Gruppentheorie

Matthias Künzer

Universität Stuttgart

13. Mai 2025

Inhalt

Verzeichnis der Sätze und einiger sonstiger Aussagen

Vorwort

Automorphismengruppen

Jedes mathematische Objekt X hat eine Automorphismengruppe $\mathrm{Aut}(X)$, bestehend aus den invertierbaren Morphismen von X nach X. Ist X von Interesse, so hilft oft $\mathrm{Aut}(X)$ beim Studium von X. Ist X nicht von sonderlichem Interesse, so kann trotzdem $\mathrm{Aut}(X)$ betrachtenswert sein.

Es hat e.g. die Körpererweiterung $\mathbf{C}|\mathbf{R}$ die Automorphismengruppe $\{\,\mathrm{id}_{\mathbf{C}}\,,\,\kappa\,\} \simeq \mathrm{C}_2\,,$ wobei $\kappa(z) := \bar{z}$ das komplex Konjugierte zu $z \in \mathbf{C}$ bezeichnet.

Es hat e.g. die Menge $\{1,2,3,4,5\}$ als Automorphismengruppe die symmetrische Gruppe $\mathrm{S}_5\,.$

Es hat e.g. für einen Körper K und $n \geqslant 0$ der Vektorraum K^n die Automorphismengruppe $\mathrm{GL}_n(K)$.

Es hat e.g. die Gruppe S_5 die Automorphismengruppe $\mathrm{Aut}(\mathrm{S}_5) \simeq \mathrm{S}_5\,.$

Man abstrahiert von Automorphismengruppen zu Gruppen, um einen flexibleren Formalismus zur Verfügung zu haben, in welchem auch dann Untergruppen und Faktorgruppen gebildet werden dürfen, wenn diese nicht unmittelbar als Automorphismengruppen auftreten.

Analyse von Gruppen

Gruppen sollen analysiert werden, indem sie als aus kleinstmöglichen Bestandteilen zusammengesetzt beschrieben werden.

Diese Bestandteile heißen Kompositionsfaktoren. Wie Gruppen aus diesen zusammengesetzt sein können, versucht die Erweiterungstheorie zu beschreiben.

Betrachten wir einmal die symmetrische Gruppe $\mathrm{S}_5\,.$ Das Signum ist ein surjektiver Gruppenmorphismus von S_5 nach $\{-1,+1\} \simeq \mathrm{C}_2\,.$ Der Kern des Signums ist die alternierende Gruppe $\mathrm{A}_5\,.$ Diese stellt das kleinste nichtabelsche Beispiel einer einfachen Gruppe dar, i.e. einer Gruppe ohne nichttriviale Normalteiler. Die Kompositionsfaktoren von S_5 sind A_5 und $\mathrm{C}_2\,.$

$$\begin{array}{l} \mathrm{S}_5 \\ \big|\,{\scriptstyle \mathrm{C}_2} \\ \mathrm{A}_5 \\ \big|\,{\scriptstyle \mathrm{A}_5} \\ 1 \end{array}$$

Zwar ist S_5 nicht als direktes Produkt $\mathrm{A}_5 \times \mathrm{C}_2$ rekonstruierbar, wohl aber noch als semidirektes Produkt,

$$\mathrm{S}_5 \;\simeq\; \mathrm{A}_5 \rtimes \mathrm{C}_2 \;,$$

zu dessen Bildung eine Operation von C_2 auf A_5 zu berücksichtigen ist.

Betrachten wir ferner die Gruppe $\mathrm{GL}_n(K)$. Sei hierbei K ein endlicher Körper und $n \geqslant 2$. Die Determinante gibt einen surjektiven Gruppenmorphisms von $\mathrm{GL}_n(K)$ nach $K \setminus \{0\} = \mathrm{GL}_1(K)$. Der Kern der Determinante ist die Gruppe $\mathrm{SL}_n(K)$. Die darin liegenden Diagonalmatrizen mit konstanter Diagonale bilden das Zentrum $\mathrm{Z}(\mathrm{SL}_n(K))$ dieser Gruppe, was darin ein i.a. nichttrivialer Normalteiler ist. Die Gruppen $\mathrm{GL}_1(K)$ und $\mathrm{Z}(\mathrm{SL}_n(K))$ sind abelsch, sogar zyklisch, ihre Kompositionsfaktoren mithin zyklisch von Primordnung. Schließlich ist die Faktorgruppe $\mathrm{PSL}_n(K) := \mathrm{SL}_n(K)/\mathrm{Z}(\mathrm{SL}_n(K))$ eine einfache Gruppe, solange nur $(K,n) \notin \{\,(\mathbf{F}_2\,,2),\,(\mathbf{F}_3\,,2)\,\}$ ist. Somit hat diesenfalls die Gruppe $\mathrm{GL}_n(K)$ als Kompositionsfaktoren $\mathrm{PSL}_n(K)$ und weitere zyklische Gruppen von Primordnung.

$$\begin{array}{c} \mathrm{GL}_n(K) \\ \big|\,{\scriptstyle \text{abelsch}} \\ \mathrm{SL}_n(K) \\ \big|\,{\scriptstyle \mathrm{PSL}_n(K)} \\ \mathrm{Z}(\mathrm{SL}_n(K)) \\ \big|\,{\scriptstyle \text{abelsch}} \\ 1 \end{array}$$

Es ist zwar

$$\mathrm{GL}_n(K) \;\simeq\; \mathrm{SL}_n(K) \rtimes \mathrm{GL}_1(K) \;,$$

jedoch ist i.a. dann

$$\mathrm{Z}(\mathrm{SL}_n(K)) \;\rightarrowtail\; \mathrm{SL}_n(K) \;\twoheadrightarrow\; \mathrm{PSL}_n(K)$$

eine nichtspaltende Erweiterung, i.e. $\mathrm{SL}_n(K)$ ist nicht als semidirektes Produkt seiner Untergruppe $\mathrm{Z}(\mathrm{SL}_n(K))$ und seiner Faktorgruppe $\mathrm{PSL}_n(K)$ schreibbar. Die Tatsache, daß $\mathrm{Z}(\mathrm{SL}_n(K))$ zentral in $\mathrm{SL}_n(K)$ liegt, hat hierbei auch nicht geholfen.

Charakterisierung von Gruppen über Erzeuger

Man kann eine Gruppe vollständig beschreiben, wenn man, grob gesprochen, ein Tupel von Gruppenerzeugern vorgibt und dazuhin eine hinreichende Menge von Relationen, i.e. von Produktausdrücken in diesen Erzeugern oder ihren Inversen, welche in dieser Gruppe Produkt 1 haben.

So etwa ist die Gruppe

$$S \;:=\; \langle\, s_1\,,\, s_2\,,\, s_3\,,\, s_4 \;:\; s_1^2\,,\, s_2^2\,,\, s_3^2\,,\, s_4^2\,,\, (s_1s_2)^3\,,\, (s_2s_3)^3\,,\, (s_3s_4)^3\,,\, (s_1s_3)^2\,,\, (s_1s_4)^2\,,\, (s_2s_4)^2\,\rangle$$

erzeugt von den Elementen $s_1\,,\, s_2\,,\, s_3\,,\, s_4$; in ihr gelten die Gleichungen $s_1^2 = 1$, $s_2^2 = 1$, $s_3^2 = 1$, $\ldots$, $(s_2s_4)^2 = 1$; und zu jeder Gruppe, die von Elementen $\tilde{s}_1\,,\, \tilde{s}_2\,,\, \tilde{s}_3\,,\, \tilde{s}_4$ erzeugt

wird, für welche die entsprechenden Gleichungen gelten, gibt es genau einen Gruppenmorphismus von S, welcher $s_i \longmapsto \tilde{s}_i$ abbildet für $i \in [1,4]$.

Konstruiert wird diese Gruppe S als Faktorgruppe der freien Gruppe auf der Menge $\{ s_1 , s_2 , s_3 , s_4 \}$ modulo dem von den Relationen s_1^2, s_2^2, s_3^2, $\dots$, $(s_2 s_4)^2$ erzeugten Normalteiler.

Insbesondere erhalten wir den Gruppenmorphismus $S \longrightarrow \mathrm{S}_5$, der $s_i \longmapsto (i,\, i+1)$ abbildet für $i \in [1,4]$. Dieser ist sogar ein Isomorphismus. Damit haben wir S_5 in Erzeugern und Relationen beschrieben.

Für eine gegebene endliche Gruppe G sucht man nun einen solchen Isomorphismus von einer geeigneten durch Erzeuger und Relationen gegebenen Gruppe nach G. Hierzu läßt man eine freie Gruppe, i.e. eine mit Erzeugern ohne Relationen, auf G operieren und wendet den Bahnenalgorithmus an, um den Zentralisator von 1_G unter dieser Operation zu berechnen und daraus die benötigten Relationen abzuleiten.

Organisatorisches

Inhaltlich orientieren wir uns an bekannten Darstellungen der Materie; cf. **[2]**, **[3]**. Die Verantwortung für Fehler und Unklarheiten im vorliegenden Skript trage ich natürlich selbst. Für diesbezügliche Hinweise bin ich dankbar.

Vorausgesetzt werden elementare Kenntnisse über Gruppen aus der Linearen Algebra und der Algebra, insbesondere die Begriffe der Gruppe, der Untergruppe, der Nebenklassen, des Normalteilers, der Faktorgruppe, des Gruppenmorphismus; cf. e.g. **[6,** §3.2]. Sylowsätze und Jordan-Hölder werden nochmals angesprochen. Der Hauptsatz über endlich erzeugte abelsche Gruppen wird in den Übungen wiederholt, nach Herleitung des Elementarteilersatzes über $\mathbf{Z}$; cf. auch e.g. **[8,** §1].

Auf Übungen und Lösungen wird im Skript manchmal Bezug genommen, sie sind daher als Bestandteil des Skripts anzusehen.

Dank geht an Monika Truong für Diskussionen über Jordan-Hölder und weitere Hinweise. Dank geht an Maximilian Hofmann für ausgearbeitete Lösungen zu Aufgaben und weitere Hinweise. Dank geht an Alisa Baransegeta, Jonas Dallendörfer, Nadine Hilligardt, Carlo Klapproth, Veronika Klein, Nora Krauss und Sebastian Nitsche für Korrekturen und Hinweise. Dank geht an Elias Schwesig und Maximilian Kotte für Korrekturen und Hinweise. Für weitere Hinweise auf Fehler und Unklarheiten bin ich dankbar.

Stuttgart, im Wintersemester 2015/16 und im Sommersemester 2025

Matthias Künzer

Konventionen. Seien X, Y, Z Mengen. Seien G und H Gruppen.

- Sind a, $b \in \mathbf{Z}$, so schreiben wir $[a,b] := \{z \in \mathbf{Z} \,:\, a \leqslant z \leqslant b\}$ für das ganzzahlige Intervall.
- Ist $p > 0$ eine Primzahl und $x \in \mathbf{Z} \smallsetminus \{0\}$, so schreiben wir $\mathrm{v}_p(x) := \max\{\, \alpha \in \mathbf{Z}_{\geqslant 0} \,:\, x \in p^\alpha \mathbf{Z} \,\}$ für die Bewertung (engl. valuation) von x bei p. Wir setzen noch $\mathrm{v}_p(0) = +\infty$.
- Ist $n \in \mathbf{Z}$ und $p \in \mathbf{Z}_{>0}$ prim, so schreiben wir $n[p] := p^{\mathrm{v}_p(n)}$ für den p-Anteil von n.
- Sind a, b, $x \in \mathbf{Z}$, so bedeute $a \equiv_x b$, daß $a - b \in x\mathbf{Z}$ ist.
- Es stehe "für $x \in X$" kurz für "für alle $x \in X$".
- Ist A eine Aussage, so sei $\partial_A = 1$, falls A wahr ist, und $\partial_A = 0$, falls A falsch ist. Für x, $x' \in X$ schreiben wir oft $\partial_{x,y} := \partial_{x=y}$.
- Es bedeutet $Y \subset X$, daß $Y \subseteq X$ und $Y \neq X$ ist.
- Sei $\mathrm{Pot}(X)$ die Potenzmenge von X, i.e. die Menge aller Teilmengen von X.
- Sei I eine Menge und sei $Y_i \subseteq X$ für $i \in I$. Schreiben wir $\bigsqcup_{i\in I} Y_i$ für $\bigcup_{i\in I} Y_i$, so bringen wir dadurch zum Ausdruck, daß $Y_i \cap Y_j = \emptyset$ ist für i, $j \in I$ mit $i \neq j$.
- Ist X endlich, so bezeichne $|X|$ die Anzahl ihrer Elemente.
- Für $k \geqslant 0$ schreiben wir $X^{\times k} := \prod_{i\in[1,k]} X = \{\, (x_i)_{i\in[1,k]} \,:\, x_i \in X \text{ für } i \in [1,k] \,\}$.
- Es bezeichnet $\mathrm{id} = \mathrm{id}_X$ die identische Abbildung von X nach X.
- Sei ${}_{\mathrm{Abb}}(X,Y)$ die Menge der Abbildungen von X nach Y.
- Sei $f : X \longrightarrow Y$ eine Abbildung. Sei $X' \subseteq X$, $Y' \subseteq Y$ und $f(X') \subseteq Y'$. Wir schreiben $f|_{X'}^{Y'} : X' \longrightarrow Y'$, $x' \longmapsto f(x')$ für die Einschränkung. Ist $Y' = Y$, so schreiben wir auch $f|_{X'} := f|_{X'}^{Y}$. Ist $X' = X$, so schreiben wir auch $f|^{Y'} := f|_{X}^{Y'}$.
- Ist $f : X \longrightarrow Y$ bijektiv, so bezeichnet häufig $f^- := f^{-1} : Y \longrightarrow X$ ihre Umkehrabbildung, i.e. $f^- \circ f = \mathrm{id}_X$ und $f \circ f^- = \mathrm{id}_Y$.
- Ist $f : X \times Y \longrightarrow Z$ eine Abbildung und sind $X' \subseteq X$ und $Y' \subseteq Y$, so schreiben wir $f(X',Y') := \{\, f(x',y') \,:\, x' \in X',\, y' \in Y' \,\}$.
- Eine Äquivalenzrelation auf X heißt diskret, wenn ihre Äquivalenzklassen alle einelementig sind; sie heißt verklumpt, wenn ihre einzige Äquivalenzklasse gleich X ist.
- Sei $(X, \leqslant)$ ein Poset, i.e. eine teilgeordnete Menge (partially ordered set).

  Es heißt $x \in X$ *minimal*, falls es kein $y \in X$ mit $y < x$ gibt. Es heißt $x \in X$ *initial*, falls $x \leqslant z$ für alle $z \in X$ gilt. Es heißt $x \in X$ *maximal*, falls es kein $y \in X$ mit $x < y$ gibt. Es heißt $x \in X$ *terminal*, falls $z \leqslant x$ für alle $z \in X$ gilt. Es existieren höchstens ein initiales und höchstens ein terminales Element in X. Für $a \in X$ schreiben wir $X_{>a} := \{\, x \in X \,:\, x > a \,\}$, etc.
- Sei G endlich. Es heißt $|G|$ auch die Ordnung von G. Für $g \in G$ heißt $|\langle g \rangle|$ auch die Ordnung von g. Es heißt $\exp(G) := \mathrm{kgV}(\, |\langle g \rangle| \,:\, g \in G \,)$ der Exponent von G. Es ist $\exp(G)$ ein Teiler von $|G|$.
- Die Gruppe G werde, wenn nichts anderes festgelegt wird, multiplikativ geschrieben, mit multiplikativ neutralem Element $1 = 1_G$.
- Wird eine abelsche Gruppe A additiv geschrieben, dann heißt ihr additives neutrales Element $0 = 0_A$. Es bezeichnet $A^\times := A \smallsetminus \{0\}$.
- Es bezeichnet S_X die symmetrische Gruppe auf X, bestehend aus den Bijektionen von X nach X, mit der Komposition ($\circ$) als Multiplikation und mit $1_{\mathrm{S}_n} = \mathrm{id}_{[1,n]} = \mathrm{id}$. Für $n \geqslant 0$ schreiben wir auch $\mathrm{S}_n := \mathrm{S}_{[1,n]}$. Wir verwenden die Zykelschreibweise, nach der e.g. $(1,5,2)(3,4)$ so abbildet: $1 \mapsto 5$, $5 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 4$, $4 \mapsto 3$. Ein 2-Zykel heißt auch Transposition.

- Sei $n \geqslant 1$. Es bezeichet C_n die zyklische Gruppe von Ordnung n, in welcher ein Erzeuger von Ordnung n existiert. Es ist C_n isomorph zur additiven Gruppe von $\mathbf{Z}/n\mathbf{Z}$.
- Sei A ein Ring. Es bezeichnet $\mathrm{U}(A) := \{\, a \in A \,:\, \text{es gibt ein } b \in A \text{ mit } ab = 1 \text{ und } ba = 1 \,\}$ die Einheitengruppe von A.
- Sei $n \geqslant 2$. Der Kern des Signummorphismus $\mathrm{sgn} : \mathrm{S}_n \to \mathrm{U}(\mathbf{Z}) = \{-1, +1\}$ ist die alternierende Gruppe A_n .
- Sei R ein kommutativer Ring. Seien $n, m \geqslant 0$. Sei $R^{m\times n}$ die Menge der $m \times n$-Matrizen. Für $i \in [1, m]$ und $j \in [1, n]$ ist $\mathrm{e}_{i,\,j} \in R^{m\times n}$ das Element, das an Position (i, j) den Eintrag 1 hat, ansonsten überall den Eintrag 0.

  Sei $\mathrm{E}_n := \sum_{i\in[1,n]} \mathrm{e}_{i,i} \in R^{n\times n}$ die Einheitsmatrix.

  Sei $\mathrm{diag}(\lambda_1\,, \ldots,\, \lambda_n) = \sum_{i\in[1,n]} \lambda_i \mathrm{e}_{i,i}$, wobei $\lambda_i \in R$ für $i \in [1, n]$.

  Sei $R^m := R^{m\times 1}$. Für $i \in [1, m]$ ist $\mathrm{e}_i \in R^m$ das Element, das an Position i den Eintrag 1 hat, ansonsten überall den Eintrag 0, genannt der i-te Standardbasisvektor. I.e. $\mathrm{e}_i = \mathrm{e}_{i,1}$.
- Sei R ein kommutativer Ring. Es bezeichnet

$$\mathrm{GL}_n(R) \;=\; \mathrm{U}(R^{n\times n}) \;=\; \{\, M \in R^{n\times n} \,:\, \det(M) \in \mathrm{U}(R) \,\}$$

  die Gruppe der invertierbaren Elemente aus $R^{n\times n}$. So zum Beispiel kann $\mathrm{U}(R) = \mathrm{GL}_1(R)$ identifiziert werden. Es bezeichnet

$$\mathrm{SL}_n(R) \;=\; \{\, M \in R^{n\times n} \,:\, \det(M) = 1 \,\}$$

  den Kern des Gruppenmorphismus $\det : \mathrm{GL}_n(R) \longrightarrow \mathrm{U}(R)$. Ferner bezeichnet

$$\mathrm{PSL}_n(R) \;=\; \mathrm{SL}_n(R)/\mathrm{Z}(\mathrm{SL}_n(R)) \;.$$

- Sei K ein Körper. Sei V ein K-Vektorraum. Es bezeichnet $\mathrm{GL}(V)$ die Gruppe der bijektiven K-linearen Abbildungen von V nach V, mit der Komposition als Multiplikation. Es ist also $\mathrm{GL}(K^n)$ isomorph zu $\mathrm{GL}_n(K)$ vermöge des Isomorphismus, der einem Element $\varphi \in \mathrm{GL}(K^n)$ die beschreibende Matrix bezüglich Standardbasis zuordnet.
- Es bezeichnet manchmal $\rightarrowtail$ einen injektiven Gruppenmorphismus, $\twoheadrightarrow$ einen surjektiven, $\xrightarrow{\sim}$ einen bijektiven.
- Eine abelsche Gruppe A heißt endlich erzeugt, wenn es ein $n \geqslant 0$ und einen surjektiven Gruppenmorphismus $f : \mathbf{Z}^n \twoheadrightarrow A$ gibt.

