrm{A}_5/\mathrm{A}_5$ ist und da entweder $I\mathrm{A}_5=\mathrm{A}_5$ oder $I\mathrm{A}_5=\mathrm{S}_5$ ist, ist entweder $I=\mathrm{A}_5$ oder $I\cap\mathrm{A}_5$ ein Normalteiler der Ordnung 30 in A_5. Da es letzteren nach Aufgabe 11.(2) nicht geben kann, folgt $I=\mathrm{A}_5$.

Wir *behaupten* folgenden Gruppenisomorphismus.

$$\begin{array}{ccccc} G & \xrightarrow{\ \sim\ } & \mathrm{A}_5 & \times & \mathrm{U}(\mathbf{F}_4) \\ g & \longmapsto & (\sigma(g) & , & \det(g)) \end{array}$$

Es genügt, die Surjektivität zu zeigen. Da σ die Untergruppe A_5 als Bild hat, folgt dies bereits aus $\left(\begin{smallmatrix}\alpha&0\\0&\alpha\end{smallmatrix}\right)\longmapsto(\mathrm{id},\alpha^2)$. Dies zeigt die *Behauptung.*

Beachte, daß $\mathrm{U}(\mathbf{F}_4) \simeq \mathrm{C}_3$.

Ohne Einschränkung können wir also G durch $\mathrm{A}_5 \times \mathrm{C}_3$ wechseln. Sei $\mathrm{C}_3 = \langle c \rangle$.

Sei M' eine minimale Menge von fastzyklischen Untergruppen von A_5 mit der Eigenschaft, daß

$$\begin{array}{ccc} \bigoplus_{U \in M'} \mathrm{V}(U) & \xrightarrow{\ \mathrm{ind}\uparrow_{M'}^{\mathrm{A}_5}\ } & \mathrm{V}(\mathrm{A}_5) \\ (\varphi_U)_{U \in M'} & \longmapsto & \sum_{U \in M'} \varphi_U\uparrow_U^{\mathrm{A}_5} \end{array}$$

surjektiv ist, i.e. daß jeder irreduzible Charakter von $\mathrm{A}_5 \times \mathrm{C}_3$ eine $\mathbf{Z}$-Linearkombination aus von Untergruppen aus M nach A_5 induzierten Charakteren ist.

Sei $M := \{\, U \times \mathrm{C}_3 \,:\, U \in M' \,\}$. Wir *behaupten,* daß M eine minimale Menge ist wie in der Aufgabe verlangt.

Zunächst sollte M aus fastzyklischen Untergruppen bestehen. Sei $U \in M'$. Schreibe $U \simeq C \times P$, wobei $p \in \{2,3,5\}$, C zyklisch von Ordnung teilerfremd zu p und P eine p-Gruppe. Dann ist $C \times P \times \mathrm{C}_3$ fastzyklisch, falls $p = 3$ oder falls ($p \in \{2,5\}$ und P zyklisch) oder falls ($p \in \{2,5\}$ und $|C| \not\equiv_3 0$). Zu betrachten bleibt also der Fall $p = 2$ und $P \simeq \mathrm{D}_8$, wobei dann $C \simeq \mathrm{C}_3$. Es gibt aber in A_5 keine Untergruppe isomorph zu $\mathrm{D}_8 \times \mathrm{C}_3$, da $\mathrm{C}_{\mathrm{A}_5}\big((1,2,3)\big) = \langle (1,2,3) \rangle$, da $20 = |\,^{\mathrm{S}_5}(1,2,3)| = |\,^{\mathrm{A}_5}(1,2,3)|$; cf. Lösung zu Aufgabe 42.(2).

Zeigen wir die Surjektivität von $\mathrm{ind}\uparrow_M^{\mathrm{A}_5 \times \mathrm{C}_3}$. Sei χ ein irreduzibler Charakter von A_5 . Sei ψ ein irreduzibler Charakter von C_3 . Nach Voraussetzung ist $\chi = \sum_{i \in [1,r]} z_i \varphi_i\uparrow_{U_i}^{\mathrm{A}_5}$, wobei $r \geqslant 0$ ist, wobei $z_i \in \mathbf{Z}$ und $U_i \in M'$ sind für $i \in [1,r]$ und wobei φ_i ein irreduzibler Charakter von U_i ist für $i \in [1,r]$. Mit Aufgabe 51 ist also auch

$$\chi \boxdot \psi \;=\; \sum_{i \in [1,r]} z_i \varphi_i\uparrow_{U_i}^{\mathrm{A}_5} \boxdot \psi \;=\; \sum_{i \in [1,r]} z_i (\varphi_i \boxdot \psi)\uparrow_{U_i \times \mathrm{C}_3}^{\mathrm{A}_5 \times \mathrm{C}_3} .$$

Nach Aufgabe 41 und obiger Behauptung zeigt dies, daß jeder irreduzible und damit jeder Charakter von $\mathrm{A}_5 \times \mathrm{C}_3$ eine $\mathbf{Z}$-Linearkombination aus von Untergruppen aus M nach $\mathrm{A}_5 \times \mathrm{C}_3$ induzierten Charakteren ist.

Zeigen wir nun die diesbezügliche Minimalität von M.

Sei $N \subset M$ eine echte Teilmenge von M. Sei *angenommen,* $\mathrm{ind}\uparrow_N^{\mathrm{A}_5 \times \mathrm{C}_3}$ sei surjektiv.

Sei $N' = \{\, U \leqslant \mathrm{A}_5 \,:\, U \times \mathrm{C}_3 \in N \,\}$. Es ist $N' \subset M'$, denn für $U, \tilde{U} \leqslant \mathrm{A}_5$ folgt aus $U \times \mathrm{C}_3 = \tilde{U} \times \mathrm{C}_3$, daß $U = \tilde{U}$ ist.

Sei ψ_0 der triviale Charakter von C_3 .

Wegen der Minimalität von M' gibt es einen Charakter χ von A_5 , welcher nicht im Bild von $\mathrm{ind}\uparrow_{N'}^{\mathrm{A}_5}$ liegt. Dahingegen ist dank Aufgabe 41

$$\chi \boxdot \psi_0 \;=\; \sum_{i \in [1,r]} z_i (\varphi_i \boxdot \psi_i)\uparrow_{U_i \times \mathrm{C}_3}^{\mathrm{A}_5 \times \mathrm{C}_3} \;=\; \sum_{i \in [1,r]} z_i \varphi_i\uparrow_{U_i}^{\mathrm{A}_5} \boxdot \psi_i \;,$$

für $r \geqslant 0$, $z_i \in \mathbf{Z}$ und $U_i \in N'$, und irreduzible Charaktere φ_i von A_5 und ψ_i von C_3 geeignet gewählt. Einschränken dieser Gleichheit auf A_5 liefert wegen $\psi_0(1) = 1$ und $\psi_i(1) = 1$ für $i \in [1,r]$ die Gleichheit

$$\chi \;=\; (\chi \boxdot \psi_0)\downarrow_{\mathrm{A}_5}^{\mathrm{A}_5 \times \mathrm{C}_3} \;=\; \sum_{i \in [1,r]} z_i (\varphi_i\uparrow_{U_i}^{\mathrm{A}_5} \boxdot \psi_i)\downarrow_{\mathrm{A}_5}^{\mathrm{A}_5 \times \mathrm{C}_3} \;=\; \sum_{i \in [1,r]} z_i \varphi_i\uparrow_{U_i}^{\mathrm{A}_5} \;,$$

und dies steht im *Widerspruch* dazu, daß χ nicht im Bild von $\mathrm{ind}\uparrow_{N'}^{\mathrm{A}_5}$ liegt.

Dies zeigt die *Behauptung.*

Es bleibt also eine Menge M' wie beschrieben zu bestimmen, also bestehend aus fastzyklischen Untergruppen von A_5 mit der Eigenschaft, daß

$$\begin{array}{ccc} \bigoplus_{U\in M'} \mathrm{V}(U) & \xrightarrow{\ \mathrm{ind}\downarrow_{M'}^{\mathrm{A}_5}\ } & \mathrm{V}(\mathrm{A}_5) \\ (\varphi_U)_{U\in M'} & \longmapsto & \sum_{U\in M'} \varphi_U\uparrow_U^{\mathrm{A}_5} \end{array}$$

surjektiv ist, i.e. daß jeder irreduzible Charakter von A_5 eine $\mathbf{Z}$-Linearkombination aus von Untergruppen aus M nach A_5 induzierten Charakteren ist.

Zunächst soll nun die **Charaktertafel von** A_5 erstellt werden. Was die Charaktertafel von S_5 angeht, cf. Lösung zu Aufgabe 42.(2). Das Bahnenlemma, Lemma 5, werde stillschweigend verwendet.

Es ist $\mathrm{C}_{\mathrm{S}_5}((1,2,3)) = \langle (1,2,3),(4,5)\rangle$, von Ordnung 6, woraus $\mathrm{C}_{\mathrm{A}_5}((1,2,3)) < \mathrm{C}_{\mathrm{S}_5}((1,2,3))$, und also $\mathrm{C}_{\mathrm{A}_5}((1,2,3)) = \langle (1,2,3)\rangle$, von Ordnung 3, folgt; was zur Folge hat, daß $|\,^{\mathrm{A}_5}(1,2,3)| = 20$ ist, i.e. $^{\mathrm{A}_5}(1,2,3) = {}^{\mathrm{S}_5}(1,2,3)$.

Es ist desweiteren $\mathrm{C}_{\mathrm{S}_5}((1,2)(3,4)) = \langle (1,2),(3,4),(1,3)(2,3)\rangle$, von Ordnung 8, woraus $\mathrm{C}_{\mathrm{A}_5}((1,2)(3,4)) < \mathrm{C}_{\mathrm{S}_5}((1,2)(3,4))$, und also $\mathrm{C}_{\mathrm{A}_5}((1,2)(3,4)) = \langle (1,2)(3,4),(1,3)(2,4)\rangle$, von Ordnung 4, folgt; was zur Folge hat, daß $|\,^{\mathrm{A}_5}(1,2)(3,4)| = 20$ ist, i.e. $^{\mathrm{A}_5}(1,2)(3,4) = {}^{\mathrm{S}_5}(1,2)(3,4)$.

Schließlich ist $\mathrm{C}_{\mathrm{S}_5}((1,2,3,4,5)) = \langle (1,2,3,4,5)\rangle$, von Ordnung 5, woraus $\mathrm{C}_{\mathrm{A}_5}((1,2,3,4,5)) = \mathrm{C}_{\mathrm{S}_5}((1,2,3,4,5))$ folgt; was zur Folge hat, daß $|\,^{\mathrm{A}_5}(1,2,3,4,5)| = 12$ ist. Wir *behaupten*, daß $^{(4,5)}(1,2,3,4,5) = (1,2,3,5,4)$ und $(1,2,3,4,5)$ in A_5 nicht zueinander konjugiert sind. *Wäre* dem so, dann wäre $^{(4,5)}(1,2,3,4,5) = {}^{\tau}(1,2,3,4,5)$ für ein $\tau \in \mathrm{A}_5$, also $(4,5)\circ\tau \in \mathrm{C}_{\mathrm{S}_5}((1,2,3,4,5)) \leqslant \mathrm{A}_5$ und somit $\tau \in (4,5)\mathrm{A}_5$, was *nicht* der Fall ist. Genau wie eben folgt nun auch, daß $|\,^{\mathrm{A}_5}(1,2,3,5,4)| = 12$ ist.