  Man sagt diesenfalls auch, A sei von den Elementen $f(\mathrm{e}_1), \ldots, f(\mathrm{e}_n)$ erzeugt.
- Ein Gruppenmorphismus $f : G \longrightarrow H$ wird trivial genannt, wenn $f(g) = 1$ ist für alle $g \in G$. Wir schreiben diesenfalls auch $f = ! = !_{G,H}$.
- Ein Gruppenmorphismus von G nach G heißt Endomorphismus. Ein bijektiver Endomorphismus heißt Automorphismus.
- Für $g \in G$ bezeichne häufig $g^- := g^{-1}$ das Inverse zu g, i.e. $gg^- = 1 = g^-g$. Gesprochen wird g^- als "g invers".
- Für $g \in G$, $a \in \mathbf{Z}$ und $b \in \mathbf{Z}_{\geqslant 0}$ sei $g^{a^b} := g^{(a^b)}$.
- Für $g,\, x \in G$ ist ${}^g x := gxg^-$. Gesprochen wird ${}^g x$ als "x links hoch g".
- Für $g,\, h \in G$ ist $[g, h] := g^-h^-gh$ der Kommutator von g und h.
- Ist $S \subseteq G$, dann ist $\langle S\rangle \leqslant G$ das Untergruppenerzeugnis von S in G, i.e. unter den Untergruppen von G, die S enthalten, die initiale. Mit anderen Worten, $\langle S\rangle$ ist der Schnitt aller Untergruppen von G, die S enthalten. Abermals mit anderen Worten, $\langle S\rangle$ ist die Menge aller endlichen Produkte in den Elementen von S und ihrer Inversen. So ist e.g. $\langle\emptyset\rangle = \{1\} =: 1$.

- Für $U, V \leqslant G$ ist $[U,V] := \langle\, [u,v] \,:\, u \in U,\ v \in V \,\rangle$. Beachte $[U,V] = [V,U]$. Speziell ist $G^{(1)} := [G,G]$ die Kommutatoruntergruppe von G; cf. Aufgabe 13, Definition 81.
- Es bedeutet $U \leqslant G$, daß U eine Untergruppe von G ist. Es bedeutet $U < G$, daß $U \leqslant G$ und $U \neq G$ ist; es heißt dann U echte Untergruppe von G.
- Es bedeutet $N \trianglelefteqslant G$, daß N eine normale Untergruppe von G ist, auch Normalteiler genannt. Es bedeutet $U \triangleleft G$, daß $U \trianglelefteqslant G$ und $U \neq G$ ist.
- Eine Gruppe G mit $|G| > 1$ heißt einfach, wenn 1 und G die einzigen Normalteiler von G sind.
- Für $U \leqslant G$ mit G/U endlich schreiben wir $[G : U] := |G/U|$ für den Index von U in G.
- Für eine endliche Gruppe G schreiben wir $\pi(G) := \{\, p > 0 \text{ prim} \,:\, |G| \equiv_p 0 \,\}$.
- Sei $G \xrightarrow{f} H$ ein Gruppenmorphismus. Sein Kern werde $\mathrm{Kern}(f) \trianglelefteqslant G$, sein Bild $\mathrm{Im}(f) \leqslant H$ geschrieben.
- Eine Sequenz von Gruppen und Gruppenmorphismen $G' \xrightarrow{u} G \xrightarrow{v} G''$ heißt exakt bei G, wenn $\mathrm{Kern}(v) = \mathrm{Im}(u)$ ist. Eine solche exakte Sequenz heißt rechtsexakt, falls v surjektiv ist; linksexakt, falls u surjektiv ist; kurz exakt, falls u injektiv und v surjektiv ist.

  Diesenfalls heißt G auch Erweiterung von G' mit G''.

Kapitel 1

G-Mengentheorie

Sei G eine Gruppe.

1.1 Operationen von Gruppen

Definition 1 Ein Paar (M, α) bestehend aus einer Menge M und einem Gruppenmorphismus $\alpha : G \longrightarrow \mathrm{S}_M$ heißt *G-Menge*. Hierbei heißt α *Operation* von G auf M.

Wir schreiben oft kurz $M := (M, \alpha)$ und $gm = g \cdot m := (\alpha(g))(m)$.

Ist α injektiv, so heißt M eine *treue* G-Menge.

Bemerkung. Sei M eine Menge.

(1) Sei gegeben ein Gruppenmorphismus $\alpha : G \longrightarrow \mathrm{S}_M$. Dieser liefert die Abbildung $\mu : G \times M \longrightarrow M$, $(g, m) \mapsto \alpha(g)(m) =: g \cdot m = gm$. Für diese gilt

$$1 \cdot m \;=\; \alpha(1)(m) \;=\; \mathrm{id}_M(m) \;=\; m$$

und

$$g \cdot (h \cdot m) \;=\; (\alpha(g) \circ \alpha(h))(m) \;=\; \alpha(gh)(m) \;=\; (gh) \cdot m$$

für $m \in M$ und $g, h \in G$.

(2) Sei nun gegeben eine Abbildung $\mu : G \times M \longrightarrow M$, $(g, m) \mapsto g \cdot m = gm$, für welche

$$\begin{aligned} 1 \cdot m &= m \\ g \cdot (h \cdot m) &= (gh) \cdot m \end{aligned}$$

für $m \in M$ und $g, h \in G$ gelten. Dann wird für $g \in G$ die Abbildung $M \longrightarrow M$, $m \longmapsto g \cdot m$ beidseitig invertiert von der Abbildung $M \longrightarrow M$, $m \longmapsto g^- \cdot m$, da zum

einen $g \cdot (g^- \cdot m) = (gg^-) \cdot m = 1 \cdot m = m$ und zum anderen $g^- \cdot (g \cdot m) = (g^- g) \cdot m = 1 \cdot m = m$ ist für $m \in M$. Somit ist die Abbildung

$$\alpha \ : \ G \longrightarrow \mathrm{S}_M \ , \quad g \longmapsto (m \mapsto g \cdot m)$$

wohldefiniert. Sie ist ein Gruppenmorphismus, da $(\alpha(g) \circ \alpha(h))(m) = g \cdot (h \cdot m) = (gh) \cdot m = \alpha(gh)(m)$ ist für $m \in M$, mithin $\alpha(g) \circ \alpha(h) = \alpha(gh)$ für $g, h \in G$.

Kurz, man kann zur Konstruktion einer G-Operation auf M wahlweise direkt einen Gruppenmorphismus $\alpha : G \longrightarrow \mathrm{S}_M$ als Operation angeben wie in (1) oder in Definition 1, oder aber man kann eine Abbildung $\mu : G \times M \longrightarrow M$ angeben mit den in (2) beschriebenen Eigenschaften.

Beispiel 2

(1) Sei $n \geqslant 0$. Es ist $[1, n]$ eine S_n-Menge via $\mathrm{id}_{\mathrm{S}_n} : \mathrm{S}_n \longrightarrow \mathrm{S}_n$, i.e. via $\sigma \cdot i = \sigma(i)$ für $\sigma \in \mathrm{S}_n$ und $i \in [1, n]$.

Sei $U \leqslant \mathrm{S}_n$. Betrachte den Einbettungsmorphismus $\iota : U \longrightarrow \mathrm{S}_n$. Dann ist $[1, n] = ([1, n], \iota)$ eine treue U-Menge.

(2) Sei H eine Gruppe. Sei $\varphi : H \longrightarrow G$ ein Gruppenmorphismus. Sei $M = (M, \alpha)$ eine G-Menge. Nach Einschränkung auf H entlang φ wird $(M, \alpha \circ \varphi)$ eine H-Menge. Manchmal schreibt man diese $M\downarrow_\varphi$ oder $M\downarrow^G_H$.

Wir haben e.g. in (1) die S_n-Menge $[1, n]$ entlang ι auf U eingeschränkt.

(3) Ist $U \leqslant G$, dann ist die Faktormenge G/U eine G-Menge via $g \cdot xU := gxU$ für $x, g \in G$. Da $1 \cdot xU = xU$ und da $g \cdot (h \cdot xU) = ghxU = (gh) \cdot xU$ für $g, h, x \in G$ ist, definiert dies in der Tat eine G-Menge mit Operation $\alpha : G \longrightarrow \mathrm{S}_{G/U}$, $g \longmapsto (xU \mapsto gxU)$.

Insbesondere wird für $U = 1$ so G zu einer G-Menge via Linksmultiplikation.

Es ist $x \in G$ genau dann in $\mathrm{Kern}(\alpha)$ enthalten, wenn für $g \in G$ gilt, daß $xgU = gU$, i.e. $g^- xgU = U$, i.e. $g^- xg \in U$, i.e. $x \in {}^gU$ ist. Also ist $\mathrm{Kern}(\alpha) = \bigcap_{g \in G} {}^gU$. Insbesondere ist G/U treu genau dann, wenn $\bigcap_{g \in G} {}^gU = 1$ ist.

(4) Sei K ein Körper. Sei V ein K-Vektorraum. Via $\alpha : \mathrm{GL}(V) \longrightarrow \mathrm{S}_V$, $\varphi \longmapsto \varphi$ ist V eine $\mathrm{GL}(V)$-Menge, i.e. via $\varphi \cdot v = \varphi(v)$ für $\varphi \in \mathrm{GL}(V)$ und $v \in V$. Ist H eine Gruppe und $\gamma : H \longrightarrow \mathrm{GL}(V)$ ein Gruppenmorphismus, so wird $V\downarrow_\gamma = (V, \alpha \circ \gamma)$ auch zu einer H-Menge; cf. (2).

(5) Es ist G eine G-Menge via Konjugation, i.e. via $g \cdot x := {}^g x$ für $g, x \in G$. Da $1 \cdot x = x$ und da $g \cdot (h \cdot x) = {}^g({}^h x) = {}^{gh} x = (gh) \cdot x$ für $g, h, x \in G$ ist, definiert dies in der Tat eine G-Menge mit Operation $\beta : G \longrightarrow \mathrm{S}_G$, $g \longmapsto (x \mapsto {}^g x)$.

Vorsicht, die G-Mengen-Multiplikation ist nicht die Gruppenmultiplikation.

Es ist $g \in G$ genau dann in $\mathrm{Kern}(\beta)$ enthalten, wenn für $x \in G$ gilt, daß ${}^g x = x$, i.e. $gx = xg$ ist. Also ist $\mathrm{Kern}(\beta) = \{\, g \in G \ : \ gx = xg \text{ für } x \in G \,\} = \mathrm{Z}(G)$ das Zentrum von G.

Definition 3 Seien G-Mengen M und N gegeben.

Eine Abbildung $a : M \longrightarrow N$ heißt eine *G-Abbildung* oder ein *Morphismus von G-Mengen,* wenn $ga(m) = a(gm)$ für $g \in G$ und $m \in M$ gilt.

Eine bijektive G-Abbildung von M nach N heißt *G-Bijektion* oder *Isomorphismus von G-Mengen*, angedeutet durch $M \xrightarrow{\sim} N$. Existiert ein Isomorphismus von G-Mengen von M nach N, so heißen M und N *isomorph,* geschrieben $M \simeq N$.

Eine G-Menge isomorph zu $G/1$ heißt *regulär*; eine G-Menge isomorph zu G/G heißt *trivial*; cf. Beispiel 2.(3).

Beispiel 4 Sei $U \leqslant V \leqslant G$. Dann ist $f : G/U \longrightarrow G/V$, $gU \longmapsto gV$ eine wohldefinierte surjektive G-Abbildung. Wohldefiniert ist f, da für $g \in G$ und $u \in U$ auch $guV = gV$ ist. Surjektiv ist f nach Konstruktion. Es ist f eine G-Abbildung, da für $x, g \in G$ sich $f(xgU) = xgV = xf(gU)$ ergibt.

Beispiel 5 Sei M eine G-Menge. Betrachte G als G-Menge via Linksmultiplikation; cf. Beispiel 2.(3). Sei $m \in M$.

Es ist $G \longrightarrow M$, $g \longmapsto gm$ eine G-Abbildung.

Bemerkung 6 Seien G-Mengen M, N, P gegeben.

(1) Es ist id_M eine G-Abbildung.

(2) Sind $M \xrightarrow{a} N \xrightarrow{b} P$ beides G-Abbildungen, dann auch $M \xrightarrow{b \circ a} P$.

(3) Ist $M \xrightarrow{a} N$ eine bijektive G-Abbildung, dann auch a^- wegen

$$a^-(gm) \;=\; a^-(g \cdot a(a^-(m))) \;=\; a^-(a(g \cdot a^-(m))) \;=\; g \cdot a^-(m)$$

für $g \in G$ und $m \in M$. Ist $M \simeq N$, so folgt also $N \simeq M$.

Definition 7 Sei M eine G-Menge. Eine Teilmenge $N \subseteq M$ heißt *G-Teilmenge,* wenn für $g \in G$ und $n \in N$ auch $gn \in N$ liegt. Diesenfalls ist N via $G \longrightarrow \mathrm{S}_N$, $g \longmapsto (n \mapsto gn)$ wieder eine G-Menge. Wir haben die G-Abbildung $N \longrightarrow M$, $n \longmapsto n$.

Beispiel 8

(1) Sei $k \geqslant 0$. Seien G-Mengen M_i für $i \in [1,k]$ gegeben. Es wird $M := \prod_{i \in [1,k]} M_i$ mittels $\alpha : G \longrightarrow \mathrm{S}_M$, $g \longmapsto ((m_i)_i \mapsto (gm_i)_i)$ eine G-Menge.

(2) Sei $k \geqslant 0$. Sei M eine G-Menge. Schreibe $M^{\times k} := \prod_{i \in [1,k]} M$. Sei

$$M^{\times k, \neq} \;:=\; \{\, (m_i)_i \in M^{\times k} \,:\, m_i \neq m_j \text{ für } i, j \in [1,k] \text{ mit } i \neq j \,\}\,.$$

Es ist $M^{\times k, \neq}$ eine G-Teilmenge von $M^{\times k}$.

Definition 9 Sei $M = (M, \alpha)$ eine G-Menge. Eine Äquivalenzrelation $(\sim)$ auf M heißt *G-Äquivalenzrelation*, falls für $m,\, m' \in M$ und $g \in G$ aus $m \sim m'$ auch $gm \sim gm'$ folgt.

Schreibe $\bar{M} := M/(\sim)$. Schreibe $\bar{m}$ für die Äquivalenzklasse von m. Ist $(\sim)$ eine G-Äquivalenzrelation, dann ist $\bar{M}$ vermöge $g \cdot \bar{m} := \overline{gm}$ für $g \in G$ und $m \in M$ eine G-Menge. Denn es ist $1\bar{m} = \bar{m}$ und $g(h\bar{m}) = g\overline{hm} = \overline{ghm} = (gh)\bar{m}$ für $m \in M$ und $g,\, h \in G$, was die Operation $\bar{\alpha} : G \longrightarrow \mathrm{S}_{\bar{M}}\,,\ g \longmapsto (\bar{m} \mapsto \overline{gm})$ liefert.

Wir haben die G-Abbildung $r : M \longrightarrow \bar{M},\ m \longmapsto \bar{m}$.

Beispiel 10 Sei eine G-Abbildung $f : M \longrightarrow N$ zwischen G-Mengen gegeben.

Es ist $f(M)$ eine G-Teilmenge von N.

Sei die Äquivalenzrelation $(\sim)$ auf M definiert durch

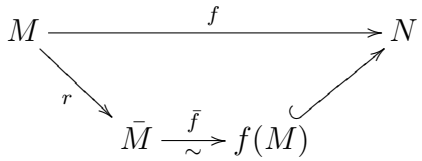
$$m \ \sim\ m' \qquad :\Longleftrightarrow \qquad f(m) \ =\ f(m')$$

für $m,\, m' \in M$. Es ist $(\sim)$ eine G-Äquivalenzrelation, da für $g \in G$ und $m,\, m' \in M$ mit $m \sim m'$ auch $f(gm) = gf(m) = gf(m') = f(gm')$ und somit $gm \sim gm'$ gilt.

Es ist

$$\begin{array}{rccc} \bar{f} & : & \bar{M} & \longrightarrow & f(M) \\ & & \bar{m} & \longmapsto & f(m) \end{array}$$

eine G-Bijektion. Denn da $m \sim m'$ genau dann gilt, wenn $f(m) = f(m')$, ist $\bar{f}$ wohldefiniert und injektiv. Nach Konstruktion ist $\bar{f}$ zudem surjektiv.



Definition 11 Sei M eine G-Menge.

(1) Wir definieren eine Äquivalenzrelation $(\sim)$ auf M durch

$$m \ \sim\ m' \qquad :\Longleftrightarrow \qquad \text{es gibt ein } g \in G \text{ mit } gm = m'\ .$$

Wir erkennen $(\sim)$ als reflexiv dank 1, als symmetrisch dank Inversem und als transitiv dank Produkt.

Es ist $(\sim)$ eine G-Äquivalenzrelation, mit zugehöriger trivialer Operation $! : G \longrightarrow \mathrm{S}_{\bar{M}}$. Denn sind $m,\, m' \in M$ und $g \in G$ mit $gm = m'$ gegeben, dann ist für $x \in G$ auch ${}^{x}gxm = xm'$.

(2) Die *Bahn* unter G oder *G-Bahn* von $m \in M$ sei die Äquivalenzklasse

$$Gm \ :=\ \{\, gm \,:\, g \in G \,\}$$

von m. Es ist Gm eine G-Teilmenge von M.

(3) Es heißt M *transitiv,* wenn M aus genau einer Bahn besteht.

Beispiel 12 Sei G als G-Menge via Konjugation aufgefaßt; cf. Beispiel 2.(5).

Die Bahnen von G unter dieser Operation von G heißen *Konjugationsklassen.* Ist $x \in G$, so schreiben wir ${}^G x := \{\, {}^g x \,:\, g \in G \,\}$ für die Konjugationsklasse von x.

Bemerkung 13 *Sei M eine transitive G-Menge.*

(1) *Die einzigen G-Teilmengen von M sind $\emptyset$ und M.*

(2) *Ist $M \longrightarrow T$ eine surjektive G-Abbildung in eine G-Menge T, dann ist auch T transitiv.*

Beweis.

Ad (1). Sei $X \subseteq M$ eine G-Teilmenge. Ist $X \neq \emptyset$, so können wir $x \in X$ wählen, und es wird $M = Gx \subseteq X$, i.e. $M = X$.

Ad (2). Seien $t, t' \in T$ gegeben. Wähle $m, m' \in M$ mit $f(m) = t$ und $f(m') = t'$. Da M transitiv ist, können wir $g \in G$ mit $gm = m'$ wählen. Es wird $gt = gf(m) = f(gm) = f(m') = t'$. ▫

Definition 14 Sei $k \geqslant 0$.

Eine G-Menge M heißt *k-fach transitiv,* wenn $M^{\times k, \neq}$ transitiv ist.

E.g. ist M einfach transitiv genau dann, wenn M transitiv ist.

Bemerkung 15 *Sei M eine G-Menge. Sei $0 \leqslant k \leqslant \ell$. Ist M eine ℓ-fach transitive G-Menge, so ist sie auch k-fach transitiv.*

Beweis. Wegen der ℓ-fachen Transitivität von M ist $|M| \geqslant \ell$. Die G-Abbildung

$$\begin{array}{rcl} M^{\times \ell, \neq} & \longrightarrow & M^{\times k, \neq} \\ (m_i)_{i \in [1,\ell]} & \longmapsto & (m_i)_{i \in [1,k]} \end{array}$$

ist mithin surjektiv. Aus der Transitivität von $M^{\times \ell, \neq}$ folgt also die Transitivität von $M^{\times k, \neq}$; cf. Bemerkung 13.(2). ▫

Beispiel 16

(1) Sei $n \geqslant 0$. Es ist $[1, n]$ eine n-fach transitive S_n-Menge, da für jedes Tupel paarweiser verschiedener Elemente aus $[1, n]$ ein – sogar genau ein – Element aus S_n existiert, das $(\,1\,,\,2\,,\ldots,\,n\,)$ auf dieses Tupel schickt.

Da die S_n-Abbildung $\mathrm{S}_n \longrightarrow [1, n]^{\times n, \neq}$, $\rho \longmapsto (\rho(i))_i$ nicht nur surjektiv, sondern auch injektiv ist, ist $[1, n]^{\times n, \neq}$ übrigens nicht nur transitiv, sondern sogar regulär; cf. Beispiel 5.

(2) Die alternierende Gruppe $\mathrm{A}_4 \leqslant \mathrm{S}_4$ ist gegeben durch

$$\begin{aligned}\mathrm{A}_4 \;=\; & \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3),\\ & (1,2,3), (1,2,4), (1,3,2), (1,3,4), (1,4,2), (1,4,3), (2,3,4), (2,4,3)\}\,.\end{aligned}$$

Die A_4-Menge $[1,4]$ ist 2-fach transitiv, da

$$\begin{aligned}& \mathrm{A}_4(\,1\,,\,2\,)\\ =\;& \{\,(\,\sigma(1)\,,\,\sigma(2)\,)\,:\,\sigma\in\mathrm{A}_4\,\}\\ =\;& \{\,(\,1\,,\,2\,)\,,\,(\,2\,,\,1\,)\,,\,(\,3\,,\,4\,)\,,\,(\,4\,,\,3\,)\,,\\ & \quad(\,2\,,\,3\,)\,,\,(\,2\,,\,4\,)\,,\,(\,3\,,\,1\,)\,,\,(\,3\,,\,2\,)\,,\,(\,4\,,\,1\,)\,,\,(\,4\,,\,2\,)\,,\,(\,1\,,\,3\,)\,,\,(\,1\,,\,4\,)\,\}\\ =\;& [1,4]^{\times 2,\neq}\,.\end{aligned}$$

Cf. auch Aufgabe 5.

Es ist aber $[1,4]$ keine 3-fach transitive A_4-Menge, da $(\,1\,,\,2\,,\,3\,)$ nicht mittels eines Elements aus A_4 nach $(\,1\,,\,2\,,\,4\,)$ multipliziert werden kann.

Übrigens ist $[1,4]^{\times 2,\neq}$ auch regulär, wie der Isomorphismus $\mathrm{A}_4 \xrightarrow{\sim} [1,4]^{\times 2,\neq}$, $\sigma \longmapsto (\,\sigma(1)\,,\,\sigma(2)\,)$ zeigt; cf. Beispiel 5.

1.2 Zentralisator

Sei $M = (M, \alpha)$ eine G-Menge; cf. Definition 1.

Definition 17 Sei $N \subseteq M$ eine Teilmenge. Sei

$$\mathrm{C}_G(N) \;:=\; \{\, g \in G \,:\, gn = n \text{ für } n \in N \,\}$$

der *Zentralisator* (oder *Stabilisator*) von N ([1]).

Da $1n = n$ ist und da aus $g,\, h \in \mathrm{C}_G(N)$ folgt, daß $h^- n = n$ und also auch $gh^- n = n$ ist für $n \in N$, ist $\mathrm{C}_G(N) \leqslant G$.

Insbesondere ist $\mathrm{C}_G(M) = \mathrm{Kern}(\alpha) \trianglelefteq G$.

Für $m \in M$ schreiben wir auch $\mathrm{C}_G(m) := \mathrm{C}_G(\{m\})$.

Ist $N \subseteq G$, so bezeichnet $\mathrm{C}_G(N)$ den Zentralisator von N als Teilmenge von G, gesehen als G-Menge via Konjugation; cf. Beispiel 2.(5).

Bemerkung 18 *Sei $N \subseteq M$ eine Teilmenge. Sei $x \in G$. Schreibe $xN := \{\, xn \,:\, n \in N \,\}$. Es ist*

$$\mathrm{C}_G(xN) \;=\; {}^x\mathrm{C}_G(N)\,.$$

[1] Das C in $\mathrm{C}_G(N)$ steht für engl. centraliser.

Beweis. Es ist $g \in \mathrm{C}_G(xN)$ genau dann, wenn $gxn = xn$ für $n \in N$, i.e. $x^- gxn = n$ für $n \in N$, i.e. $x^- gx \in \mathrm{C}_G(N)$, i.e. $g \in {}^x\mathrm{C}_G(N)$. ▫

Beispiel 19 Betrachte G als G-Menge via Konjugation.

Es ist $\mathrm{Z}(G) := \mathrm{C}_G(G) = \{\, z \in G \,:\, {}^z g = g \text{ für } g \in G \,\} = \{\, z \in G \,:\, zg = gz \text{ für } g \in G \,\}$ das *Zentrum* von G.

Lemma 20 (Bahnenlemma) *Sei $m \in M$.*

Wir haben die G-Bijektion

$$\begin{array}{rcl} G/\mathrm{C}_G(m) & \xrightarrow[\sim]{\beta_m} & Gm \\ g\mathrm{C}_G(m) & \longmapsto & gm\,. \end{array}$$

Beweis. Schreibe $C := \mathrm{C}_G(m)$.

Es ist β_m wohldefiniert und injektiv, da für $g, \tilde{g} \in G$ genau dann $gm = \tilde{g}m$ ist, wenn $m = g^- \tilde{g} m$ ist, i.e. $g^- \tilde{g} \in C$, i.e. $g^- \tilde{g} C = C$, i.e. $\tilde{g} C = gC$.

Es ist β_m surjektiv.

Es ist β_m eine G-Abbildung, da für $h \in G$ und $g \in G$ sich $\beta_m(hgC) = hgm = h\beta_m(gC)$ ergibt. ▫

Cf. auch Beispiel 10.

Korollar 21 *Ist G endlich und M transitiv, so ist $|M|$ ein Teiler von $|G|$.*

Beweis. Sei $m \in M$. Es ist $|G| = |Gm| \cdot |\mathrm{C}_G(m)| = |M| \cdot |\mathrm{C}_G(m)|$; cf. Lemma 20. ▫

Bemerkung 22 *Sei M transitiv. Sei $m \in M$.*

Sei $f : M \longrightarrow T$ eine surjektive G-Abbildung in eine G-Menge T. Dann gelten $(1, 2, 3)$.

(1) *Es ist $\mathrm{C}_G(m) \leqslant \mathrm{C}_G(f(m)) \leqslant G$.*

(2) *Es ist $\mathrm{C}_G(m) = \mathrm{C}_G(f(m))$ genau dann, wenn f bijektiv ist.*

(3) *Es ist $\mathrm{C}_G(f(m)) = G$ genau dann, wenn T trivial ist.*

Beweis. Es ist T transitiv; cf. Bemerkung 13.(2). Also ist T isomorph zu $G/\mathrm{C}_G(f(m))$ gemäß Lemma 20.

Ad (1). Für $g \in G$ folgt aus $g \in \mathrm{C}_G(m)$, daß $gf(m) = f(gm) = f(m)$ und also $g \in \mathrm{C}_G(f(m))$ ist.

Ad (2). Sei f injektiv. Ist $g \in \mathrm{C}_G(f(m))$, dann folgt aus $f(gm) = gf(m) = f(m)$, daß $gm = m$ und also $g \in \mathrm{C}_G(m)$ ist. Also ist $\mathrm{C}_G(m) = \mathrm{C}_G(f(m))$; cf. (1).

Sei umgekehrt $\mathrm{C}_G(m) = \mathrm{C}_G(f(m))$. Sind g, $h \in G$ gegeben mit $f(gm) = f(hm)$, dann ist $gf(m) = hf(m)$, also $h^- gf(m) = f(m)$, also $h^- g \in \mathrm{C}_G(f(m)) = \mathrm{C}_G(m)$, also $h^- gm = m$ und somit $gm = hm$. Also ist f injektiv.

Ad (3). Ist T trivial, dann ist $|T| = 1$ und also $\mathrm{C}_G(f(m)) = G$.

Ist umgekehrt $\mathrm{C}_G(f(m)) = G$, dann ist T isomorph zu G/G, i.e. trivial. ▫

1.3 Fixpunkte

Sei M eine G-Menge.

Definition 23 Sei $A \subseteq G$ eine Teilmenge. Sei

$$\mathrm{Fix}_A(M) \;:=\; \{\, m \in M \,:\, am = m \text{ für } a \in A \,\}$$

die Menge der *Fixpunkte* von M unter A. Ist $A = \{g\}$ für ein $g \in G$, so schreiben wir auch $\mathrm{Fix}_g(M) := \mathrm{Fix}_{\{g\}}(M)$.

Bemerkung 24 *Sei $x \in G$. Sei $A \subseteq G$. Es ist $\mathrm{Fix}_{({}^xA)}(M) = x\,\mathrm{Fix}_A(M)$.*

Beweis. Es ist $m \in \mathrm{Fix}_{{}^xA}(M)$ genau dann, wenn ${}^xa \cdot m = m$ für $a \in A$, i.e. wenn $ax^- m = x^- m$ für $a \in A$, i.e. wenn $x^- m \in \mathrm{Fix}_A(M)$, i.e. wenn $m \in x\,\mathrm{Fix}_A(M)$. ▫

Lemma 25 (Cauchy) *Seien G und M endlich.*
Sei $t := |\{\, {}^Gg \,:\, g \in G \,\}|$. Wähle $g_i \in G$ für $i \in [1,t]$ mit $G = \bigsqcup_{i\in[1,t]} {}^Gg_i$.
Dann ist

$$|\{\, Gm \,:\, m \in M \,\}| \;=\; \frac{1}{|G|}\sum_{g\in G} |\,\mathrm{Fix}_g(M)| \;=\; \sum_{i\in[1,t]} \frac{|\,\mathrm{Fix}_{g_i}(M)|}{|\mathrm{C}_G(g_i)|}\;.$$

Beweis.

Zeigen wir die erste Gleichheit. Sei $\ell := |\{\, Gm \,:\, m \in M \,\}|$. Wähle $m_i \in M$ mit $M = \bigsqcup_{i\in[1,\ell]} Gm_i$. Es wird

$$\begin{array}{rcl}
\sum_{g\in G} |\,\mathrm{Fix}_g(M)| & = & |\{\, (g,m) \in G \times M \,:\, m \in \mathrm{Fix}_g(M) \,\}| \\
& = & |\{\, (g,m) \in G \times M \,:\, gm = m \,\}| \\
& = & |\{\, (g,m) \in G \times M \,:\, g \in \mathrm{C}_G(m) \,\}| \\
& = & \sum_{m\in M} |\mathrm{C}_G(m)| \\
& \overset{\text{L. 20}}{=} & |G| \sum_{m\in M} |Gm|^{-1} \\
& = & |G| \sum_{i\in[1,\ell]} |Gm_i|\,|Gm_i|^{-1} \\
& = & |G| \cdot \ell\;.
\end{array}$$

Zeigen wir die zweite Gleichheit. Es genügt, $\frac{1}{|G|}\sum_{g\in {}^G g_i} |\operatorname{Fix}_g(M)| \overset{!}{=} \frac{|\operatorname{Fix}_{g_i}(M)|}{|\mathrm{C}_G(g_i)|}$ zu zeigen für $i \in [1,t]$. Gemäß Bemerkung 24 ist

$$\begin{aligned}\sum_{g\in {}^G g_i} |\operatorname{Fix}_g(M)| &\overset{\text{B. 24}}{=} \sum_{g\in {}^G g_i} |\operatorname{Fix}_{g_i}(M)| \\ &= |{}^G g_i| \cdot |\operatorname{Fix}_{g_i}(M)| \\ &\overset{\text{L. 20}}{=} |G| \cdot |\mathrm{C}_G(g_i)|^{-1} \cdot |\operatorname{Fix}_{g_i}(M)| \,.\end{aligned}$$

□

Lemma 25 ist auch ein Spezialfall der Frobenius-Reziprozität aus der Charaktertheorie, sofern diese bekannt sein sollte. Sei dazu o.E. M transitiv. Es ist $g \mapsto |\operatorname{Fix}_g(M)|$ der Charakter des zu M gehörigen Permutationsmodul, welcher sich aus dem trivialen Charakter von $\mathrm{C}_G(m)$ durch Induktion nach G ergibt, wobei $m \in M$ zu wählen ist. Da das Skalarprodukt des trivialen Charakters von $\mathrm{C}_G(m)$ mit sich selbst gleich 1 ist, gilt dies dank dieser Reziprozität auch für das Skalarprodukt dieses Charakters mit dem trivialen Charakter von G.

1.4 Primitivität

Sei $M = (M, \alpha)$ eine G-Menge; cf. Definition 1.

Definition 26 Sei M nichttrivial und transitiv.

(1) Es heißt M *primitiv*, wenn für jede surjektive G-Abbildung $f : M \longrightarrow\!\!\!\!\!\rightarrow T$ in eine G-Menge T entweder f bijektiv ist oder T trivial ist.

(2) Eine nichtleere Teilmenge $B \subseteq M$ heißt *Block* von M, wenn für $g \in G$ entweder $gB = B$ oder $gB \cap B = \emptyset$ ist.

Grob gesprochen: Eine transitive G-Menge hat nur die unvermeidbaren Teilobjekte; cf. Bemerkung 13.(1). Eine primitive G-Menge hat zudem nur die unvermeidbaren Faktorobjekte.

Beispiel 27 Sei G endlich. Dann ist M endlich. Ist $|M|$ prim, dann ist M primitiv. Denn ist $f : M \longrightarrow\!\!\!\!\!\rightarrow T$ eine surjektive G-Abbildung in eine nichttriviale G-Menge T und ist $m \in M$, so ist $\mathrm{C}_G(m) \leqslant \mathrm{C}_G(f(m)) < G$ nach Bemerkung 22.(1, 3), folglich $[G : \mathrm{C}_G(f(m))]$ ungleich 1 und Teiler der Primzahl $[G : \mathrm{C}_G(m)] \overset{\text{L. 20}}{=} |M|$, folglich $[G : \mathrm{C}_G(f(m))] = [G : \mathrm{C}_G(m)]$, i.e. $\mathrm{C}_G(m) = \mathrm{C}_G(f(m))$, i.e. f bijektiv; cf. Bemerkung 22.(2).

Lemma 28 *Sei an M nichttrivial und transitiv.*

Die folgenden Aussagen $(1, 2, 3, 4, 5)$ sind äquivalent.

(1) *Es ist M primitiv.*

(2) *Es gibt auf M keine G-Äquivalenzrelation, die weder diskret noch verklumpt ist.*

(3) *Es gibt in M keinen Block B mit $|B| > 1$ und $B \subset M$.*

(4) *Für ein $m \in M$ ist $\mathrm{C}_G(m)$ maximal in der Menge der echten Untergruppen von G.*

(5) *Für jedes $m \in M$ ist $\mathrm{C}_G(m)$ maximal in der Menge der echten Untergruppen von G.*

Beweis.

Ad (5) $\Rightarrow$ (4). Da M transitiv ist, ist $M \neq \emptyset$.

Ad (4) $\Rightarrow$ (5). Für $x \in G$ und $m_0 \in M$ ist $\mathrm{C}_G(xm_0) = {}^x\mathrm{C}_G(m_0)$, sodaß aus $\mathrm{C}_G(m_0)$ maximal folgt, daß auch $\mathrm{C}_G(xm_0)$ maximal ist; cf. Bemerkung 18. Dank Transitivität von M folgt also aus $\mathrm{C}_G(m_0)$ maximal für ein $m_0 \in M$, daß $\mathrm{C}_G(m)$ maximal ist für alle $m \in M$.

Ad (5) $\Rightarrow$ (1). Sei $f : M \longrightarrow T$ eine surjektive G-Abbildung in eine nichttriviale G-Menge T. Wir haben f als bijektiv nachzuweisen.

Sei $m \in M$. Es ist $\mathrm{C}_G(m) \leqslant \mathrm{C}_G(f(m)) \leqslant G$; cf. Bemerkung 22.(1). Da T nichttrivial ist, ist $\mathrm{C}_G(f(m)) < G$; cf. Bemerkung 22.(3). Da $\mathrm{C}_G(m)$ maximal ist, folgt $\mathrm{C}_G(m) = \mathrm{C}_G(f(m))$. Mithin ist f bijektiv; cf. Bemerkung 22.(2).

Ad (1) $\Rightarrow$ (5). Sei $m \in M$ gegeben. Es ist $\mathrm{C}_G(m) < G$, da sonst $M = Gm = \{m\}$ folgte, mithin M trivial wäre, was nicht der Fall ist.

Annahme, es gibt $\mathrm{C}_G(m) < U < G$. Dann ist G/U nichttrivial. Wir erhalten als Kompositum von $M \xrightarrow{\sim} G/\mathrm{C}_G(m) \longrightarrow G/U$ eine surjektive, nichtinjektive G-Abbildung; cf. Beispiel 4, Lemma 20. Dies steht im *Widerspruch* zur Primitivität von M.

Ad ($\neg$1) $\Rightarrow$ ($\neg$2). Sei M nicht primitiv. Dann gibt es eine surjektive, nichtinjektive G-Abbildung $f : M \longrightarrow T$ mit T nichttriviale G-Menge. Für $m, m' \in M$ setzen wir $m \sim m' :\Leftrightarrow f(m) = f(m')$. Dann ist ($\sim$) eine G-Äquivalenzrelation; cf. Beispiel 10. Da f nichtinjektiv ist, ist ($\sim$) nicht diskret. Da T nichttrivial ist, ist ($\sim$) nicht verklumpt.

Ad ($\neg$2) $\Rightarrow$ ($\neg$1). Sei ($\sim$) eine G-Äquivalenzrelation auf M, die weder diskret noch verklumpt ist. Schreibe $\bar{M} := M/(\sim)$ und $\bar{m}$ für die Äquivalenzklasse von $m \in M$. Wir haben die surjektive G-Abbildung $M \longrightarrow \bar{M}$, $m \longmapsto \bar{m}$; cf. Definition 9. Es ist $\bar{M}$ nichttrivial, da ($\sim$) nicht verklumpt ist. Es ist diese Abbildung nicht bijektiv, da ($\sim$) nicht diskret ist.

Ad ($\neg$2) $\Rightarrow$ ($\neg$3). Sei ($\sim$) eine G-Äquivalenzrelation auf M, die weder diskret noch verklumpt ist. Für $m \in M$ und $g \in G$ gibt die Multiplikation mit g eine Bijektion von der Äquivalenzklasse von m zur Äquivalenzklasse von gm. Somit ist jede Äquivalenzklasse von ($\sim$) ein Block. Sei B eine Äquivalenzklasse von ($\sim$), mithin ein Block. Es ist $|B| > 1$, da ($\sim$) nicht diskret ist. Es ist $B \subset M$, da ($\sim$) nicht verklumpt ist.