Wir ordnen Konjugationsklassenrepräsentanten von A_5 wie folgt an, darunter die Konjugationsklassenlängen.

id	$(1,2,3)$	$(1,2)(3,4)$	$(1,2,3,4,5)$	$(1,2,3,5,4)$
1	20	15	12	12

Wir schreiben Charaktere dementsprechend als Zeilenvektoren.

Sei $\psi_1 := (1\,1\,1\,1\,1)$ der triviale Charakter.

Sei $\psi_2 := \chi_{5,3}\downarrow_{\mathrm{A}_5}^{\mathrm{S}_5} = (4\,1\,0\,{-1}\,{-1})$. Es ist ${}_{\mathrm{A}_5}\langle\psi_2\,,\,\psi_2\rangle = \frac{1}{60}(4\cdot4\cdot1+1\cdot1\cdot20+0\cdot0\cdot15+(-1)\cdot(-1)\cdot12+(-1)\cdot(-1)\cdot12) = 1$. Also ist ψ_2 irreduzibel.

Sei $\psi_3 := \chi_{5,6}\downarrow_{\mathrm{A}_5}^{\mathrm{S}_5} = (5\,{-1}\,1\,0\,0)$. Es ist ${}_{\mathrm{A}_5}\langle\psi_3\,,\,\psi_3\rangle = \frac{1}{60}(5\cdot5\cdot1+(-1)\cdot(-1)\cdot20+1\cdot1\cdot15+0\cdot0\cdot12+0\cdot0\cdot12) = 1$. Also ist ψ_3 irreduzibel.

Es fehlen uns noch zwei weitere irreduzible Charaktere von A_5, genannt ψ_4 und ψ_5.

Aus $\psi_1(1)^2+\psi_2(1)^2+\psi_3(1)^2+\psi_4(1)^2+\psi_5(1)^2 = 60$ und $\psi_4(1)$, $\psi_5(1) \in \mathbf{Z}_{\geqslant 1}$ folgt, daß $\psi_4(1) = 3$ und $\psi_5(1) = 3$ ist. Wir setzen

$$\begin{array}{rcl} \psi_4 & =: & (3\,u\;\;v\;\;x\;\;y) \\ \psi_5 & =: & (3\,u'\;v'\;x'\;y') \end{array},$$

wobei u, v, x, y, u', v', x', $y' \in \mathcal{O}$, so daß nach unserem momentanen Kenntnisstand die Charaktertafel von A_5 die folgende Gestalt hat.

$$X(\mathrm{A}_5) = \begin{array}{c|ccccc} & \mathrm{id} & (1,2,3) & (1,2)(3,4) & (1,2,3,4,5) & (1,2,3,5,4) \\ & 1 & 20 & 15 & 12 & 12 \\ \hline \psi_1 & 1 & 1 & 1 & 1 & 1 \\ \psi_2 & 4 & 1 & 0 & -1 & -1 \\ \psi_3 & 5 & -1 & 1 & 0 & 0 \\ \psi_4 & 3 & u & v & x & y \\ \psi_5 & 3 & u' & v' & x' & y' \end{array}$$

Sei $\sigma := (4,5)$. Sei $c_\sigma : \mathrm{A}_5 \longrightarrow \mathrm{A}_5\,,\ \tau \longmapsto {}^{\sigma}\tau$; cf. Satz 123, Beispiel 126.

Zu ψ_4 gibt es nun den irreduziblen Charakter $\psi_4 \circ c_\sigma$; cf. Aufgabe 33.(4).

Aus Gradgründen kann nun nur $\psi_4 \circ c_\sigma = \psi_4$ oder $\psi_4 \circ c_\sigma = \psi_5$ sein.

Ersteres *hieße* zum einen $(3\ u\ v\ y\ x) = (3\ u\ v\ x\ y)$, also $x = y$; zum anderen aber auch $\psi_5 \circ c_\sigma = \psi_5$, also $x' = y'$. Die vertikale Orthogonalitätsrelation für die letzten beiden Spalten gäbe $0 = 1 \cdot 1 + (-1) \cdot (-1) + 0 \cdot 0 + x \cdot \overline{x} + x' \cdot \overline{x'}$, also $|x|^2 + |x'|^2 = -2$, was *nicht* geht.

Also gilt zweiteres, i.e. $\psi_4 \circ c_\sigma = \psi_5$. Somit ist $u = u'$ und $v = v'$ und $x = y'$ und $x' = y$. Die Charaktertafel von A_5 hat nach momentanem Kenntnisstand die folgende Form.

$$X(\mathrm{A}_5) \;=\; \begin{array}{c} \\ \psi_1 \\ \psi_2 \\ \psi_3 \\ \psi_4 \\ \psi_5 \end{array} \begin{array}{c} \begin{array}{ccccc} \mathrm{id} & (1,2,3) & (1,2)(3,4) & (1,2,3,4,5) & (1,2,3,5,4) \\ 1 & 20 & 15 & 12 & 12 \end{array} \\ \left[\begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \\ 4 & 1 & 0 & -1 & -1 \\ 5 & -1 & 1 & 0 & 0 \\ 3 & u & v & x & y \\ 3 & u & v & y & x \end{array}\right] \end{array}$$

Die vertikale Orthogonalitätsrelation für die erste und die zweite Spalte gibt

$$0 \;=\; 1 \cdot 1 + 4 \cdot 1 + 5 \cdot (-1) + 3 \cdot u + 3 \cdot u \;=\; 6u\,,$$

und also $u = 0$.