Ad ($\neg$3) $\Rightarrow$ ($\neg$2). Sei $B \subset M$ ein Block mit $|B| > 1$. Für $m, m' \in M$ gelte $m \sim m'$, wenn es ein $g \in G$ gibt mit $gm \in B$ und $gm' \in B$. Es ist ($\sim$) eine Äquivalenzrelation, denn Reflexivität folgt aus M transitiv, Symmetrie folgt aus der Konstruktion, und Transitivität

ergibt sich, da für m, m', $m'' \in M$ und g, $h \in G$ aus gm, $gm' \in B$ und hm', $hm'' \in B$ auch $gm' \in B \cap gh^- B$, also $B = gh^- B$ und somit $gm'' \in gh^- B = B$ folgt. Es ist $(\sim)$ eine G-Äquivalenzrelation, da für m, $m' \in M$ und g, $x \in G$ aus gm, $gm' \in B$ auch $gx^-(xm)$, $gx^-(xm') \in B$ folgt. Es ist $(\sim)$ nicht diskret, da $|B| > 1$. Es ist $(\sim)$ nicht verklumpt, da $B \subset M$ und infolgedessen für $m \in M \smallsetminus B$, $b \in B$ und $g \in G$ nicht gm, $gb \in B$ gelten kann, da ansonsten aus $b \in B \cap g^- B$ auch $B = g^- B \ni m$ folgte. ▫

Lemma 29 *Sei M zweifach transitiv. Dann ist M primitiv.*

Beweis. Es ist $M^{\times 2, \neq} \neq \emptyset$, also $|M| \geqslant 2$ und somit M nichttrivial. Es ist M transitiv; cf. Bemerkung 15.

Annahme, M ist nicht primitiv. Dann gibt es eine G-Äquivalenzrelation $(\sim)$ auf M, die weder diskret noch verklumpt ist; cf. Lemma 28. Wähle m, m', $m'' \in M$ mit $m \neq m'$ und $m \sim m' \not\sim m''$. Da M zweifach transitiv ist, gibt es ein $g \in G$ mit $g(m, m') = (m, m'')$, i.e. mit $gm = m$ und $gm' = m''$. Dann aber ist $m'' = gm' \sim gm = m$, und wir haben einen *Widerspruch.* ▫

Beispiel 30 Sei $n \geqslant 2$. Sei $G := \mathrm{S}_n$. Sei $M := [1, n]$; cf. Beispiel 2.(1). Es ist $\mathrm{C}_{\mathrm{S}_n}(n) = \mathrm{S}_{[1,n-1]} = \mathrm{S}_{n-1}$.

Es ist $[1, n]$ eine n-fach transitive S_n-Menge; cf. Beispiel 16.(1). Da $n \geqslant 2$, ist $[1, n]$ auch eine 2-fach transitive S_n-Menge; cf. Bemerkung 15. Folglich ist $[1, n]$ eine primitive S_n-Menge; cf. Lemma 29. Also ist $\mathrm{S}_{n-1} < \mathrm{S}_n$ eine maximale echte Untergruppe; cf. Lemma 28. Ist n prim, dann ist dies auch von vornherein klar.

Beispiel 31 Sei K ein Körper.

Sei V ein endlichdimensionaler K-Vektorraum mit $n := \dim_K V \geqslant 2$.

Es ist V eine $\mathrm{GL}(V)$-Menge; cf. Beispiel 2.(4). Es ist $V^\times \subseteq V$ eine $\mathrm{GL}(V)$-Teilmenge.

Für v, $\tilde{v} \in V^\times$ sei $v \sim \tilde{v}$, wenn es ein $\lambda \in K^\times$ gibt mit $\lambda v = \tilde{v}$. Es ist $(\sim)$ eine Äquivalenzrelation, reflexiv dank 1, symmetrisch dank λ^-, transitiv dank Produkt. Es ist $(\sim)$ eine $\mathrm{GL}(V)$-Äquivalenzrelation, da für $\alpha \in \mathrm{GL}(V)$, für v, $\tilde{v} \in V^\times$ und $\lambda \in K^\times$ aus $\lambda v = \tilde{v}$ folgt, daß $\lambda\alpha(v) = \alpha(\lambda v) = \alpha(\tilde{v})$ ist.

Schreibe $\mathrm{P}(V) := V^\times/(\sim)$ für die resultierende $\mathrm{GL}(V)$-Menge. Für $v \in V^\times$ ist die Äquivalenzklasse $\bar{v}$ die von v aufgespannte Gerade in V, ausgenommen 0. Geometrisch gesehen ist $\mathrm{P}(V)$ der projektive Raum von V.

Durch Einschränkung wird $\mathrm{P}(V)$ zu einer $\mathrm{SL}(V)$-Menge; cf. Beispiel 2.(2).

Wir wollen $\mathrm{P}(V)$ als zweifach transitive $\mathrm{SL}(V)$-Menge erkennen.

Zunächst ist $\mathrm{P}(V)^{\times 2, \neq} \neq \emptyset$, da $|\mathrm{P}(V)| \geqslant 2$, da $\dim_K V \geqslant 2$.

Für $\bar{v}$, $\bar{v}' \in \mathrm{P}(V)$ mit $\bar{v} \neq \bar{v}'$ ist (v, v') linear unabhängig, sodaß wir (v, v') zu einer Basis $(v_1, v_2, \ldots, v_n)$ von V ergänzen können, wobei $v_1 = v$ und $v_2 = v'$.

Für $\bar{w}$, $\bar{w}' \in \mathrm{P}(V)$ mit $\bar{w} \neq \bar{w}'$ ist (w, w') linear unabhängig, sodaß wir (w, w') zu einer Basis $(w_1\,,\, w_2\,,\, \ldots\,,\, w_n)$ von V ergänzen können, wobei $w_1 = w$ und $w_2 = w'$.

Es gibt genau ein $\alpha \in \mathrm{GL}(V)$ mit $\alpha(v_i) = w_i$ für $i \in [1, n]$.

Es gibt genau ein $\beta \in \mathrm{GL}(V)$ mit $\beta(v_1) = w_1/\det(\alpha)$ und $\beta(v_i) = w_i$ für $i \in [2, n]$. Es ist $\det(\beta) = \det(\alpha)/\det(\alpha) = 1$, i.e. $\beta \in \mathrm{SL}(V)$. Es ist $\beta \cdot (\bar{v}, \bar{v}') = \beta \cdot (\bar{v}_1\,,\, \bar{v}_2) = (\overline{w_1/\det(\alpha)}, \bar{w}_2) = (\bar{w}_1\,,\, \bar{w}_2) = (\bar{w}, \bar{w}')$.

Folglich ist $\mathrm{P}(V)$ eine zweifach transitive und damit auch primitive $\mathrm{SL}(V)$-Menge; cf. Lemma 29.

Sei $m \geqslant 2$. Wir schreiben auch $\mathrm{P}^{m-1}(K) := \mathrm{P}(K^m)$. Es ist also auch $\mathrm{P}^{m-1}(K)$ eine zweifach transitive und somit primitive $\mathrm{SL}_m(K)$-Menge.

1.5 Bahnenalgorithmus

Sei G endlich erzeugt, i.e. sei es uns möglich, eine endliche Teilmenge $S \subseteq G$ zu wählen mit

$$G \;=\; \langle S \rangle\ .$$

Schreibe $S^{\pm} := S \cup \{\, s^- \,:\, s \in S,\ |\langle s \rangle| = \infty \,\}$.

Dann ist jedes Element von G schreibbar als ein Produkt von Elementen aus $S^{\pm}$.

Falls G endlich ist, dann ist $S = S^{\pm}$.

Sei M eine G-Menge.

Sei $m \in M$ gegeben mit Gm endlich.

> Der Bahnenalgorithmus wird zugleich die Berechnung von Gm und von Erzeugern von $\mathrm{C}_G(m)$ liefern.

Lemma 32 (Schreier)

Wähle $T \subseteq G$ mit $Tm = Gm$, mit $|T| = |Gm|$ und mit $1 \in T$.

Sei $\tau : G \longrightarrow T$ festgelegt durch $\tau(g)m = gm$ für $g \in G$. Insbesondere ist $\tau(t) = t$ für $t \in T$, speziell auch $\tau(1) = 1$.

Dann ist

$$\mathrm{C}_G(m) \;=\; \langle\, \tau(xt)^- xt \,:\, x \in S^{\pm},\ t \in T \,\rangle$$

Beweis.

Ad $\geqslant$. Es ist $xtm = \tau(xt)m$, i.e. $\tau(xt)^- xtm = m$, i.e. $\tau(xt)^- xt \in \mathrm{C}_G(m)$ für $x \in S^{\pm}$ und $t \in T$.

Ad $\leqslant$. Sei $g \in \mathrm{C}_G(m)$. Schreibe $g = x_k\, x_{k-1} \cdot \ldots \cdot x_1$ mit $k \geqslant 0$ und $x_i \in S^{\pm}$ für $i \in [1, k]$.

Wir setzen rekursiv $t_1 := 1$ und $t_{i+1} := \tau(x_i t_i)$ für $i \in [1,k]$. Schreibe $y_i := \tau(x_i t_i)^- x_i t_i = t_{i+1}^- x_i t_i$ für $i \in [1,k]$. Es wird

$$\begin{aligned} y &:= y_k\, y_{k-1} \cdot \ldots \cdot y_2\, y_1 \\ &= (t_{k+1}^- x_k t_k)(t_k^- x_{k-1} t_{k-1}) \cdot \ldots \cdot (t_3^- x_2 t_2)(t_2^- x_1 t_1) \\ &= t_{k+1}^-\, x_k\, x_{k-1} \cdot \ldots \cdot x_2\, x_1 \\ &= t_{k+1}^- g\ . \end{aligned}$$

Da, wie schon gesehen, $y \in \mathrm{C}_G(m)$ liegt, ist $m = ym = t_{k+1}^- gm = t_{k+1}^- m$, also $t_{k+1} m = m = 1 \cdot m$ und somit $t_{k+1} = \tau(1) = 1$. Es folgt

$$g \ = \ y \ \in \ \langle\, \tau(xt)^- xt \ : \ x \in S^{\pm},\ t \in T \,\rangle\ .$$

□

Algorithmus 33 (Bahnenalgorithmus)

Setze

$$N_0 \ := \ \{m\}$$

und für $i \geqslant 0$ rekursiv

$$N_{i+1} \ := \ \{\, xn \ : \ x \in S^{\pm},\ n \in N_i\,,\ xn \notin \bigsqcup_{h\in[0,i]} N_h \,\}\ .$$

Setze

$$T_0 \ := \ \{1\}\ .$$

Beachte $T_0\, m = N_0$.

Setze für $i \geqslant 0$

$$\tilde{T}_{i+1} \ := \ \{\, xt \ : \ x \in S^{\pm},\ t \in T_i\,,\ xtm \in N_{i+1} \,\}$$

Induktiv nehmen wir $T_i\, m = N_i$ an. Es folgt $\tilde{T}_{i+1}\, m = N_{i+1}$. Wähle $T_{i+1} \subseteq \tilde{T}_{i+1}$ so, daß $T_{i+1} \longrightarrow N_{i+1}$, $\hat{t} \longmapsto \hat{t}m$ bijektiv ist. I.e. für alle $\hat{n} \in N_{i+1}$ gibt es genau ein $\hat{t} \in T_{i+1}$ mit $\hat{t}m = \hat{n}$. Insbesondere folgt auch $T_{i+1}\, m = N_{i+1}$.

Für $i \geqslant 0$ schreiben wir $N_{[0,i]} := \bigsqcup_{h\in[0,i]} N_h$ und $T_{[0,i]} := \bigsqcup_{h\in[0,i]} T_h$.

E.g. ist $N_{i+1} = \{\, xn \ : \ x \in S^{\pm},\ n \in N_i\,,\ xn \notin N_{[0,i]} \,\}$.

Für gegebenes $i \geqslant 0$ folgt aus $N_i = \emptyset$ auch $N_{i+1} = \emptyset$. Also gibt es genau ein

$$j \ \geqslant \ 0$$

mit $N_i \neq \emptyset$ für $i \leqslant j$ und $N_i = \emptyset$ für $i \geqslant j+1$.

Sei $g \in G$. Schreibe $gm = x_\ell\, x_{\ell-1} \cdot \ldots \cdot x_1 m$ mit $\ell \geqslant 0$ und $x_i \in S^{\pm}$ für $i \in [1,\ell]$; sei hierfür ℓ minimal. Wir *behaupten* $gm \overset{!}{\in} N_\ell$. Wir wollen induktiv $x_i\, x_{i-1} \cdot \ldots \cdot x_1 m \overset{!}{\in} N_i$ zeigen für $i \in [0,\ell]$. Die Aussage ist richtig für $i = 0$. Sei die Aussage richtig für ein $i \in [0, \ell-1]$. Es wird $x_{i+1}\, x_i\, x_{i-1} \cdot \ldots \cdot x_1 m \notin N_{[0,i]}$, da *sonst* $x_{i+1}\, x_i\, x_{i-1} \cdot \ldots \cdot x_1 m = y_k\, y_{k-1} \cdot \ldots \cdot y_1 m$

wäre für ein $k \in [0,i]$ und gewisse $y_h \in S^{\pm}$ für $h \in [1,k]$, woraus $gm = x_\ell\, x_{\ell-1} \cdot \ldots \cdot x_1 m = x_\ell\, x_{\ell-1} \cdot \ldots \cdot x_{i+2}\, y_k\, y_{k-1} \cdot \ldots \cdot y_1 m$ folgte, was wegen der Minimalität von ℓ *nicht* so ist. Folglich ist $x_{i+1}\, x_i\, x_{i-1} \cdot \ldots \cdot x_1 m \in N_{i+1}$. Dies zeigt die Induktion. Die *Behauptung* folgt hieraus für $i = \ell$.

Insbesondere ist $N_{[0,j]} = Gm$.

Somit gibt es für jedes $g \in G$ genau ein $t \in T_{[0,j]}$ mit $tm = gm$. Sei $\tau : G \longrightarrow T_{[0,j]}$ mit $gm = \tau(g)m$ für $g \in G$.

Sei $\hat{R} := \{\, xt \,:\, x \in S^{\pm},\ t \in T_{[0,j]} \,\}$. Gemäß Lemma 32 ist

$$\mathrm{C}_G(m) \;=\; \langle\, \tau(xt)^- xt \,:\, x \in S^{\pm},\ t \in T_{[0,j]} \,\rangle \;=\; \langle\, \tau(r)^- r \,:\, r \in \hat{R} \,\rangle\ .$$

Für $r \in \hat{R} \cap T_{[0,j]}$ ist $\tau(r)^- r = 1$. Für

$$\hat{R} \;\supseteq\; R \;\supseteq\; \hat{R} \smallsetminus T_{[0,j]}$$

ist also immer noch

$$\mathrm{C}_G(m) \;=\; \langle\, \tau(r)^- r \,:\, r \in R \,\rangle\ .$$

Zur Durchführung des Algorithmus erstelle man in der Praxis wie folgt einen Baum, bestehend aus Elementen von M als Ecken und hinzugefügten Kanten. Man arbeite die Schritte von rechts nach links ab. Innerhalb eines Schritts arbeite man von oben nach unten.

Schritt 0. Beginne rechts mit m als Wurzel. Es ist $N_0 = \{m\}$. Es ist $T_0 = \{1\}$.

Schritt 1. Multipliziere m mit den Elementen von $S^{\pm}$. Verbinde m nach links mit den Produkten, wobei auf den Kanten die benötigten Faktoren aus $S^{\pm}$ notiert werden. Elemente, die dabei entstehen und die bereits vorher in den Schritten 0 bis 1 aufgetreten sind, werden markiert. Die unmarkierten entstandenen Elemente bilden N_1. Ferner besteht T_1 aus den auf den Kanten von einem unmarkierten entstandenen Element zur Wurzel m notierten Gruppenelementen.

Schritt 2. Multipliziere die Elemente von N_1 mit den Elemente von $S^{\pm}$. Verbinde die Elemente von N_1 nach links mit den aus ihnen hervorgegangenen Produkten, wobei auf den Kanten die benötigten Faktoren aus $S^{\pm}$ notiert werden. Elemente, die dabei entstehen und die bereits vorher in den Schritten 0 bis 2 aufgetreten sind, werden markiert. Die unmarkierten entstandenen Elemente bilden N_2. Ferner besteht T_2 aus den Produkten der auf den Kantenzügen von einem unmarkierten entstandenen Element zur Wurzel m notierten Gruppenelementen.

Schritt 3. Multipliziere die Elemente von N_2 mit den Elemente von $S^{\pm}$. Verbinde die Elemente von N_2 nach links mit den aus ihnen hervorgegangenen Produkten, wobei auf den Kanten die benötigten Faktoren aus $S^{\pm}$ notiert werden. Elemente, die dabei entstehen und die bereits vorher in den Schritten 0 bis 3 aufgetreten sind, werden markiert. Die unmarkierten entstandenen Elemente bilden N_3. Ferner besteht T_3 aus den Produkten

der auf den Kantenzügen von einem unmarkierten entstandenen Element zur Wurzel m notierten Gruppenelementen.

Usf.

Dies setzen wir so fort, bis sich für ein $j \geqslant 0$ dann $N_j \neq \emptyset$, aber $N_{j+1} = \emptyset$ ergibt.

Dann besteht Gm aus den unmarkierten Elementen des Baums.

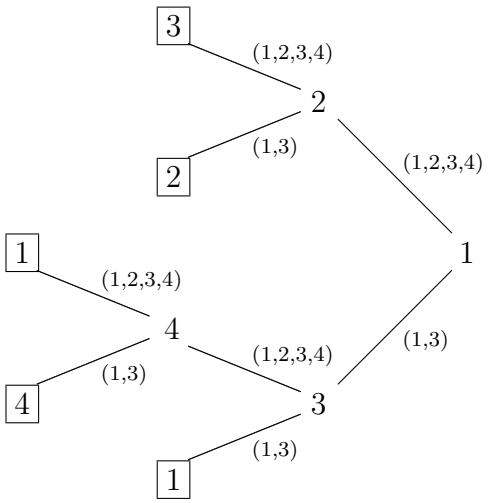
Für jedes markierte Element des Baums nehmen wir das Produkt r der auf dem Kantenzug von diesem Element nach m notierten Faktoren. Dieses markierte Element tritt rechts oder oberhalb von sich bereits unmarkiert im Baum auf. Das Produkt der auf dem Kantenzug von diesem unmarkierten Element nach m markierten Faktoren ist $\tau(r)$. Bilde $\tau(r)^- r$. Sodann ist $\mathrm{C}_G(m)$ erzeugt von den so entstandenen Elementen $\tau(r)^- r$.

Oft kann durch direkte Betrachtung das so gewonnene Erzeugendensystem von $\mathrm{C}_G(m)$ noch reduziert werden.

Beispiel 34 Sei $G := \langle (1,2,3,4), (1,3) \rangle \leqslant \mathrm{S}_4$. Sei $S := \{(1,2,3,4), (1,3)\}$. Es ist $S^{\pm} = S$, da alle Elemente von S endliche Ordnung haben.

Sei $M := [1,4]$; cf. Beispiel 2.(1). Sei $m = 1$.

Durchführung des Bahnenalgorithmus, Algorithmus 33, liefert folgenden von rechts nach links erstellten Baum.



Somit ist M transitiv.

In der Notation von Algorithmus 33 ist $j = 2$ und

$$T_{[0,2]} \;=\; \{ \overbrace{\mathrm{id}}^{\in T_0} \,,\, \overbrace{(1,2,3,4)\,,\,(1,3)}^{\in T_1} \,,\, \overbrace{\underbrace{(1,2,3,4)\circ(1,3)}_{=(1,4)(2,3)}}^{\in T_2} \}$$

Ferner ist $\mathrm{C}_G(m)$ erzeugt von folgender Liste von Elementen.

$$\begin{aligned}
(1,3)^- \circ ((1,2,3,4) \circ (1,2,3,4)) &= (2,4) \\
(1,2,3,4)^- \circ ((1,3) \circ (1,2,3,4)) &= (2,4) \\
\mathrm{id}^- \circ ((1,2,3,4) \circ (1,2,3,4) \circ (1,3)) &= (2,4) \\
((1,2,3,4) \circ (1,3))^- \circ ((1,3) \circ (1,2,3,4) \circ (1,3)) &= (2,4) \\
\mathrm{id}^- \circ ((1,3) \circ (1,3)) &= \mathrm{id}
\end{aligned}$$

Folglich ist $\mathrm{C}_G(m) = \langle (2,4) \rangle$.

Insbesondere ist $|\mathrm{C}_G(m)| = 2$ und $|Gm| = 4$, woraus wir $|G| = |Gm| \cdot |\mathrm{C}_G(m)| = 8$ entnehmen; cf. Lemma 20.

> Ist die Ordnung von $\mathrm{C}_G(m)$ an dieser Stelle noch nicht ablesbar, so kann das Verfahren fortgesetzt werden, indem $m' \in M \setminus \{m\}$ gewählt und die Operation von $\mathrm{C}_G(m)$ auf $M \setminus \{m\}$ betrachtet wird. Diese Iteration des Bahnenalgorithmus nennt man Schreier-Sims-Algorithmus.

Kapitel 2

Anwendungen der G-Mengentheorie

2.1 Sylow

Wir folgen [**1,** (5.17), §6].

Sei G eine endliche Gruppe. Sei $p > 0$ eine Primzahl.

Definition 35

(1) Eine endliche Gruppe H heißt *p-Gruppe*, falls $|H| = |H|[p]$ ist, i.e. falls $|H|$ eine Potenz von p ist.

(2) Es heißt $U \leqslant G$ eine *p-Untergruppe,* falls U eine p-Gruppe ist.

(3) Es heißt $P \leqslant G$ eine *p-Sylowuntergruppe*, kurz: *p-Sylowgruppe*, falls $|P| = |G|[p]$ ist, i.e. falls P eine p-Untergruppe von G und $[G : P]$ teilerfremd zu p ist.

(4) Die Menge der p-Sylowuntergruppen von G wird mit $\mathrm{Syl}_p(G)$ bezeichnet. Es ist $\mathrm{Syl}_p(G)$ eine G-Teilmenge von $\mathrm{Pot}(G)$ im Sinne von Aufgabe 4.(7).

Lemma 36 *Sei M eine nichtleere endliche G-Menge.*

Gebe es für jedes $m \in M$ eine p-Untergruppe $P(m) \leqslant G$ mit $\mathrm{Fix}_{P(m)}(M) = \{m\}$.

Dann ist M transitiv und $|M| \equiv_p 1$.

Beweis. Wähle $n \in M$. Betrachte die G-Teilmengen $N := Gn$ und $N' := M \smallsetminus Gn$ von M. Dies sind insbesondere $P(n)$-Teilmengen der $P(n)$-Menge $M\downarrow_{P(n)}$. Es ist $\mathrm{Fix}_{P(n)}(M) = \{n\}$. Dank Aufgabe 7.(1) ist

$$|N| \equiv_p |\mathrm{Fix}_{P(n)}(N)| = |\{n\} \cap N| = |\{n\}| = 1$$

und

$$|N'| \equiv_p |\mathrm{Fix}_{P(n)}(N')| = |\{n\} \cap N'| = |\emptyset| = 0 .$$

Da N zudem eine transitive G-Menge ist, bleibt $N \stackrel{!}{=} M$ zu zeigen, i.e. $N' \stackrel{!}{=} \emptyset$.

Annahme $N' \neq \emptyset$. Wähle $n' \in N'$. Es ist $\mathrm{Fix}_{P(n')}(M) = \{n'\}$. Folglich ist mit Aufgabe 7.(1)

$$|N'| \equiv_p |\mathrm{Fix}_{P(n')}(N')| = |\{n'\} \cap N'| = |\{n'\}| = 1 ,$$

im *Widerspruch* zu $|N'| \equiv_p 0$. □

Lemma 37 *Sei* $\Omega := \{ U \leqslant G : U \text{ ist eine } p\text{-Untergruppe von } G \}$. *Es operiert* G *auf* Ω *via Konjugation; cf. Aufgabe* 4.(7).

Sei $\Omega_{\max} \subseteq \Omega$ *die* G*-Teilmenge der maximalen Elemente von* Ω*, i.e. die Menge der maximalen* p*-Untergruppen von* G*. Dies ist eine* G*-Teilmenge von* Ω*; cf. Aufgabe* 4.(8).

Es ist $\Omega_{\max} \neq \emptyset$.

Für $Q \in \Omega_{\max}$ *ist* $\mathrm{Fix}_Q(\Omega_{\max}) = \{Q\}$.

Beweis. Da $1 \in \Omega$ liegt und da Ω endlich ist, ist $\Omega_{\max} \neq \emptyset$.

Zeigen wir $\mathrm{Fix}_Q(\Omega_{\max}) \stackrel{!}{=} \{Q\}$.

Ad $\supseteq$. Da ${}^gQ = Q$ für $g \in Q$ ist, ist $Q \in \mathrm{Fix}_Q(\Omega_{\max})$.

Ad $\subseteq$. Sei $P \in \mathrm{Fix}_Q(\Omega_{\max})$ gegeben, i.e. sei ${}^gP = P$ für $g \in Q$, i.e. sei $Q \leqslant \mathrm{N}_G(P)$; cf. Aufgabe 4.(6). Dann ist $PQ \leqslant G$ mit $|PQ| = |P| \cdot |Q| / |P \cap Q|$; cf. Aufgabe 12.(1, 2). Insbesondere ist $|PQ|$ eine Potenz von p.

Annahme, es ist $P \neq Q$. Wegen Maximalität von Q ist dann auch $Q \not\leqslant P$. Somit ist $PQ > P$, im *Widerspruch* zur Maximalität von P. □

Satz 38 (Sylow) *Sei an die endliche Gruppe* G *und die Primzahl* $p > 0$ *erinnert.*

(1) *Es ist* $\mathrm{Syl}_p(G) \neq \emptyset$.

(2) *Es ist* $\mathrm{Syl}_p(G)$ *eine transitive* G*-Menge unter der Konjugationsoperation.*

(3) *Es ist* $|\mathrm{Syl}_p(G)| \equiv_p 1$.
Für $P \in \mathrm{Syl}_p(G)$ *ist dabei* $|\mathrm{Syl}_p(G)| = |G| / |\mathrm{N}_G(P)|$, *was* $|G|/|G|[p]$ *teilt.*

(4) *Sei* $U \leqslant G$ *eine* p*-Untergruppe. Dann gibt es ein* $P \in \mathrm{Syl}_p(G)$ *mit* $U \leqslant P$.

Beweis. Sei $\Omega_{\max}$ die Menge der maximalen p-Untergruppen von G; cf. Lemma 37. Dank Lemma 37 können wir Lemma 36 verwenden um zu schließen, daß $\Omega_{\max}$ transitiv und $|\Omega_{\max}| \equiv_p 1$ ist.

Wir zeigen $\mathrm{Syl}_p(G) \stackrel{!}{=} \Omega_{\max}$. Zu zeigen ist dazu nur $\mathrm{Syl}_p(G) \supseteq \Omega_{\max}$.

Annahme, es gibt ein $Q \in \Omega_{\max}$ mit $|Q| < |G|[p]$. Sei $N := \mathrm{N}_G(Q)$; cf. Aufgabe 4.(6). Es ist $[G : N] = |\Omega_{\max}| \equiv_p 1$; cf. Lemma 20. Also ist $|N|[p] = |G|[p]$, mithin $[N : Q] \equiv_p 0$. Folglich gibt es in N/Q eine Untergruppe von Ordnung p ; cf. Aufgabe 7.(2). Deren Urbild in N ist eine Untergruppe von G von Ordnung $p \cdot |Q|$, die Q enthält; cf. Aufgabe 17. Dies steht aber im *Widerspruch* zu $Q \in \Omega_{\max}$.

Nun folgt (2) aus $\Omega_{\max}$ transitiv. Es folgt (3) aus $|\Omega_{\max}| \equiv_p 1$ sowie aus Lemma 20 und $P \leqslant \mathrm{N}_G(P)$; cf. Aufgabe 4.(6). Insbesondere folgt (1). Es folgt (4) aus der Konstruktion von $\Omega_{\max}$. ▫

Cf. auch [**7,** Satz 13].

Beispiel 39 Es ist $\mathrm{Syl}_3(\mathrm{S}_4) = \{ \langle (1,2,3) \rangle , \langle (1,2,4) \rangle , \langle (1,3,4) \rangle , \langle (2,3,4) \rangle \}$. Somit ist in der Tat $|\mathrm{Syl}_3(\mathrm{S}_4)| = 4 \equiv_3 1$; cf. Satz 38.(3).

Korollar 40 *Sei $P \in \mathrm{Syl}_p(G)$ gewählt; cf. Satz* 38.(1)*.*

Genau dann ist $P \trianglelefteq G$, wenn $|\mathrm{Syl}_p(G)| = 1$ ist.

Beweis. Ist $P \trianglelefteq G$, dann ist $\mathrm{Syl}_p(G) = \{ {}^gP : g \in G \} = \{P\}$ gemäß Satz 38.(2) und also $|\mathrm{Syl}_p(G)| = 1$.

Ist andererseits $|\mathrm{Syl}_p(G)| = 1$, dann ist $\mathrm{Syl}_p(G) = \{P\}$. Sei $g \in G$. Da $|{}^gP| = |P|$, folgt ${}^gP \in \mathrm{Syl}_p(G) = \{P\}$ und also ${}^gP = P$. Daher ist $P \trianglelefteq G$. ▫

2.2 Normalteilererzeugnis

Bemerkung 41 (und Definition)

Sei G eine Gruppe. Sei $T \subseteq G$. Sei

$$ {}^G\langle\!\langle T \rangle\!\rangle := \bigcap_{T \subseteq N \trianglelefteq G} N \, . $$

das Normalteilererzeugnis *von T in G.*

Es liegt $T \subseteq {}^G\langle\!\langle T \rangle\!\rangle \trianglelefteq G$. Es liegt ${}^G\langle\!\langle T \rangle\!\rangle$ in jedem Normalteiler von G, der T enthält.

Kurz, ${}^G\langle\!\langle T \rangle\!\rangle$ ist initial unter den Normalteilern von G, die T enthalten.

Es ist ${}^G\langle\!\langle T \rangle\!\rangle = \langle \bigcup_{g \in G} {}^gT \rangle$. Also ist jedes Element von ${}^G\langle\!\langle T \rangle\!\rangle$ ein Produkt von Konjugierten von Elementen von T und ihrer Inversen.

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

Nach Konstruktion liegt ${}^G\langle\!|\, T \,|\!\rangle$ in jedem Normalteiler von G, der T enthält.

Wir haben ${}^G\langle\!|\, T \,|\!\rangle \overset{!}{=} \langle \bigcup_{g\in G} {}^gT \rangle$ zu zeigen.

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

Zu $\overset{!}{\geqslant}$. Es ist $T \subseteq {}^G\langle\!|\, T \,|\!\rangle$. Da ${}^G\langle\!|\, T \,|\!\rangle \trianglelefteq G$ ist, ist auch ${}^gT \subseteq {}^G\langle\!|\, T \,|\!\rangle$ für $g \in G$. Da ${}^G\langle\!|\, T \,|\!\rangle \leqslant G$ ist, folgt schließlich $\langle \bigcup_{g\in G} {}^gT \rangle \leqslant {}^G\langle\!|\, T \,|\!\rangle$. ▫

2.3 Einfachheit

2.3.1 Iwasawa

Sei G eine Gruppe.

Definition 42

(1) Ist $1 < G$ und enthält G nur die Normalteiler 1 und G, dann heißt G *einfach*.

(2) Wir erinnern an die Kommutatoruntergruppe $G^{(1)} = \langle [x,y] \,:\, x,\, y \in G \rangle \trianglelefteq G$. Ist $G = G^{(1)}$, so heißt G *perfekt*; cf. Aufgabe 13.

Lemma 43 (Iwasawa-Kriterium)

Sei $M = (M, \alpha)$ eine primitive G-Menge. Sei $m \in M$.

Schreibe $K := \mathrm{Kern}(\alpha)$ und $C := \mathrm{C}_G(m)$.

Sei $A \trianglelefteq C$ mit A abelsch und ${}^G\langle\!|\, A \,|\!\rangle = G$. Dann gelten $(1, 2)$.

(1) *Sei $N \trianglelefteq G$ gegeben mit $N \not\leqslant K$. Dann ist $G^{(1)} \leqslant N$.*

(2) *Ist G perfekt, dann ist G/K einfach.*

Beweis.

Ad (1). Es ist $\bigcap_{g\in G} {}^gC = \bigcap_{g\in G} \mathrm{C}_G(gm) = K$ wegen der Transitivität von M; cf. Bemerkung 18. Aus $N \trianglelefteq G$ und $N \not\leqslant K$ folgt also $N \not\leqslant C$. Da C eine maximale echte Untergruppe von G ist, folgt $G = NC$; cf. Lemma 28, Aufgabe 12.(2).

Sei $g \in G$. Sei $a \in A$. Schreibe $g = nc$ mit $n \in N$ und $c \in C$. Es wird ${}^ga = n(cac^-)n^- = n \cdot {}^{cac^-}n^- \cdot (cac^-) \in NA$. Folglich ist ${}^gA \leqslant NA$.

Es folgt $G = {}^G\langle\!|\, A \,|\!\rangle = \langle \bigcup_{g\in G} {}^gA \rangle \leqslant NA \leqslant G$, also $NA = G$.

Nun ist aber $G/N = NA/N \simeq A/(A \cap N)$ abelsch; cf. Aufgabe 12.(2). Also ist $G^{(1)} \leqslant N$; cf. Aufgabe 13.(4).

Ad (2). Da M nichttrivial und transitiv ist, ist $G/K \neq 1$.

Jeder Normalteiler von G/K ungleich 1 ist von der Form N/K mit $K < N \trianglelefteq G$; cf. Aufgabe 17. Wir haben $N \stackrel{!}{=} G$ zu zeigen.

Wegen G perfekt und wegen (1) ist aber $G = G^{(1)} \leqslant N \trianglelefteq G$, also $N = G$. ▫

2.3.2 Einfachheit von A_n für $n \geqslant 5$

Lemma 44 *Sei $n \geqslant 2$. Es wird A_n von $\{\, \sigma \in \mathrm{A}_n : \sigma \text{ ist 3-Zykel} \,\}$ erzeugt.*

Beweis. Induktion über n. Es ist $\mathrm{A}_2 = 1$.

Sei $n \geqslant 2$. Sei $\rho \in \mathrm{A}_{n+1}$ gegeben. Ist $\rho(n+1) = n+1$, dann ist $\rho \in \mathrm{A}_n$, also Produkt von 3-Zykeln.

Sei $\rho(n+1) \neq n+1$. Wir wählen $\ell \in [1, n+1] \setminus \{n+1, \rho(n+1)\}$, möglich, da $n \geqslant 2$. Dann ist mit $\rho' := (\rho(n+1), n+1, \ell) \circ \rho$ wieder $\rho'(n+1) = n+1$. Also ist $\rho' \in \mathrm{A}_n$ und somit Produkt von 3-Zykeln. Folglich ist auch ρ Produkt von 3-Zykeln. ▫

Lemma 45 *Sei $n \geqslant 5$. Sei $N \trianglelefteq \mathrm{A}_n$. Enthält N einen 3-Zykel, dann ist $N = \mathrm{A}_n$.*

Beweis. Sei $(a, b, c) \in N$ mit a, b, $c \in [1, n]$ mit $|\{a, b, c\}| = 3$. Für $\sigma \in \mathrm{A}_n$ ist ${}^{\sigma}(a, b, c) = (\sigma(a), \sigma(b), \sigma(c))$. Da A_n auf $[1, n]$ dreifach transitiv operiert, liegen alle 3-Zykel in $\mathrm{A}_n^{(1)}$; cf. Aufgabe 5. Also ist $N = \mathrm{A}_n$; cf. Lemma 44. ▫

Lemma 46 *Sei $n \geqslant 5$. Es ist A_n perfekt.*

Beweis. Dank Lemma 45 bleibt also zu zeigen, daß $\mathrm{A}_n^{(1)}$ einen 3-Zykel enthält.

Es ist $[(1,2,3), (3,4,5)] = (1,3,2) \circ (3,5,4) \circ (1,2,3) \circ (3,4,5) = (2,5,3) \in \mathrm{A}_n^{(1)}$. ▫

Lemma 47 *Es ist A_5 einfach.*

Beweis. Es operiert $G := \mathrm{A}_5$ dreifach transitiv und treu auf $[1, 5]$; cf. Aufgabe 5. Also operiert G primitiv auf $[1, 5]$; cf. Bemerkung 15, Lemma 29.

Es ist $\mathrm{A}_4 = \mathrm{C}_G(5) =: C$.

Es ist $A := \langle\, (1,2)(3,4), (1,3)(2,4) \,\rangle = {}^{C}\mathrm{id} \sqcup {}^{C}(1,2)(3,4) \trianglelefteq C$. Es enthält ${}^{G}\langle\!|\, A \,|\!\rangle$ die Elemente $(1,2)(3,4)$, ${}^{(1,2)(4,5)}(1,2)(3,4) = (1,2)(3,5)$ und ${}^{(1,3)(2,5)}(1,3)(2,4) = (1,3)(4,5)$. Also ist ${}^{G}\langle\!|\, A \,|\!\rangle = G$; cf. Aufgabe 14.

Somit folgt die Einfachheit von A_5 aus Lemma 43.(2). ▫

Da wegen Index 5 ohnehin klar ist, daß A_4 eine maximale echte Untergruppe in A_5 ist, wurden die allgemeinen Zusammenhänge für primitive Operationen in Lemma 47 nicht wirklich benötigt und sollen hiermit nur illustriert werden.

Satz 48 (Einfachheit der alternierenden Gruppe)

Es ist A_n *einfach für* $n \geqslant 5$.

Beweis. Induktion über $n \geqslant 5$. Für $n = 5$ ist dies Lemma 47.

Sei $n \geqslant 6$.

Behauptung 1. *Für* $N \lhd \mathrm{A}_n$ *ist* $|N|$ *ein Teiler von* n.

Es ist $N \cap \mathrm{A}_{n-1} \leqslant \mathrm{A}_{n-1}$, dank Induktion also $N \cap \mathrm{A}_{n-1} = 1$ oder $N \cap \mathrm{A}_{n-1} = \mathrm{A}_{n-1}$.

Ist $N \cap \mathrm{A}_{n-1} = \mathrm{A}_{n-1}$, dann enthält N einen 3-Zykel, da $n - 1 \geqslant 3$. Also ist $N = \mathrm{A}_n$; cf. Lemma 45. Dies ist ausgeschlossen.

Ist $N \cap \mathrm{A}_{n-1} = 1$, dann ist

$$\mathrm{A}_{n-1} \;\simeq\; \mathrm{A}_{n-1}/(N \cap \mathrm{A}_{n-1}) \;\simeq\; N\mathrm{A}_{n-1}/N \;\leqslant\; \mathrm{A}_n/N\,;$$

cf. Aufgabe 12.(2). Es folgt, daß $|\mathrm{A}_{n-1}|$ ein Teiler von $[\mathrm{A}_n : N]$ ist. Somit ist $|N|$ ein Teiler von $|\mathrm{A}_n|/|\mathrm{A}_{n-1}| = n$.

Dies zeigt *Behauptung* 1.

Behauptung 2. *Sei* $N \lhd \mathrm{A}_n$. *Dann ist* $N \leqslant M := N \circ {}^{(1,2)}N \lhd \mathrm{A}_n$ *und auch* $M \lhd \mathrm{S}_n$.

Es ist ${}^{(1,2)}N \leqslant {}^{(1,2)}\mathrm{A}_n = \mathrm{A}_n$, denn für $\rho \in N$ und $\xi \in \mathrm{A}_n$ erhalten wir

$${}^{({}^{(1,2)}\xi)}({}^{(1,2)}\rho) \;=\; ({}^{(1,2)}\xi)({}^{(1,2)}\rho)({}^{(1,2)}\xi)^- \;=\; {}^{(1,2)}(\xi\rho\xi^-) \in {}^{(1,2)}N\,.$$

Es ist $M = N \circ {}^{(1,2)}N = {}^{(1,2)}N \circ N \leqslant \mathrm{A}_n$; cf. Aufgabe 12.(2, 3). Es ist

$$\begin{array}{rcl} |M| & = & |N| \cdot |\,{}^{(1,2)}N|/|N \cap {}^{(1,2)}N| \\ & \overset{\text{Beh. 1}}{\leqslant} & n \cdot n \\ & < & n \cdot ((n-1) \cdot 2) \\ & \leqslant & n \cdot ((n-1) \cdot (n-2)) \cdot (n-3)/2 \\ & \leqslant & n!/2 \\ & = & |\mathrm{A}_n|\,; \end{array}$$

cf. Aufgabe 12.(1).