Die vertikale Orthogonalitätsrelation für die erste und die dritte Spalte gibt

$$0 \;=\; 1 \cdot 1 + 4 \cdot 0 + 5 \cdot 1 + 3 \cdot v + 3 \cdot v \;=\; 6 + 6v\,,$$

und also $v = -1$.

Die vertikale Orthogonalitätsrelation für die vierte mit der dritten Spalte gibt nun $0 = 1 \cdot 1 + (-1) \cdot 0 + 0 \cdot 1 + x \cdot (-1) + y \cdot (-1)$, also $y = 1 - x$.

Die Charaktertafel von A_5 hat nach momentanem Kenntnisstand die folgende Form.

$$X(\mathrm{A}_5) \;=\; \begin{array}{c} \\ \psi_1 \\ \psi_2 \\ \psi_3 \\ \psi_4 \\ \psi_5 \end{array} \begin{array}{c} \begin{array}{ccccc} \mathrm{id} & (1,2,3) & (1,2)(3,4) & (1,2,3,4,5) & (1,2,3,5,4) \\ 1 & 20 & 15 & 12 & 12 \end{array} \\ \left[\begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \\ 4 & 1 & 0 & -1 & -1 \\ 5 & -1 & 1 & 0 & 0 \\ 3 & 0 & -1 & x & 1-x \\ 3 & 0 & -1 & 1-x & x \end{array}\right] \end{array}$$

Mit $\psi_4 = (3\ 0\ -1\ x\ \ 1-x)$ ist nun auch $\overline{\psi_4} = (3\ 0\ -1\ \overline{x}\ \ 1-\overline{x})$ ein irreduzibler Charakter von A_5 ; cf. Aufgabe 25.(3).

Wäre $x \notin \mathbf{R}$, dann wäre $\overline{\psi_4} = \psi_5$. Die horizontale Orthogonalitätsrelation gäbe $0 = {}_{\mathrm{A}_5}\langle \psi_4\,,\, \psi_5 \rangle = \frac{1}{60}(1 \cdot 3 \cdot 3 + 20 \cdot 0 \cdot 0 + 15 \cdot (-1) \cdot (-1) + 12 \cdot x \cdot x + 12 \cdot (1-x) \cdot (1-x))$, also $x^2 - x + \frac{3}{2} = 0$, also $x = \frac{1}{2}(1 \pm \mathrm{i}\sqrt{5})$, also $x \cdot \overline{x} = \frac{3}{2} \notin \mathbf{Z} = \mathcal{O} \cap \mathbf{Q}$. Aber mit $x \in \mathcal{O}$ ist auch $\overline{x} \in \mathcal{O}$, und somit $x \cdot \overline{x} \in \mathcal{O}$, und wir haben einen *Widerspruch.*

Also ist $x \in \mathbf{R}$. Dann aber gibt die horizontale Orthogonalitätsrelation $1 = {}_{\mathrm{A}_5}\langle \psi_4\,,\, \psi_4 \rangle = \frac{1}{60}(1 \cdot 3 \cdot 3 + 20 \cdot 0 \cdot 0 + 15 \cdot (-1) \cdot (-1) + 12 \cdot x \cdot x + 12 \cdot (1-x) \cdot (1-x))$, also $x^2 - x - 1 = 0$, also $x = \frac{1}{2}(1 \pm \sqrt{5})$.

Nach eventuellem Vertauschen von ψ_4 und ψ_5 erhalten wir also

$$X(\mathrm{A}_5) = \begin{array}{c} \\ \psi_1 \\ \psi_2 \\ \psi_3 \\ \psi_4 \\ \psi_5 \end{array} \begin{array}{c} \begin{array}{ccccc} \mathrm{id} & (1,2,3) & (1,2)(3,4) & (1,2,3,4,5) & (1,2,3,5,4) \\ 1 & 20 & 15 & 12 & 12 \end{array} \\ \left[\begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \\ 4 & 1 & 0 & -1 & -1 \\ 5 & -1 & 1 & 0 & 0 \\ 3 & 0 & -1 & \frac{1}{2}(1+\sqrt{5}) & \frac{1}{2}(1-\sqrt{5}) \\ 3 & 0 & -1 & \frac{1}{2}(1-\sqrt{5}) & \frac{1}{2}(1+\sqrt{5}) \end{array}\right] \end{array} .$$