Es bleibt ${}^{\sigma}M \overset{!}{=} M$ zu zeigen für $\sigma \in \mathrm{S}_n$. Falls $\sigma \in \mathrm{A}_n$, ist ${}^{\sigma}M = M$ wegen $M \leqslant \mathrm{A}_n$. Falls $\sigma \in \mathrm{S}_n \smallsetminus \mathrm{A}_n$, dann sei $\sigma' := \sigma \circ (1,2) \in \mathrm{A}_n$, womit dann $\sigma = \sigma' \circ (1,2)$ und also

$${}^{\sigma}M \;=\; {}^{\sigma}(N \circ {}^{(1,2)}N) \;=\; {}^{\sigma'\circ(1,2)}(N \circ {}^{(1,2)}N) \;=\; {}^{\sigma'}({}^{(1,2)}N \circ N) \;=\; {}^{\sigma'}M \;=\; M\,.$$

wird wegen $M \trianglelefteqslant \mathrm{A}_n$. Dies zeigt *Behauptung* 2.

Annahme, es gibt $1 < N \lhd \mathrm{A}_n$. Dank Behauptung 2 ist o.E. auch $N \lhd \mathrm{S}_n$.

Die folgende Fallunterscheidung ist nicht disjunkt.

Fall 1 : Es gibt in N ein Element, welches einen Zykel von einer Länge $k \geqslant 3$ enthält.

Dann gibt es darin auch ein Element ρ, welches den Zykel $(1, 2, 3, \ldots, k)$ enthält. Es wird

$$N \ni [\rho, (1,2)] = [(1,2,3,\ldots,k), (1,2)] = (1,2,3,\ldots,k)^- \circ (2,1,3,\ldots,k) = (1,2,k) ,$$

was mit Lemma 45 zu $N = \mathrm{A}_n$ führte, was aber nicht so ist. Fall 1 tritt also nicht auf.

Fall 2 : Es gibt ein Element in N, das aus zwei Transpositionen besteht.

Dann liegen auch $(1,2)(3,4)$ und $(1,2)(3,5)$ in N. Es folgt

$$N \ni [(1,2)(3,4), (1,2)(3,5)] = [(3,4), (3,5)] = (3,4,5) ,$$

und wir sind in Fall 1, welcher nicht auftritt. Also tritt auch Fall 2 nicht auf.

Fall 3 : Es gibt es ein Element in N, dessen Zykeldarstellung mindestens drei Transpositionen aufweist.

Also gibt es darin auch ein Element ρ, welches $(1,2)(3,4)(5,6)$ enthält. Dann ist

$$N \ni [(2,4,6), \rho] = [(2,4,6), (1,2)(3,4)(5,6)] = (1,3,5)(2,6,4) ,$$

und wir sind in Fall 1, welcher nicht auftritt. Also tritt auch Fall 3 nicht auf.

Wir haben einen *Widerspruch.* ▫

2.3.3 Einfachheit von $\mathrm{PSL}_n(F)$ für $(n, |F|) \notin \{ (2,2), (2,3) \}$

Satz 49 (Einfachheit der projektiven speziellen Gruppe)

Sei F ein Körper. Sei $n \geqslant 2$. Sei $(n, |F|) \notin \{ (2,2), (2,3) \}$.

Wir erinnern an $\mathrm{PSL}_n(F) = \mathrm{SL}_n(F)/\mathrm{Z}(\mathrm{SL}_n(F))$.

Es ist $\mathrm{PSL}_n(F)$ *einfach.*

Beweis. Es ist $G := \mathrm{SL}_n(F)$ perfekt; cf. Aufgabe 18.

Es ist $M := \mathrm{P}^{n-1}(F)$ eine primitive G-Menge; cf. Beispiel 31.

Sei $m := \overline{\mathrm{e}_1} = \overline{\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}} \in M$. Sei $C := \mathrm{C}_G(m) = \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \leqslant \mathrm{SL}_n(F)$.

Wir haben den Gruppenmorphismus $C \longrightarrow \mathrm{GL}_{n-1}(F)$, $(x_{i,j})_{i,j\in[1,n]} \longmapsto (x_{i,j})_{i,j\in[2,n]}$.

Sei $A := \left(\begin{smallmatrix} 1 & * \\ 0 & \mathrm{E}_{n-1} \end{smallmatrix}\right) \trianglelefteqslant C$ sein Kern. Es ist A abelsch.

Es ist ${}^{G}\langle\!\langle\, A \,\rangle\!\rangle = G$; cf. Aufgabe 18.(3).

Es ist der Kern K der Operation von G auf M gleich $\mathrm{Z}(G)$; cf. Aufgabe 11.(5).

Also zeigt Lemma 43.(2), daß $G/K = \mathrm{PSL}_n(F)$ einfach ist. ▫

2.4 Präsentationen

2.4.1 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 $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$ 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.

Es ist $uvw := (uv)w = u(vw)$ für $u,\ v,\ w \in \mathrm{F}_0(X)$.

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 $ux^{\varepsilon}x^{-\varepsilon}v \rightsquigarrow uv$ ist.

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 $u = v$ ist.

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 $n = 4$,

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

ist. 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 50 *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 51 (und Definition)

Zusammen mit der Multiplikation von Bemerkung 50 *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. Wir verwenden Aufgabe 1.

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 $[u][\emptyset] = [u\emptyset] = [u]$ für $u \in \mathrm{F}_0(X)$.

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

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

sodaß $[u][v] = [uv] = [\emptyset] = 1$ ist. ▫

Lemma 52 (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 $\hat{f} \circ \iota = f$.

$$\begin{array}{ccc} \mathrm{F}(X) & \overset{\exists! \hat{f}}{\dashrightarrow} & G \\ {\scriptstyle \iota}\uparrow & \nearrow_{f} & \\ X & & \end{array}$$

Hierbei ist

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

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 51. Also ist

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

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

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

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 $\hat{f} : \mathrm{F}(X) \longrightarrow G$, $[u] \longmapsto \tilde{f}(u)$ als Abbildung wohldefiniert ist.

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

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

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

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

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

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

□

Notation 53 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 $[x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}] = [x_1^{\varepsilon_1}] \cdot \ldots \cdot [x_n^{\varepsilon_n}] = x_1^{\varepsilon_1} \cdot \ldots \cdot x_n^{\varepsilon_n}$, wobei $n \in \mathbf{Z}_{\geqslant 0}$, $x_i \in X$ und $\varepsilon_i \in \{-1,+1\}$ für $i \in [1,n]$.

2.4.2 Endliche Präsentationen via Erzeuger und Relationen

Notation 54 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

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

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 *endlich präsentiert.*

Nach Konstruktion ist das Bild einer Relation r_j in $\langle\, x_1\,,\ldots,x_n\,:\,r_1\,,\ldots,\,r_m\,\rangle$ unter der Restklassenabbildung von $\mathrm{F}(X)$ nach $\langle\, x_1\,,\ldots,x_n\,:\,r_1\,,\ldots,\,r_m\,\rangle$ gleich 1.

Unter Mißbrauch von Notation schreiben wir für $i \in [1,n]$ das Bild eines Elements x_i unter dieser Restklassenabbildung wieder

$$x_i \;:=\; x_i{}^{\mathrm{F}(X)}\langle\!\langle\, \{r_1\,,\ldots,r_m\}\,\rangle\!\rangle \;\overset{\text{N. 53}}{=}\; [x_i^{+1}]^{\mathrm{F}(X)}\langle\!\langle\, \{r_1\,,\ldots,r_m\}\,\rangle\!\rangle\ .$$

Die beiden Surjektionen

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

zeigen, daß in dieser Notation jedes Element in $\langle\, x_1\,,\ldots,x_n\,:\,r_1\,,\ldots,\,r_m\,\rangle$ von der Form $x_{i_1}^{\varepsilon_1}\cdot\ldots\cdot x_{i_k}^{\varepsilon_k}$ 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 55 (Universelle Eigenschaft einer endlich präsentierten Gruppe)

Wir befinden uns weiterhin in der Situation von Notation 54.

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

Wir erinnern daran, daß der Gruppenmorphismus $\hat{f} : \mathrm{F}(X) \longrightarrow G$ ein Element

$$y \;=\; x_{i_1}^{\varepsilon_1}\cdot\ldots\cdot x_{i_k}^{\varepsilon_k}$$

für $k \in \mathbf{Z}_{\geqslant 0}$ und $i_j \in [1,n]$, $\varepsilon_j \in \{-1,+1\}$ für $j \in [1,k]$ auf

$$\hat{f}(y) \;=\; f(x_{i_1})^{\varepsilon_1}\cdot\ldots\cdot f(x_{i_k})^{\varepsilon_k}$$

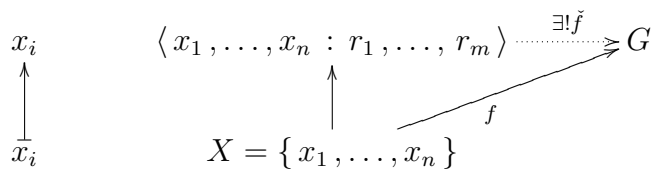
schickt; cf. Lemma 52.

Sei an f dazuhin

$$\hat{f}(r_j) \;=\; 1_G \qquad \text{für } \; j \in [1,m]$$

vorausgesetzt.

Dann gibt es genau einen Gruppenmorphismus $\check{f} : \langle\, x_1\,,\ldots,x_n\,:\,r_1\,,\ldots,\,r_m\,\rangle \longrightarrow G$ mit $\check{f}(x_i) = f(x_i)$ 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

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

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 52. Nach Voraussetzung ist $\hat{f}(r_j) = 1$ für $j \in [1,m]$, i.e. $\{r_1\,, \ldots, r_m\} \subseteq \mathrm{Kern}(\hat{f}) \trianglelefteq \mathrm{F}(X)$. Also ist ${}^{\mathrm{F}(X)}\langle\!\langle\, \{r_1\,, \ldots, r_m\}\,\rangle\!\rangle \leqslant \mathrm{Kern}(\hat{f})$; cf. Bemerkung 41.

Somit ist der Gruppenmorphismus

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

wohldefiniert. Er schickt x_i nach $\hat{f}(x_i) = \hat{f}([x_i^{+1}]) = f(x_i)$ für $i \in [1,n]$. ▫

Beispiel 56 Sei $\mathrm{D}_8 := \langle\, a,\, b \;:\; a^4,\, b^2,\, (ba)^2\,\rangle$.

In D_8 ist jedes Element von der Form $a^{i_1}b^{j_1} \cdot \ldots \cdot a^{i_\ell}b^{j_\ell}$, wobei $\ell \geqslant 0$ und $i_k\,,\, j_k \in \mathbf{Z}$ für $k \in [1,\ell]$.

Dabei ist o.E. $i_k \in [0,3]$ und $j_k \in [0,1]$ für $k \in [1,\ell]$. Denn aus $a^4 = 1$ folgt $a^- = a^3$, und aus $b^2 = 1$ folgt $b^- = b$.

Ferner ist $baba = 1$, und also auch $ba = a^-b = a^3b$.

Somit ist in D_8 jedes Element von der Form a^ib^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 $ba = a^3b$ die Faktoren b nach rechts tauschen; e.g. wird $baabab = a^3babab = a^3a^3bbab = a^2 1ab = a^3b$. Insbesondere ist $|\mathrm{D}_8| \leqslant 8$. Vorsicht, bislang wissen wir nur, daß wegen $a^4 = 1$ die Ordnung $|\langle a\rangle|$ ein Teiler von 4 ist. Genauso wissen wir bislang nur, daß $|\langle b\rangle|$ ein Teiler von 2 ist.

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

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

Also gibt Satz 55 den 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 34. 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 $j = \tilde{j}$. Insbesondere ist $|\langle a\rangle| = 4$ und $|\langle b\rangle| = 2$.

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

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

Beispiel 57 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 gibt Satz 55 den 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 ${}^{a^ib^j}b = {}^{a^i}b = a^iba^{-i} = a^{2i}b \neq ab$ für alle $i \in [0,3]$ und $j \in [0,1]$. Also ist $\check{u}$ nicht inner.

Beispiel 58 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 22.

2.4.3 Bahnenalgorithmus für Relationen

Bemerkung 59 *Seien F und G Gruppen. Sei $\varphi : F \longrightarrow G$ ein Gruppenmorphismus.*

Es ist G eine G-Menge via Linksmultiplikation. Durch Einschränkung entlang φ wird G zu einer F-Menge. Cf. Beispiel 2. Für diese ist

$$\mathrm{C}_F(1_G) \;=\; \mathrm{Kern}(\varphi)\,.$$

Beweis. Sei $f \in F$ gegeben. Es ist $f \in \mathrm{C}_F(1_G)$ genau dann, wenn $1_G = f \cdot 1_G = \varphi(f) \cdot 1_G = \varphi(f)$ ist, i.e. wenn $f \in \mathrm{Kern}(\varphi)$ ist. ▫

Algorithmus 60 Sei G eine endliche Gruppe.

Sei $n \geqslant 0$ und $\{\, g_i \,:\, i \in [1,n] \,\}$ mit $G = \langle\, g_i \,:\, i \in [1,n] \,\rangle$.

Sei $\{\, \hat{g}_i \,:\, i \in [1,n] \,\}$ eine Menge mit $\hat{g}_i \neq \hat{g}_j$ für $i,\, j \in [1,n]$ mit $i \neq j$.

Wir verfügen dank universeller Eigenschaft einer freien Gruppe, cf. Lemma 52, über den surjektiven Gruppenmorphismus

$$\begin{array}{rcll} F \;:=\; \mathrm{F}(\{\, \hat{g}_i \,:\, i \in [1,n] \,\}) & \xrightarrow{\varphi} & G & \\ \hat{g}_i & \longmapsto & g_i & \text{für } i \in [1,n]\,. \end{array}$$

Betrachte G als G-Menge via Multiplikation; cf. Beispiel 2.(3). Durch Einschränkung entlang φ wird G dann zu einer F-Menge; cf. Beispiel 2.(2).

Bestimme mittels Bahnenalgorithmus, Algorithmus 33, ein $m \geqslant 0$ und eine endliche Teilmenge $\{\, k_j \,:\, j \in [1,m] \,\} \subseteq \mathrm{C}_F(1_G) \overset{\text{B.59}}{=} \mathrm{Kern}(\varphi)$ mit

$$\mathrm{Kern}(\varphi) \;=\; \langle\, k_j \,:\, j \in [1,m] \,\rangle\,.$$

Dann ist insbesondere

$$\mathrm{Kern}(\varphi) \;=\; {}^{F}\langle\!|\, k_j \,:\, j \in [1,m] \,|\!\rangle\,.$$

Somit erhalten wir den Isomorphismus

$$\begin{array}{rcll} \langle\, \hat{g}_1, \ldots, \hat{g}_n \,:\, k_1, \ldots, k_m \,\rangle & \xrightarrow[\sim]{\bar{\varphi}} & G & \\ \hat{g}_i \,\mathrm{Kern}(\varphi) & \longmapsto & g_i & \text{für } i \in [1,n]\,. \end{array}$$

Oft kann die in Algorithmus 60 gefundene Liste von Relationen noch mittels folgender Bemerkung 61 reduziert werden.

Bemerkung 61 *Sei F eine Gruppe. Sei $X \subseteq F$. Seien $y, z \in F$. Sei*

$$ {}^{f}y\,{}^{F}\langle\!|\, X \,|\!\rangle \;=\; z\,{}^{F}\langle\!|\, X \,|\!\rangle \;. $$

für ein $f \in F$. Dann ist

$$ {}^{F}\langle\!|\, X \cup \{y\} \,|\!\rangle \;=\; {}^{F}\langle\!|\, X \cup \{z\} \,|\!\rangle \;. $$

Ist $z = 1$, dann ist insbesondere

$$ {}^{F}\langle\!|\, X \cup \{y\} \,|\!\rangle \;=\; {}^{F}\langle\!|\, X \,|\!\rangle \;. $$

Beweis. Es genügt, ${}^{F}\langle\!|\, X \cup \{y\} \,|\!\rangle \overset{!}{\subseteq} {}^{F}\langle\!|\, X \cup \{z\} \,|\!\rangle$ zu zeigen.

Schreibe $N := {}^{F}\langle\!|\, X \cup \{z\} \,|\!\rangle \trianglelefteqslant F$. Wir haben $X \cup \{y\} \overset{!}{\subseteq} N$ zu zeigen.

Es genügt, $y \overset{!}{\in} N$ zu zeigen.

Es ist $y = f^{-}ztf$ für ein $t \in {}^{F}\langle\!|\, X \,|\!\rangle \leqslant N$. Da $z \in N$ liegt, folgt $zt \in N$ und also $y \in N$. ▫

Beispiel 62 Betrachte $G := \langle (1,2,3,4), (1,3) \rangle \leqslant \mathrm{S}_4$.

Wir kennen schon aus Beispiel 56 den Isomorphismus

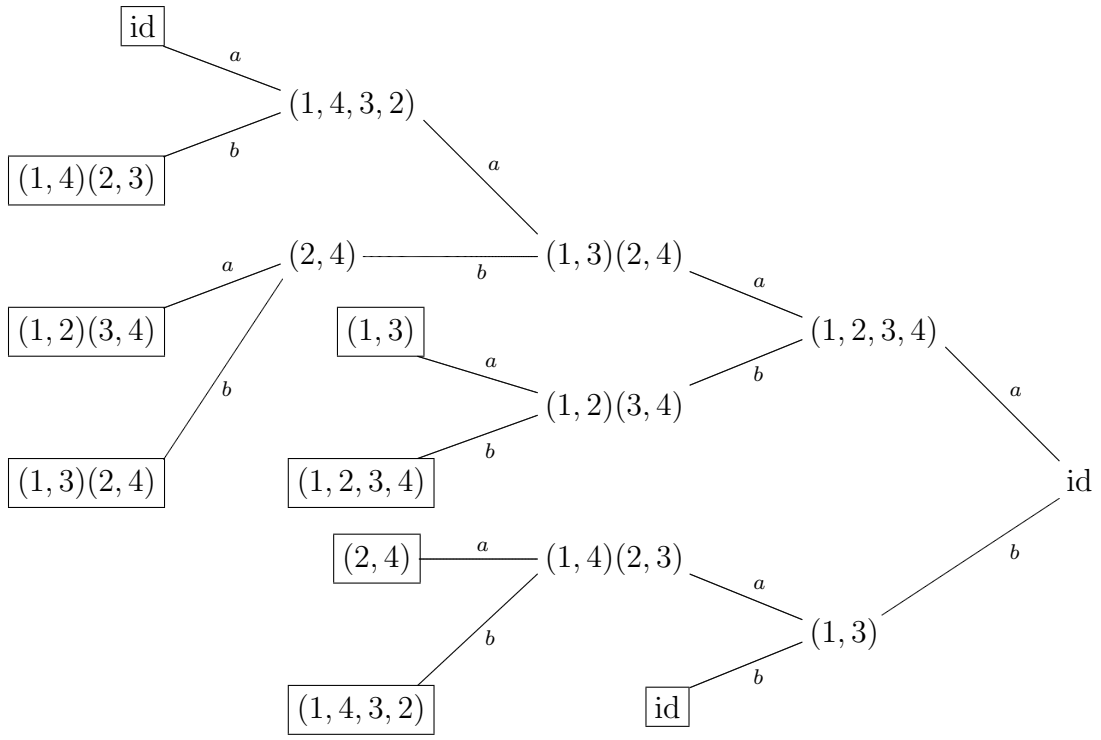
$$ \mathrm{D}_8 \;=\; \langle\, a, b \,:\, a^4,\, b^2,\, (ba)^2 \,\rangle \;\xrightarrow{\sim}\; G \;, \quad a \longmapsto (1,2,3,4) \;, \quad b \longmapsto (1,3) \;. $$

Wir wollen diesen abermals herleiten, diesesmal unter Verwendung von Algorithmus 60.

Wir haben den surjektiven Gruppenmorphismus

$$ \begin{array}{rcl} F \;:=\; \mathrm{F}(\{a,b\}) & \xrightarrow{\varphi} & G \\ a & \longmapsto & (1,2,3,4) \\ b & \longmapsto & (1,3) \;, \end{array} $$

vermöge dessen G zu einer F-Menge wird. Zur Berechnung von $\mathrm{C}_F(1_G) = \mathrm{C}_F(\mathrm{id})$ erstellen wir folgenden Baum.



Die markierten Stellen, von oben nach unten gelesen und von rechts nach links, liefern die folgenden Relationen.

$$b^2\ ,\ \ b^-aba\ ,\ \ a^-b^2a\ ,\ \ (ba^2)^-a^2b\ ,\ \ a^{-3}(bab)\ ,\ \ a^4\ ,\ \ (ab)^-ba^3\ ,\ \ (ba)^-aba^2\ ,\ \ a^{-2}b^2a^2$$

Nun wenden wir Bemerkung 61 an.

All diese Relationen außer b^2 und a^4 modulo dem von a^4 und b^2 erzeugten Normalteiler vereinfacht, ergibt folgende Liste von Relationen.

$$b^2\ ,\ \ baba\ ,\ \ a^2ba^2b\ ,\ \ abab\ ,\ \ a^4\ ,\ \ ba^3ba^3\ ,\ \ a^3baba^2$$

All diese Relationen außer b^2, a^4, $(ba)^2$ modulo dem von b^2, a^4, $(ba)^2$ erzeugten Normalteiler vereinfacht, ergibt folgende Liste von Relationen.

$$b^2\ ,\ \ baba\ ,\ \ a^4$$

Somit ist in der Tat

$$\begin{array}{rcccl} \mathrm{D}_8 & = & \langle\, a, b \,:\, a^4,\ b^2,\ (ba)^2 \,\rangle & \xrightarrow[\sim]{\bar{\varphi}} & G \\ & & & a & \longmapsto & (1,2,3,4) \\ & & & b & \longmapsto & (1,3) \end{array}$$

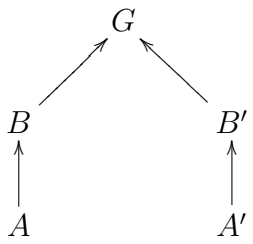
Kapitel 3

Erweiterungen

3.1 Jordan-Hölder

Sei G eine Gruppe.

Lemma 63 (Schmetterlingslemma)
Sei $A \trianglelefteq B \leqslant G$. Sei $A' \trianglelefteq B' \leqslant G$.



Dann ist

$$\begin{array}{rcl}(A\cap B')(B\cap A') & \trianglelefteq & B\cap B' \\ A(B\cap A') & \trianglelefteq & A(B\cap B') \\ (A\cap B')A' & \trianglelefteq & (B\cap B')A' \,.\end{array}$$

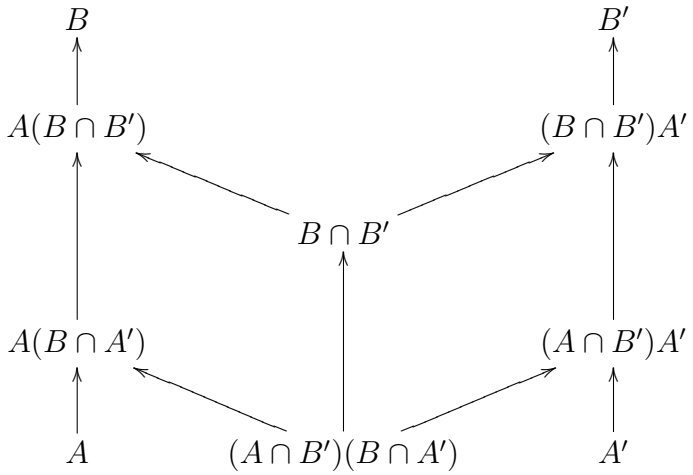
Wir haben die folgenden Isomorphismen.

$$\begin{array}{rcl}\big(B\cap B'\big)/\big((A\cap B')(B\cap A')\big) & \xrightarrow[\sim]{\varphi} & \big(A(B\cap B')\big)/\big(A(B\cap A')\big) \\ x\big((A\cap B')(B\cap A')\big) & \longmapsto & x\big(A(B\cap A')\big)\end{array}$$

$$\begin{array}{rcl}\big(B\cap B'\big)/\big((A\cap B')(B\cap A')\big) & \xrightarrow[\sim]{\varphi'} & \big((B\cap B')A'\big)/\big((A\cap B')A'\big) \\ x\big((A\cap B')(B\cap A')\big) & \longmapsto & x\big((A\cap B')A'\big)\end{array}$$

Insbesondere ist

$$\big(A(B\cap B')\big)/\big(A(B\cap A')\big) \;\simeq\; \big((B\cap B')A'\big)/\big((A\cap B')A'\big)\,.$$



Beweis. Wegen $A \trianglelefteqslant B$ ist $A \cap B' \trianglelefteqslant B \cap B'$. Dito ist $B \cap A' \trianglelefteqslant B \cap B'$. Insgesamt ist also $(A \cap B')(B \cap A') \trianglelefteqslant B \cap B'$; cf. Aufgabe 12.(3).

Wegen $A \trianglelefteqslant B$ und $B \cap A' \trianglelefteqslant B \cap B' \leqslant B$ ist $A(B \cap A') \leqslant A(B \cap B') \leqslant B$; cf. Aufgabe 12.(2). Ist $a \in A$, $y \in B \cap B'$ und ist $\tilde{a} \in A$ und $x \in B \cap A'$, dann ist ${}^{(ay)}(\tilde{a}x) = {}^{ay}\tilde{a} \cdot {}^{ay}x \in A(B \cap A')$, da ${}^{ay}\tilde{a} \in A$ wegen $A \trianglelefteqslant B$ und da $z := {}^{y}x \in B \cap A'$ und mithin ${}^{ay}x = aza^{-} = a({}^{z}a)^{-}z \in A(B \cap A')$ wegen $A \trianglelefteqslant B$. Also ist $A(B \cap A') \trianglelefteqslant A(B \cap B')$.

Es genügt, den Isomorphismus φ zu zeigen.

Wohldefiniertheit. Es ist $(A \cap B')(B \cap A') \leqslant A(B \cap A')$.

Injektivität. Sei $x \in B \cap B'$ mit $x\big(A(B \cap A')\big) = 1$ gegeben. Dann ist $x = ay$ mit $a \in A$ und $y \in B \cap A'$. Es ist $a = xy^{-} \in B'$, insgesamt also $a \in A \cap B'$. Also ist $x\big((A \cap B')(B \cap A')\big) = 1$.

Surjektivität. Sei $y \in A(B \cap B') = (B \cap B')A$ gegeben; cf. Aufgabe 12.(2). Schreibe $y = xa$ mit $x \in B \cap B'$ und $a \in A$. Dann ist $y\big(A(B \cap A')\big) = xa\big(A(B \cap A')\big) = x\big(A(B \cap A')\big)$. ▫

Definition 64 Eine *Subnormalreihe* von G ist ein Tupel von Untergruppen $(U_i)_{i \in [0,s]}$ von G für ein $s \geqslant 0$, für welches $G = U_0$ und $U_i \trianglerighteqslant U_{i+1}$ für $i \in [0, s-1]$ und $U_s = 1$ gilt.

$$G \;=\; U_0 \;\trianglerighteqslant\; U_1 \;\trianglerighteqslant\; \ldots \;\trianglerighteqslant\; U_{s-1} \;\trianglerighteqslant\; U_s \;=\; 1$$

Die Faktorgruppen U_i/U_{i+1} für $i \in [0, s-1]$ heißen *Subfaktoren* dieser Subnormalreihe.

Definition 65 Seien $(U_i)_{i \in [0,s]}$ und $(V_j)_{j \in [0,t]}$ Subnormalreihen von G.

(1) Die Subnormalreihe $(U_i)_{i \in [0,s]}$ heißt *strikt,* wenn $U_i \triangleright U_{i+1}$ ist für $i \in [0, s-1]$.

(2) Die Subnormalreihe $(U_i)_{i \in [0,s]}$ heißt *Kompositionsreihe* von G, wenn U_i/U_{i+1} eine einfache Gruppe ist für $i \in [0, s-1]$. Die Subfaktoren einer Kompositionsreihe heißen auch *Kompositionsfaktoren.*

(3) Es heißt $(V_j)_{j\in[0,t]}$ *Verfeinerung* von $(U_i)_{i\in[0,s]}$, geschrieben $(U_i)_{i\in[0,s]} \preccurlyeq (V_j)_{j\in[0,t]}$, wenn es eine injektive monotone Abbildung $\rho : [0,s] \longrightarrow [0,t]$ gibt mit $\rho(0) = 0$, $\rho(s) = t$ und $U_i = V_{\rho(i)}$ für $i \in [0,s]$. Sei $(\prec) := (\preccurlyeq) \smallsetminus (=)$.

(4) Die Subnormalreihen $(U_i)_{i\in[0,s]}$ und $(V_j)_{j\in[0,t]}$ heißen *äquivalent,* wenn es eine bijektive Abbildung $\sigma : [0,s-1] \longrightarrow [0,t-1]$ gibt mit

$$U_i/U_{i+1} \;\simeq\; V_{\sigma(i)}/V_{\sigma(i)+1}$$

für $i \in [0,s-1]$.

(5) Sei $\alpha : [0,\check{s}] \longrightarrow [0,s]$ die injektive monotone Abbildung mit Bild

$$\{\, i \in [0,s-1] \,:\, U_i > U_{i+1} \,\} \cup \{s\} \;.$$

Es ist $(U_{\alpha(j)})_{j\in[1,\check{s}]}$ eine Subnormalreihe von G, genannt die *Striktifizierung* von $(U_i)_{i\in[0,s]}$. Dabei ist $\{\, U_{\alpha(j)} \,:\, j \in [1,\check{s}] \,\} = \{\, U_i \,:\, i \in [0,s] \,\}$.

Beispiel 66

(1) Es ist $(\,\mathrm{S}_3\,,\,\mathrm{A}_3\,,\,1\,)$ eine Kompositionsreihe von S_3.

(2) Betrachte $\mathrm{D}_8 = \langle\, a,\, b \,:\, a^4,\, b^2,\, (ba)^2 \,\rangle$; cf. Beispiel 56. Es sind $(\mathrm{D}_8\,,\,\langle a\rangle, \langle a^2\rangle, 1)$ und $(\mathrm{D}_8\,,\,\langle a^2, b\rangle, \langle a^2\rangle, 1)$ Kompositionsreihen von D_8. Beachte $\langle a\rangle \not\preccurlyeq \langle a^2, b\rangle$.

(3) Es ist

$$(\,\mathrm{S}_4\,,\,\mathrm{A}_4\,,\,\langle\,(1,2)(3,4)\,,\,(1,3)(2,4)\,\rangle\,,\,\langle(1,2)(3,4)\rangle\,,\,1\,)$$

eine Kompositionsreihe von S_4. Denn es ist sogar $\langle\,(1,2)(3,4)\,,\,(1,3)(2,4)\,\rangle = \{\,\mathrm{id}\,,\;(1,2)(3,4)\,,\,(1,3)(2,4)\,,\,(1,4)(2,3)\,\} \trianglelefteq \mathrm{S}_4$. Diese Kompositionsreihe ist also eine Verfeinerung der Subnormalreihe

$$(\,\mathrm{S}_4\,,\,\langle\,(1,2)(3,4)\,,\,(1,3)(2,4)\,\rangle\,,\,1\,)$$

(4) Sei $n \geqslant 5$. Es ist $(\,\mathrm{S}_n\,,\,\mathrm{A}_n\,,\,1\,)$ eine Kompositionsreihe von S_n. Cf. Satz 48.

(5) Es ist

$$(\;\mathrm{GL}_3(\mathbf{F}_7)\;,\;\langle \mathrm{SL}_3(\mathbf{F}_7), \left(\begin{smallmatrix}-1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right)\rangle\;,\;\mathrm{SL}_3(\mathbf{F}_7)\;,\;\langle\left(\begin{smallmatrix}4&0&0\\0&4&0\\0&0&4\end{smallmatrix}\right)\rangle\;)$$

eine Kompositionsreihe von $\mathrm{GL}_3(\mathbf{F}_7)$; cf. Satz 49. Darin treten, bis auf Isomorphie, die Kompositionsfaktoren C_3, C_2, $\mathrm{PSL}_3(\mathbf{F}_7)$, C_3 auf.

Bemerkung 67 *Die Menge der strikten Subnormalreihen von G, zusammen mit $(\preccurlyeq)$, ist teilgeordnet. Eine Subnormalreihe darin ist genau dann maximal, wenn sie eine Kompositionsreihe ist.*

Beweis. Es ist $(\preccurlyeq)$ reflexiv dank Identität und transitiv, da das Kompositum injektiver Abbildungen injektiv ist. Sie ist identitiv, da eine injektive monotone Abbildung von $[0,s]$ nach $[0,s]$ bereits die Identität ist.

Sei $(U_i)_{i\in[0,s]}$ eine strikte Subnormalreihe von G.

Sei $(U_i)_{i\in[0,s]}$ maximal. *Angenommen,* es ist $(U_i)_{i\in[0,s]}$ keine Kompositionsreihe. Dann gibt es ein $i \in [0,s-1]$ mit U_i/U_{i+1} nicht einfach. Sei $1 < N/U_{i+1} \lhd U_i/U_{i+1}$, wobei $U_{i+1} \lhd N \lhd U_i$; cf. Aufgabe 17.(3). Sei

$$V_j := \begin{cases} U_j & \text{falls } j \in [0,i] \\ N & \text{falls } j = i+1 \\ U_{j-1} & \text{falls } j \in [i+2, s+1] \,. \end{cases}$$

Dann ist $(V_j)_{j\in[0,s+1]}$ eine Subnormalreihe. Via $\rho : [0,s] \longrightarrow [0,s+1]$, $k \longmapsto k + \partial_{k\geqslant i+1}$ erkennen wir $(U_i)_{i\in[0,s]} \prec (V_j)_{j\in[0,s+1]}$, im *Widerspruch* zur Maximalität von $(U_i)_{i\in[0,s]}$.

Sei $(U_i)_{i\in[0,s]}$ eine Kompositionsreihe. *Angenommen,* sie sei nicht maximal.

Sei $(U_i)_{i\in[0,s]} \prec (V_j)_{j\in[0,t]}$. Wähle eine dies belegende injektive Abbildung $\rho : [0,s] \longrightarrow [0,t]$. Diese ist nicht surjektiv, da sie diesenfalls gleich $\mathrm{id}_{[0,s]}$ wäre, was wegen $(U_i)_{i\in[0,s]} \neq (V_j)_{j\in[0,t]}$ nicht möglich ist. Sei $j \in [0,t]$ nicht im Bild von ρ. Dann gibt es genau ein $i \in [0,s]$ mit $\rho(i) < j < \rho(i+1)$. Es folgt $U_i = V_{\rho(i)} > V_j > V_{\rho(i+1)} = U_{i+1}$, wobei $U_i \triangleright U_{i+1}$ und $U_i \triangleright V_i \triangleright U_{i+1}$. Also ist $1 \neq V_i/U_{i+1} \lhd U_i/U_{i+1}$, somit U_i/U_{i+1} nicht einfach, und wir haben einen *Widerspruch.* ▫

Beispiel 68 Ist G endlich, dann ist auch die Menge der Subnormalreihen von G endlich. Also liegt jedes Element dieser Menge unter einem $(\prec)$-maximalen. Da es eine strikte Subnormalreihe von G gibt, viz. $(G,1)$ falls $G \neq 1$ resp. (1) falls $G = 1$, hat G also wenigstens eine Kompositionsreihe.

Dagegen hat e.g. $\mathbf{Z} = (\mathbf{Z}, +)$ keine Kompositionsreihe, da $\mathbf{Z}$ keine einfache Untergruppe hat.

Bemerkung 69 *Äquivalente Subnormalreihen von G haben äquivalente Striktifizierungen.*

Beweis. Seien $(U_i)_{i\in[0,s]}$ und $(V_j)_{j\in[0,t]}$ äquivalente Subnormalreihen von G.

Sei $\alpha : [0, \check{s}-1] \longrightarrow [0,s-1]$ injektiv, monoton und mit Bild $\{\, i \in [0,s-1] \,:\, U_i > U_{i+1} \,\}$.

Sei $\beta : [0, \check{t}-1] \longrightarrow [0,t-1]$ injektiv, monoton und mit Bild $\{\, j \in [0,t-1] \,:\, V_j > V_{j+1} \,\}$.

Sei $\sigma : [0,s-1] \longrightarrow [0,t-1]$ eine Bijektion mit $U_i/U_{i+1} \simeq V_{\sigma(i)}/V_{\sigma(i)+1}$ für $i \in [0,s-1]$.

Für $i \in [0,s-1]$ ist $U_i = U_{i+1}$ genau dann, wenn $V_{\sigma(i)} = V_{\sigma(i)+1}$ ist. Also schränkt σ ein zu einer Bijektion $\tilde{\sigma}$ von $\{\, i \in [0,s-1] \,:\, U_i > U_{i+1} \,\}$ nach $\{\, j \in [0,t-1] \,:\, V_j > V_{j+1} \,\}$.

Somit gibt es eine Bijektion $\check{\sigma} : [0, \check{s}-1] \longrightarrow [0, \check{t}-1]$ mit $\beta \circ \check{\sigma} = \sigma \circ \alpha$.

$$\begin{array}{ccc} [0, s-1] & \xrightarrow{\sigma} & [0, t-1] \\ {\scriptstyle\alpha}\uparrow & & \uparrow{\scriptstyle\beta} \\ [0, \check{s}-1] & \xrightarrow{\check{\sigma}} & [0, \check{t}-1] \end{array}$$

Für $k \in [0, \check{s}-1]$ wird $U_{\alpha(k+1)} = U_{\alpha(k)+1}$ und also

$$\begin{array}{rcl} U_{\alpha(k)}/U_{\alpha(k+1)} & = & U_{\alpha(k)}/U_{\alpha(k)+1} \\ & \simeq & V_{\sigma(\alpha(k))}/V_{\sigma(\alpha(k))+1} \\ & = & V_{\beta(\check{\sigma}(k))}/V_{\beta(\check{\sigma}(k))+1} \\ & = & V_{\beta(\check{\sigma}(k))}/V_{\beta(\check{\sigma}(k)+1)} \ . \end{array}$$

Folglich sind die Striktifizierungen $(U_{\alpha(k)})_{k\in[0,\check{s}]}$ und $(V_{\beta(\ell)})_{\ell\in[0,\check{t}]}$ äquivalent. ▫

Bemerkung 70 *Seien $(U_i)_{i\in[0,s]}$ und $(V_j)_{j\in[0,t]}$ Subnormalreihen von G.*
Betrachte die folgenden Aussagen.

(1) *Es ist $(V_j)_{j\in[0,t]}$ eine Verfeinerung von $(U_i)_{i\in[0,s]}$.*

(2) *Es ist $\{ U_i \,:\, i \in [0,s] \} \subseteq \{ V_j \,:\, j \in [0,t] \}$.*

Es ist (1) $\Rightarrow$ (2).
Ist $(U_i)_{i\in[0,s]}$ strikt, dann ist (1) $\Leftrightarrow$ (2).