Wir können nun auch Beispiel 126 nochmals illustrieren. In der dortigen Notation können wir $D = \{\mathrm{id}, (4,5)\} = \{1, \sigma\}$ nehmen. Es ist $\psi_4 \circ c_\sigma = \psi_5 \neq \psi_4$. Also ist ${\psi_4}_{\restriction \mathrm{A}_5}^{\mathrm{S}_5}$ irreduzibel nach Mackey. In der Tat wird, wenn wir ψ_4 mit dem Wert 0 auf ganz S_5 fortsetzen,

$$\begin{array}{lcll} {\psi_4}_{\restriction \mathrm{A}_5}^{\mathrm{S}_5}(\mathrm{id}) & = & 2 \cdot \psi_4(\mathrm{id}) & = \quad 6 \\ {\psi_4}_{\restriction \mathrm{A}_5}^{\mathrm{S}_5}((1,2)) & = & \psi_4((1,2)) + \psi_4({}^{\sigma}(1,2)) & = \quad 0 \\ {\psi_4}_{\restriction \mathrm{A}_5}^{\mathrm{S}_5}((1,2,3)) & = & \psi_4((1,2,3)) + \psi_4({}^{\sigma}(1,2,3)) & = \quad 0 \\ {\psi_4}_{\restriction \mathrm{A}_5}^{\mathrm{S}_5}((1,2,3,4)) & = & \psi_4((1,2,3,4)) + \psi_4({}^{\sigma}(1,2,3,4)) & = \quad 0 \\ {\psi_4}_{\restriction \mathrm{A}_5}^{\mathrm{S}_5}((1,2,3,4,5)) & = & \psi_4((1,2,3,4,5)) + \psi_4({}^{\sigma}(1,2,3,4,5)) & = \quad 1 \\ {\psi_4}_{\restriction \mathrm{A}_5}^{\mathrm{S}_5}((1,2)(3,4)) & = & \psi_4((1,2)(3,4)) + \psi_4({}^{\sigma}(1,2)(3,4)) & = -2 \\ {\psi_4}_{\restriction \mathrm{A}_5}^{\mathrm{S}_5}((1,2,3)(4,5)) & = & \psi_4((1,2,3)(4,5)) + \psi_4({}^{\sigma}(1,2,3)(4,5)) & = \quad 0\,, \end{array}$$

und somit ${\psi_4}_{\restriction \mathrm{A}_5}^{\mathrm{S}_5} = (\,6\;0\;0\;0\;1\;-2\;0\,) = \chi_{5,5}$ in der Notation der Lösung zur Aufgabe 42.(2).

Nun zur **Bestimmung einer Menge M'.**

Sei $\mathrm{V}_4 := \langle (1,2)(3,4)\,,\, (1,3)(2,4) \rangle$. Es ist V_4 abelsch und hat die Repräsentanten der (einelementigen) Konjugationsklassen id, $(1,2)(3,4)$, $(1,3)(2,4)$ und $(1,4)(2,3)$. Ein Charakter von V_4 ist gerade ein Gruppenmorphismus von V_4 nach $\mathrm{U}(\mathbf{C})$. Wir schreiben solche Charaktere als Zeilenvektoren bezüglich der wie eben angegeben geordneten Konjugationsklassenrepräsentanten. Für einen Charakter φ von V_4 wird mit Korollar 118

$$\begin{array}{lcl} \varphi{\uparrow}_{\mathrm{V}_4}^{\mathrm{A}_5}(\mathrm{id}) & = & 15 \cdot \varphi(\mathrm{id}) \\ \varphi{\uparrow}_{\mathrm{V}_4}^{\mathrm{A}_5}((1,2)(3,4)) & = & \varphi((1,2)(3,4)) + \varphi((1,3)(2,4)) + \varphi((1,4)(2,3))\,. \end{array}$$

Alle anderen Werte sind null. Eine Koeffizientenberechnung via Skalarprodukte liefert

$$\begin{array}{lcll} (\,1\;1\;1\;1\,){\uparrow}_{\mathrm{V}_4}^{\mathrm{A}_5} & = & (\,15\;0\;3\;0\;0\,) & = \quad \psi_1 + \psi_2 + 2\psi_3 \\ (\,1\;1\;-1\;-1\,){\uparrow}_{\mathrm{V}_4}^{\mathrm{A}_5} & = & (\,15\;0\;-1\;0\;0\,) & = \quad \psi_2 + \psi_3 + \psi_4 + \psi_5\,. \end{array}$$

Die weiteren irreduziblen Charaktere von V_4, viz. $(\,1\;-1\;1\;-1\,)$ und $(\,1\;-1\;-1\;1\,)$, liefern dann nichts neues mehr.

Sei $\mathrm{C}_5 := \langle (1,2,3,4,5) \rangle$. Es ist C_5 abelsch und hat die Repräsentanten der (einelementigen) Konjugationsklassen id, $(1,2,3,4,5)$, $(1,3,5,2,4)$, $(1,4,2,5,3)$ und $(1,5,4,3,2)$. In S_5 ist $(1,3,5,2,4) = {}^{(2,3,5,4)}(1,2,3,4,5)$, $(1,4,2,5,3) = {}^{(2,4,5,3)}(1,2,3,4,5)$, $(1,5,4,3,2) = {}^{(2,5)(3,4)}(1,2,3,4,5)$, sodaß $(1,2,3,4,5)$ und $(1,5,4,3,2)$ in A_5 zu $(1,2,3,4,5)$ konjugiert sind, und $(1,3,5,2,4)$ und $(1,4,2,5,3)$ zu $(1,2,3,5,4)$. Ein Charakter von C_5 ist gerade ein Gruppenmorphismus von C_5 nach $\mathrm{U}(\mathbf{C})$; cf. Beispiel 86.(2). Wir schreiben solche Charaktere als Zeilenvektoren bezüglich der wie eben angegeben geordneten Konjugationsklassenrepräsentanten. Sei $\zeta_5 := \exp(2\pi\mathrm{i}/5)$. Für einen Charakter φ von C_5 wird mit Korollar 118

$$\begin{array}{lcl} \varphi{\uparrow}_{\mathrm{V}_4}^{\mathrm{A}_5}(\mathrm{id}) & = & 12 \cdot \varphi(\mathrm{id}) \\ \varphi{\uparrow}_{\mathrm{V}_4}^{\mathrm{A}_5}((1,2,3,4,5)) & = & \varphi((1,2,3,4,5)) + \varphi((1,5,4,3,2)) \\ \varphi{\uparrow}_{\mathrm{V}_4}^{\mathrm{A}_5}((1,2,3,5,4)) & = & \varphi((1,3,5,2,4)) + \varphi((1,4,2,5,3))\,. \end{array}$$

Alle anderen Werte sind null. Eine Koeffizientenberechnung via Skalarprodukte liefert

$$\begin{array}{lcll} (1\,1\,1\,1\,1)\restriction_{\mathrm{C}_5}^{\mathrm{A}_5} & = & (\,12\;\;0\;\;0\;\;2\;\;2\,) & = \psi_1+\psi_3+\psi_4+\psi_5 \\ (1\,\zeta_5\,\zeta_5^2\,\zeta_5^3\,\zeta_5^4)\restriction_{\mathrm{C}_5}^{\mathrm{A}_5} & = & (\,12\;\;0\;\;0\;\;\zeta_5{+}\zeta_5^4\;\;\zeta_5^2{+}\zeta_5^3\,) & = \psi_2+\psi_3+\psi_4 \\ (1\,\zeta_5^2\,\zeta_5^4\,\zeta_5\,\zeta_5^3)\restriction_{\mathrm{C}_5}^{\mathrm{A}_5} & = & (\,12\;\;0\;\;0\;\;\zeta_5^2{+}\zeta_5^3\;\;\zeta_5{+}\zeta_5^4\,) & = \psi_2+\psi_3+\psi_5\;. \end{array}$$

Hierzu beachten wir noch, daß $\xi := \zeta_5+\zeta_5^4$ eine positive reelle Zahl ist und $\xi^2+\xi-1=0$ erfüllt, woraus $\xi=\frac{1}{2}(-1+\sqrt{5})$ folgt; sowie, daß $\zeta_5^2+\zeta_5^3=-1-\xi=\frac{1}{2}(-1-\sqrt{5})$ ist. Die weiteren irreduziblen Charaktere von C_5 liefern dann nichts neues mehr.

Sei $\mathrm{C}_3 := \langle (1,2,3)\rangle$. Es ist C_3 abelsch und hat die Repräsentanten der (einelementigen) Konjugationsklassen id, $(1,2,3)$ und $(1,3,2)$. Ein Charakter von C_3 ist gerade ein Gruppenmorphismus von C_3 nach $\mathrm{U}(\mathbf{C})$; cf. Beispiel 86.(2). Wir schreiben solche Charaktere als Zeilenvektoren bezüglich der wie eben angegeben geordneten Konjugationsklassenrepräsentanten. Sei $\zeta_3 := \exp(2\pi\mathrm{i}/3)$. Für einen Charakter φ von C_3 wird mit Korollar 118

$$\begin{array}{lcl} \varphi\restriction_{\mathrm{C}_3}^{\mathrm{A}_5}(\mathrm{id}) & = & 20\cdot\varphi(\mathrm{id}) \\ \varphi\restriction_{\mathrm{C}_3}^{\mathrm{A}_5}((1,2,3)) & = & \varphi((1,2,3))+\varphi((1,3,2))\;. \end{array}$$

Alle anderen Werte sind null. Eine Koeffizientenberechnung via Skalarprodukte liefert

$$\begin{array}{lcll} (1\,1\,1)\restriction_{\mathrm{C}_3}^{\mathrm{A}_5} & = & (\,20\;\;2\;\;0\;\;0\;\;0\,) & = \psi_1+2\psi_2+\psi_3+\psi_4+\psi_5 \\ (1\,\zeta_3\,\zeta_3^2)\restriction_{\mathrm{C}_3}^{\mathrm{A}_5} & = & (\,20\;\;-1\;\;0\;\;0\;\;0\,) & = \psi_2+2\psi_3+\psi_4+\psi_5\;. \end{array}$$

Der weitere irreduzible Charakter von C_3 liefert dann nichts neues mehr.

Sei nun $M' := \{\,\mathrm{V}_4\,,\,\mathrm{C}_5\,,\,\mathrm{C}_3\,\}$. Das Bild von $\mathrm{ind}\restriction_{M'}^{\mathrm{A}_5}$ kann durch das $\mathbf{Z}$-lineare Erzeugnis der Spalten der folgenden Matrix beschrieben werden, wobei die i-te Zeile zu ψ_i gehöre für $i\in[1,5]$, und wobei die ersten zwei Spalten von V_4, die nächsten drei Spalten von C_5 und die letzten zwei Spalten von C_3 stammen.

$$\begin{pmatrix} 1&0&1&0&0&1&0\\ 1&1&1&0&1&2&1\\ 2&1&0&1&1&1&2\\ 0&1&1&1&0&1&1\\ 0&1&1&1&1&1&1 \end{pmatrix}$$

Es ist $\mathrm{ind}\restriction_{M'}^{\mathrm{A}_5}$ surjektiv, da das Elementarteilertupel dieser Matrix sich zu $(1,1,1,1,1)$ ergibt.

Ferner ist M' minimal, da sich nach Weglassen der zu V_4 gehörigen ersten zwei Spalten das Elementarteilertupel $(1,1,1,1,0)$ ergibt, da sich nach Weglassen der zu C_5 gehörigen nächsten drei Spalten das Elementarteilertupel $(1,1,1,0)$ ergibt und da sich nach Weglassen der zu C_3 gehörigen letzten zwei Spalten das Elementarteilertupel $(1,1,1,1,3)$ ergibt.

> Beachte, daß nach Identifikation von G mit $\mathrm{A}_5\times\mathrm{C}_3$ unser M' die Menge $M=\{\,\mathrm{V}_4\times\mathrm{C}_3\,,\,\mathrm{C}_5\times\mathrm{C}_3\,,\,\mathrm{C}_3\times\mathrm{C}_3\,\}$ liefert. Hierin ist die fastzyklische Gruppe $\mathrm{V}_4\times\mathrm{C}_3$ weder eine p-Gruppe für eine Primzahl p noch eine zyklische Gruppe.
>
> Beachte ferner, daß alle verwendeten nach A_5 induzierten Charaktere Grad 1 haben; cf. Korollar 162.

Aufgabe 53

(1) Seien $x,\,g,\,h\in G$. Es ist ${}^x[g,h] = {}^xg^-h^-gh = ({}^xg)^-({}^xh)^-({}^xg)({}^xh) = [{}^xg,\,{}^xh]$.
Also ist für $x\in G$ auch

$$\begin{array}{lcl} {}^xG' & = & {}^x\langle\,[g,h]\,:\,g,\,h\,\in\,G\,\rangle \\ & = & \langle\,{}^x[g,h]\,:\,g,\,h\,\in\,G\,\rangle \\ & = & \langle\,[{}^xg,\,{}^xh]\,:\,g,\,h\,\in\,G\,\rangle \\ & \leqslant & G'\;. \end{array}$$

Somit ist $G' \trianglelefteq G$.

Seien nun $x, y \in G$ gegeben. Es wird $(xG')(yG') = xyG' = yxx^-y^-xyG' = yx[x,y]G' = yxG' = (yG')(xG')$. Also ist G/G' abelsch.

Sei $\varphi : G \longrightarrow A$ ein Gruppenmorphismus in eine abelsche Gruppe A. Für $g, h \in G$ wird $\varphi([g,h]) = \varphi(g^-h^-gh) = \varphi(g)^-\varphi(h)^-\varphi(g)\varphi(h) = \varphi(h)^-\varphi(g)^-\varphi(g)\varphi(h) = 1$. Also ist $\varphi(G') = 1$. Somit ist $\bar\varphi : G/G' \longrightarrow A$, $gG' \longmapsto \bar\varphi(gG') := \varphi(g)$ ein wohldefinierter Gruppenmorphismus. Nach Konstruktion ist $\bar\varphi \circ \rho = \varphi$. Da ρ surjektiv ist, ist $\bar\varphi$ durch diese Gleichheit auch eindeutig festgelegt.

(2) Nach Aufgabe 33.(4) ist ι wohldefiniert. Da ρ surjektiv ist, ist ι injektiv.

Wir wollen $\iota(\mathrm{Irr}(G/G')) \stackrel{!}{=} \{\, \psi \in \mathrm{Irr}(G) \,:\, \psi(1) = 1 \,\}$ zeigen.

Ad $\subseteq$. Dank (1) ist G/G' abelsch. Daher ist $\chi(1) = 1$ und folglich $\iota(\chi)(1) = (\chi \circ \rho)(1) = \chi(1) = 1$ für $\chi \in \mathrm{Irr}(G/G')$; cf. Beispiel 86.(3).

Ad $\supseteq$. Sei $\psi \in \mathrm{Irr}(G)$ mit $\psi(1) = 1$. Dann ist die zu ψ gehörige Darstellung gegeben durch $\varphi : G \longrightarrow \mathrm{GL}_1(\mathbf{C})$, $g \longmapsto \varphi(g) := \psi(g)$, da hier die Spur keinen Effekt hat. Da $\mathrm{GL}_1(\mathbf{C})$ abelsch ist, ist $G' \leqslant \mathrm{Kern}\,\varphi$. Dank (1) gibt es folglich genau einen Gruppenmorphismus $\bar\varphi : G/G' \longrightarrow \mathrm{GL}_1(\mathbf{C})$ mit $\bar\varphi \circ \rho = \varphi$. Ist $\bar\psi$ der zur Darstellung $\bar\varphi$ gehörige Charakter, so folgt $\iota(\bar\psi) = \psi$.

Da G/G' abelsch ist, ist $|G/G'| = |\mathrm{Irr}(G/G')|$; cf. Beispiel 86.(3) und Lemma 87. Mit dem eben Gezeigten folgt daraus $|G/G'| = |\mathrm{Irr}(G/G')| = |\{\, \psi \in \mathrm{Irr}(G) \,:\, \psi(1) = 1 \,\}|$.

Es ist

$$\{1\} \;=\; \{\, x \in G/G' \,:\, \chi(x) = 1 \text{ für } \chi \in \mathrm{Irr}(G/G') \,\}\,,$$

da $\mathrm{X}(G/G')$ keine zwei übereinstimmenden Spalten an verschiedenen Positionen haben darf; cf. Satz 90.(2). Folglich ist

$$\begin{aligned} G' &= \{\, g \in G \,:\, \chi(\rho(g)) = 1 \text{ für } \chi \in \mathrm{Irr}(G/G') \,\} \\ &= \{\, g \in G \,:\, \psi(g) = 1 \text{ für alle } \psi \in \mathrm{Irr}(G) \text{ mit } \psi(1) = 1 \,\}\,. \end{aligned}$$

(3) Seien χ_s für $s \in [1,t]$ die paarweise verschiedenen irreduziblen Charaktere von G.

Dann ist $\chi_s(1) \in \{1, p, p^2, p^3\}$ für $s \in [1,t]$; cf. Satz 102. Schreibe

$$a_j \;:=\; |\{\, s \in [1,t] \,:\, \chi_s(1) = p^j \,\}| \;\in\; \mathbf{Z}_{\geqslant 0}$$

für $j \in [0,3]$.

Da $\sum_{s\in[1,t]} \chi_s(1)^2 = |G| = p^3$ ist nach Lemma 87 (oder nach Satz 90.(2)), ist $\sum_{j\in[0,3]} a_j p^{2j} = p^3$.

Somit sind $a_2 = 0$, $a_3 = 0$ und $a_0 + a_1 p^2 = p^3$.

Wegen der Existenz des trivialen Charakters ist $a_0 \geqslant 1$; cf. Korollar 82. Aus $a_0 \equiv_{p^2} a_0 + a_1 p^2 = p^3 \equiv_{p^2} 0$ folgt, daß wir $a_0 = p^2 a_0'$ mit $a_0' \in \mathbf{Z}_{\geqslant 1}$ schreiben können.

Somit ist $a_0' + a_1 = p$.

Dank (2) ist $a_0' p^2 = a_0 = |G/G'|$ und also ein Teiler von $|G| = p^3$.

> Wir hätten oben auch $a_0 \stackrel{(2)}{=} |G/G'| \geqslant 1$ verwenden können.

Da G nichtabelsch ist, ist $|G'| \neq 1$, also $|G/G'| \neq p^3$. Es folgt $|G/G'| = p^2$, somit also $|G'| = p$. Ferner folgt $a_0' = 1$ und also $a_1 = p - 1$.

(4) Seien χ_s für $s \in [1,t]$ die paarweise verschiedenen irreduziblen Charaktere von G.

Dann ist $\chi_s(1) \in \{\, p^i \,:\, i \in [0,k] \,\}$ für $s \in [1,t]$; cf. Satz 102. Schreibe

$$a_j \;:=\; |\{\, s \in [1,t] \,:\, \chi_s(1) = p^j \,\}| \;\in\; \mathbf{Z}_{\geqslant 0}$$

für $j \in [0,k]$.

Da $\sum_{s\in[1,t]} \chi_s(1)^2 = |G| = p^k$ ist nach Lemma 87 (oder nach Satz 90.(2)), ist $\sum_{j\in[0,k]} a_j p^{2j} = p^k$. Es ist

$$a_0 \ \equiv_{p^2} \ \sum_{j\in[0,k]} a_j p^{2j} \ = \ p^k \ \equiv_{p^2} \ 0 \ .$$

Dank (2) ist $a_0 = |G/G'|$ und also ein Teiler von $|G| = p^k$.

Es folgt $|G/G'| = p^i$ für ein $i \in [2,k]$, somit also $|G'| = p^j$ für ein $j \in [0,k-2]$.

Somit haben wir den surjektiven Gruppenmorphismus $G \longrightarrow\!\!\!\!\!\rightarrow G/G'$ mit G/G' abelsch und von Ordnung p^i mit $i \in [2,k]$.

Bleibt zu zeigen, daß jede endliche abelsche Gruppe H von Ordnung p^ℓ mit $\ell \geqslant 2$ eine Untergruppe U von Ordnung p hat. Denn dann bekommen wir einen surjektiven Gruppenmorphismus $H \longrightarrow\!\!\!\!\!\rightarrow H/U$ mit $|H/U| = p^{\ell-1}$. Mit Induktion über $\ell \geqslant 2$ erhalten wir einen surjektiven Gruppenmorphismus von H/U nach $\mathrm{C}_p \times \mathrm{C}_p$ oder nach C_{p^2}, sodaß wir zu einem surjektiven Gruppenmorphismus von H nach $\mathrm{C}_p \times \mathrm{C}_p$ oder nach C_{p^2} komponieren können.

Zur Konstruktion von U wählen wir nun ein Element $h \in H \smallsetminus \{1\}$. Dann hat h die Ordnung p^m für ein $m \in [1,\ell]$. Setze $U := \langle h^{(p^{m-1})} \rangle$. Dann ist $|U| = p$.

Alternativ kann man den Satz von Cauchy zitieren.

Literatur

[1] Curtis, C. W., Reiner, I., *Methods of representation theory, Vol. I,* Wiley, 1981.

[2] Flavell, P., *A Note on Frobenius Groups,* J. Alg. 228, p. 367-376, 2000.

[3] Garrett, P., *Cyclotomic III,* lecture script, 2004.

[4] Grove, L., *Algebra,* Academic Press, 1983

[5] Huppert, B., *Endliche Gruppen I,* Springer Grundlehren 134, 1967.

[6] Kimmerle, W., *Gruppen, Geometrie und Darstellungstheorie,* Edition Delkhofen, 2008.

[7] Künzer, M., *Computeralgebra,* Skript, Stuttgart, 2011.

[8] Nebe, G., *Darstellungstheorie,* Vorlesung und Übungen, Ulm, 2002.

[9] Roggenkamp, K. W., *Darstellungstheorie endlicher Gruppen,* 1973.

[10] Serre, J.-P., *Linear Representations of Finite Groups,* Springer GTM 42, 1971.

[11] van der Waerden, B.L., *Algebra,* Springer, 1960.