Beweis. Gibt eine injektive monotone Abbildung $\rho : [0,s] \longrightarrow [0,t]$ mit $\rho(0) = 0$, $\rho(s) = t$ und $U_i = V_{\rho(i)}$ für $i \in [0,s]$, dann ist $U_i \in \{ V_j \,:\, j \in [0,t] \}$ für $i \in [0,s]$.

Sei nun $(U_i)_{i\in[0,s]}$ strikt und $\{ U_i \,:\, i \in [0,s] \} \subseteq \{ V_j \,:\, j \in [0,t] \}$. Dann können wir für $i \in [0,s]$ den Wert $\rho(i) \in [0,t]$ wählen mit $U_i =: V_{\rho(i)}$, wobei insbesondere $\rho(0) := 0$ und $\rho(s) := s$. Da $(U_i)_{i\in[0,s]}$ strikt ist, wird ρ monoton und injektiv. ▫

Lemma 71 (Schreier) *Seien $(U_i)_{i\in[0,s]}$ und $(V_j)_{j\in[0,t]}$ Subnormalreihen von G.*

(1) *Es gibt eine Verfeinerung $(U'_k)_{k\in[0,st]}$ von $(U_i)_{i\in[0,s]}$ und eine Verfeinerung $(V'_\ell)_{\ell\in[0,st]}$ von $(V_j)_{j\in[0,t]}$ derart, daß $(U'_k)_{k\in[0,st]}$ und $(V'_\ell)_{\ell\in[0,st]}$ äquivalent sind.*

Kurz, zwei Subnormalreihen von G haben äquivalente Verfeinerungen.

(2) *Sind $(U_i)_{i\in[0,s]}$ und $(V_j)_{j\in[0,t]}$ strikt, so haben sie äquivalente Verfeinerungen, die strikte Subnormalreihen sind.*

Beweis. O.E. ist $G \neq 1$.

Ad (1). Betrachte folgende Abbildungen.

Die Bijektion $\varphi : [0, st-1] \longrightarrow [0, s-1] \times [0, t-1]$, $k \longmapsto (\varphi_1(k), \varphi_2(k))$ mit $k = t\varphi_1(k) + \varphi_2(k)$.

Die Bijektion $\psi : [0, st-1] \longrightarrow [0, t-1] \times [0, s-1]$, $\ell \longmapsto (\psi_1(\ell), \psi_2(\ell))$ mit $\ell = s\psi_1(\ell) + \psi_2(\ell)$.

Die Bijektion $\tau : [0, s-1] \times [0, t-1] \longrightarrow [0, t-1] \times [0, s-1]$, $(i, j) \longmapsto (j, i)$.

Die injektive monotone Abbildung $\alpha : [0, s] \longrightarrow [0, st]$, $i \longmapsto ti$.

Die injektive monotone Abbildung $\beta : [0, t] \longrightarrow [0, st]$, $j \longmapsto sj$.

Sei $U'_k := U_{\varphi_1(k)+1}(U_{\varphi_1(k)} \cap V_{\varphi_2(k)})$ für $k \in [0, st-1]$. Sei $U'_{st} := 1$.

Sei $V'_\ell := (V_{\psi_1(\ell)} \cap U_{\psi_2(\ell)})V_{\psi_1(\ell)+1}$ für $\ell \in [0, st-1]$. Sei $V'_{st} := 1$.

Behauptung. Sei $k \in [0, st-1]$. Es ist $U'_{k+1} = U_{\varphi_1(k)+1}(U_{\varphi_1(k)} \cap V_{\varphi_2(k)+1})$.

Ist $k \not\equiv_t -1$, dann ist

$$\begin{array}{rcl} U'_{k+1} & = & U_{\varphi_1(k+1)+1}(U_{\varphi_1(k+1)} \cap V_{\varphi_2(k+1)}) \\ & = & U_{\varphi_1(k)+1}(U_{\varphi_1(k)} \cap V_{\varphi_2(k)+1}) \ . \end{array}$$

Ist $k \equiv_t -1$, dann ist

$$\begin{array}{rcl} U'_{k+1} & = & U_{\varphi_1(k+1)+1}(U_{\varphi_1(k+1)} \cap V_{\varphi_2(k+1)}) \\ & = & U_{\varphi_1(k)+2}(U_{\varphi_1(k)+1} \cap V_0) \\ & = & U_{\varphi_1(k)+1} \\ & = & U_{\varphi_1(k)+1}(U_{\varphi_1(k)} \cap V_t) \\ & = & U_{\varphi_1(k)+1}(U_{\varphi_1(k)} \cap V_{\varphi_2(k)+1}) \ . \end{array}$$

Dies zeigt die *Behauptung.*

Es ist $(U'_k)_{k\in[0,st]}$ eine Subnormalreihe. Denn für $k \in [0, st-1]$ wird dank Behauptung

$$U'_{k+1} \ = \ U_{\varphi_1(k)+1}(U_{\varphi_1(k)} \cap V_{\varphi_2(k)+1}) \ \trianglelefteq \ U_{\varphi_1(k)+1}(U_{\varphi_1(k)} \cap V_{\varphi_2(k)}) = U'_k \ ;$$

cf. Lemma 63. Es ist $(U'_k)_{k\in[0,st]}$ eine Verfeinerung von $(U_i)_{i\in[0,s]}$. Denn für $i \in [0, s-1]$ ist

$$U'_{\alpha(i)} \ = \ U'_{it} \ = \ U_{\varphi_1(it)+1}(U_{\varphi_1(it)} \cap V_{\varphi_2(it)}) \ = \ U_{i+1}(U_i \cap V_0) \ = \ U_i \ .$$

Ferner ist $U'_{\alpha(s)} = U'_{st} = 1 = U_s$.

Genauso ist $(V'_\ell)_{\ell\in[0,st]}$ eine Subnormalreihe von G und dabei eine Verfeinerung von $(V_j)_{j\in[0,t]}$.

Wir haben die Bijektion $\sigma := \psi^{-1} \circ \tau \circ \varphi : [0, st-1] \longrightarrow [0, st-1]$. Sei $k \in [0, st-1]$. Es wird

$$(\psi_1(\sigma(k)), \psi_2(\sigma(k))) \ = \ \psi(\sigma(k)) \ = \ \psi(\psi^{-1}(\tau(\varphi(k))) \ = \ \tau(\varphi(k)) = (\varphi_2(k), \varphi_1(k)) \ .$$

Also wird

$$\begin{aligned} U'_k/U'_{k+1} &\overset{\text{Beh.}}{=} \big(U_{\varphi_1(k)+1}(U_{\varphi_1(k)} \cap V_{\varphi_2(k)})\big)/\big(U_{\varphi_1(k)+1}(U_{\varphi_1(k)} \cap V_{\varphi_2(k)+1})\big) \\ &\overset{\text{L. 63}}{\simeq} \big((U_{\varphi_1(k)} \cap V_{\varphi_2(k)})V_{\varphi_2(k)+1}\big)/\big((U_{\varphi_1(k)+1} \cap V_{\varphi_2(k)})V_{\varphi_2(k)+1}\big) \\ &= \big((V_{\varphi_2(k)} \cap U_{\varphi_1(k)})V_{\varphi_2(k)+1}\big)/\big((V_{\varphi_2(k)} \cap U_{\varphi_1(k)+1})V_{\varphi_2(k)+1}\big) \\ &\overset{\text{Beh.}}{=} \big((V_{\psi_1(\sigma(k))} \cap U_{\psi_2(\sigma(k))})V_{\psi_1(\sigma(k))+1}\big)/\big((V_{\psi_1(\sigma(k))} \cap U_{\psi_2(\sigma(k))+1})V_{\psi_1(\sigma(k))+1}\big) \\ &= V'_{\sigma(k)}/V'_{\sigma(k)+1} \ . \end{aligned}$$

Ad (2). Sei $(\check{U}'_k)_{k\in[0,a]}$ die Striktifizierung von der im Beweis zu (1) konstruierten Subnormalreihe $(U'_k)_{k\in[0,st]}$. Sei $(\check{V}'_\ell)_{\ell\in[0,b]}$ die Striktifizierung von der im Beweis zu (2) konstruierten Subnormalreihe $(V'_\ell)_{\ell\in[0,st]}$.

Es sind $(\check{U}'_k)_{k\in[0,a]}$ und $(\check{V}'_\ell)_{\ell\in[0,b]}$ äquivalent; cf. Bemerkung 69.

Es ist $\{\, U_i \,:\, i \in [0,s] \,\} \subseteq \{\, U'_k \,:\, k \in [0,st] \,\} = \{\, \check{U}'_k \,:\, k \in [0,a] \,\}$. Da $(U_i)_{i\in[0,s]}$ strikt ist, folgt $(U_i)_{i\in[0,s]} \prec (\check{U}'_k)_{k\in[0,a]}$; cf. Bemerkung 70.

Genauso ist $(V_j)_{j\in[0,t]} \prec (\check{V}'_\ell)_{\ell\in[0,b]}$. ▫

Satz 72 (Jordan, Hölder) *Weiterhin ist G eine Gruppe.*

Seien $(U_i)_{i\in[0,s]}$ und $(V_j)_{j\in[0,t]}$ Kompositionsreihen von G.

Dann sind $(U_i)_{i\in[0,s]}$ und $(V_j)_{j\in[0,t]}$ äquivalent; cf. Definition 65*.*

Sei daran erinnert, daß, falls G endlich ist, eine Kompositionsreihe von G existiert; cf. Beispiel 68*.*

Beweis. Gemäß Lemma 71 haben $(U_i)_{i\in[0,s]}$ und $(V_j)_{j\in[0,t]}$ äquivalente Verfeinerungen, die strikte Subnormalreihen sind. Da $(U_i)_{i\in[0,s]}$ eine Kompositionsreihe ist, ist sie gleich dieser ihrer Verfeinerung; da $(V_j)_{j\in[0,t]}$ eine Kompositionsreihe ist, ist sie gleich dieser ihrer Verfeinerung; cf. Bemerkung 67. Also sind bereits $(U_i)_{i\in[0,s]}$ und $(V_j)_{j\in[0,t]}$ äquivalent. ▫

3.2 Auflösbar, überauflösbar, nilpotent

Sei G eine endliche Gruppe.

Definition 73

(1) Gibt es eine Subnormalreihe $(U_i)_{i\in[0,s]}$ von G mit U_i/U_{i+1} abelsch für $i \in [0, s-1]$, dann heißt G *auflösbar.*

Eine solche Subnormalreihe heißt dann *auflösende Reihe* von G.

(2) Gibt es eine Subnormalreihe $(U_i)_{i\in[0,s]}$ von G mit U_i/U_{i+1} zyklisch für $i \in [0, s-1]$ und $U_i \trianglelefteq G$ für $i \in [0, s-1]$, dann heißt G *überauflösbar.*

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

(3) Gibt es eine Subnormalreihe $(U_i)_{i\in[0,s]}$ von G mit $U_i \trianglelefteqslant G$ für $i \in [0,s]$ und $U_i/U_{i+1} \leqslant \mathrm{Z}(G/U_{i+1})$ für $i \in [0,s-1]$, dann heißt G *nilpotent.*

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

(4) Sei $p > 0$ prim. Gibt es eine Subnormalreihe $(U_i)_{i\in[0,s]}$ von G so, daß U_i/U_{i+1} eine p-Gruppe oder eine Gruppe mit Ordnung teilerfremd zu p ist für $i \in [0,s-1]$, dann heißt G nur *p-auflösbar.*

Eine solche Reihe heißt dann *p-auflösende Reihe* von G.

Bemerkung 74

(1) Es ist G genau dann auflösbar, wenn jeder Kompositionsfaktor von G eine zyklische Gruppe von Primordnung ist.

(2) Sei $p > 0$ prim. Es ist G genau dann p-auflösbar, wenn jeder Kompositionsfaktor von G isomorph zu C_p oder von Ordnung teilerfremd zu p ist.

Beweis.

Ad (1). Ist jeder Kompositionsfaktor von G eine zyklische Gruppe von Primordnung, dann ist jede Kompositionsreihe von G auflösend.

Sei umgekehrt G auflösbar. Sei $(U_i)_{i\in[0,s]}$ eine auflösende Reihe von G, o.E. strikt. Sei $(V_j)_{j\in[0,t]}$ eine Kompositionsreihe, die diese verfeinert; cf. Bemerkung 67, Beispiel 68. Dann ist jeder Subfaktor von $(V_j)_{j\in[0,t]}$ isomorph zu einem Subfaktor einer Subnormalreihe von U_i/U_{i+1} für ein $i \in [0,s-1]$, mithin abelsch; cf. Aufgabe 17. Da alle einfachen endlichen abelschen Gruppen zyklisch von Primordnung sind, ist somit jeder Kompositionsfaktor von G zyklisch von Primordnung; cf. Aufgabe 30.(2).

Ad (2). Ist jeder Kompositionsfaktor von G von Ordnung p oder von Ordnung teilerfremd zu p, dann ist jede Kompositionsreihe von G p-auflösend.

Sei umgekehrt G eine p-auflösbare Gruppe. Sei $(U_i)_{i\in[0,s]}$ eine p-auflösende Reihe von G, o.E. strikt. Sei $(V_j)_{j\in[0,t]}$ eine Kompositionsreihe, die diese verfeinert; cf. Bemerkung 67, Beispiel 68. Dann ist jeder Subfaktor von $(V_j)_{j\in[0,t]}$ isomorph zu einem Subfaktor einer Subnormalreihe von U_i/U_{i+1} für ein $i \in [0,s-1]$, mithin eine p-Gruppe oder eine Gruppe mit Ordnung teilerfremd zu G. Es sind aber alle einfachen endlichen p-Gruppen isomorph zu C_p; cf. Aufgabe 31.(2). Also ist jeder Kompositionsfaktor von G isomorph zu C_p oder von Ordnung teilerfremd zu p. □

Die p-Auflösbarkeit soll bei uns nur eine Nebenrolle spielen.

Bemerkung 75

(1) *Sei p eine Primzahl. Ist G eine p-Gruppe, so ist G nilpotent.*

(2) *Ist* $G > 1$ *und* G *nilpotent, so ist* $\mathrm{Z}(G) > 1$.

Beweis.

Ad (1). Induktion über $|G|$. Ist $|G| = 1$, so ist nichts zu zeigen.

Sei $|G| > 1$. Dann ist $\mathrm{Z}(G) \neq 1$; cf. Aufgabe 31.(1). Nach Induktion ist $G/\mathrm{Z}(G)$ nilpotent. Also ist G nilpotent; cf. Aufgabe 32.(6).

Ad (2). Sei $(U_i)_{i\in[0,s]}$ eine nilpotent auflösende Reihe, o.E. strikt. Wegen $G > 1$ ist $s \geqslant 1$. Es ist $U_{s-1} > U_s = 1$ und $U_{s-1}/U_s \leqslant \mathrm{Z}(G/U_s)$, also $U_{s-1} \leqslant \mathrm{Z}(G)$. ▫

Bemerkung 76 *Wir haben die Implikationen*

$$G \text{ abelsch } \Rightarrow\ G \text{ nilpotent } \Rightarrow\ G \text{ überauflösbar } \Rightarrow\ G \text{ auflösbar } \Rightarrow\ G\ \ p\text{-auflösbar für } p > 0 \text{ prim}\,.$$

Beweis. Ist G abelsch, so hat G die nilpotent auflösende Reihe $(G, 1)$.

Sei G nilpotent. Zu zeigen ist, daß G überauflösbar ist. Sei also eine nilpotent auflösende Reihe $(U_i)_{i\in[0,s]}$ von G gegeben.

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

Da $U_{i-1}/U_i \leqslant \mathrm{Z}(G/U_i)$ und da $G/U_{i-1} \simeq (G/U_i)/(U_{i-1}/U_i)$, folgt dies mit Aufgabe 32.(4).

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

Ist G überauflösbar, dann ist G auflösbar.

Ist G auflösbar, dann ist dank Bemerkung 74.(1) jeder Kompositionsfaktor von G zyklisch von Primordnung, dank Bemerkung 74.(2) also G auch p-auflösbar für $p > 0$ prim. ▫

Beispiel 77

(1) Es hat S_3 die Normalteiler S_3 , A_3 und 1.

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 $\mathrm{Z}(\mathrm{S}_3) = \{\mathrm{id}\}$ ist; cf. Aufgabe 20.(2), Bemerkung 75.(2). Beachte, daß nichtsdestoweniger $\mathrm{S}_3/\mathrm{A}_3$ und A_3 nilpotent sind.

(2) Es hat A_4 die Normalteiler A_4 , $V := \langle (1,2)(3,4),\ (1,3)(2,4)\rangle$ und 1 ; und nur diese. Denn das Normalteilererzeugnis eines Elements von Ordnung 2 darin ist gleich V; das Normalteilererzeugnis eines Elements von Ordnung 3 darin ist gleich A_4 . Für letzteres beachte man, daß für $\{a, b, c, d\} \subseteq [1, 4]$ mit $|\{a, b, c, d\}| = 4$ stets (a, b, c) via (b, c, d) konjugiert ist zu (a, c, d), was $(a, b, c) \circ (a, c, d) = (b, c, d)$ zur Folge hat, sodaß das Normalteilererzeugnis von (a, b, c) die achtelementige Menge ${}^{\mathrm{A}_4}(a, b, c) \sqcup {}^{\mathrm{A}_4}(b, c, d)$ enthält.

Insbesondere ist $(\mathrm{A}_4\,, V,\, 1)$ eine Subnormalreihe von A_4.

Es ist A_4 auflösbar, da $\mathrm{A}_4/V \simeq \mathrm{C}_3$ und $V \simeq \mathrm{C}_2 \times \mathrm{C}_2$; cf. Aufgabe 2.(3).

Es ist A_4 nicht überauflösbar, da V nicht zyklisch ist und wir also keine Reihe von Normalteilern von A_4 finden können, deren letzter Subfaktor zyklisch ist. Beachte, daß nichtsdestoweniger A_4/V und V überauflösbar sind.

(3) Sei $n \geqslant 5$. Es hat S_n die Kompositionsreihe $(\mathrm{S}_n\,,\, \mathrm{A}_n\,,\, 1)$; cf. Satz 48. Somit hat S_n die Kompositionsfaktoren C_2 und A_n, die nicht beide zyklisch von Primzahlordnung sind, da $|\mathrm{A}_n| \equiv_{60} 0$. Folglich ist S_n nicht auflösbar; cf. Bemerkung 74.(1).

(4) Sei K ein endlicher Körper. Sei $\operatorname{char} K =: p > 0$. Sei $|K| = p^\alpha =: q$, wobei $\alpha \geqslant 1$.

Sei $n \geqslant 2$. Sei $(n, p^\alpha) \notin \{(2,2),(2,3)\}$. Es hat $\mathrm{GL}_n(K)$ die Subnormalreihe $(\mathrm{GL}_n(K), \mathrm{SL}_n(K), \mathrm{Z}(\mathrm{SL}_n(K)), 1)$. Da diese zu einer Kompositionsreihe verfeinerbar ist, hat $\mathrm{GL}_n(K)$ den Kompositionsfaktor $\mathrm{PSL}_n(K)$; cf. Satz 49. Es ist

$$|\,\mathrm{PSL}_n(K)| \;=\; (q^n - q^0)(q^n - q^1) \cdot \ldots \cdot (q^n - q^{n-1}) \cdot (q-1)^{-1} \cdot |\mathrm{Z}(\mathrm{SL}_n(K))|^{-1}\,.$$

Da $\mathrm{Z}(\mathrm{SL}_n(K)) \simeq \{\, x \in \mathrm{U}(K) \,:\, x^n = 1 \,\} \leqslant \mathrm{U}(K)$ ist, ist $|\mathrm{Z}(\mathrm{SL}_n(K))|$ ein Teiler von $q-1$. Folglich ist $|\mathrm{PSL}_n(K)|$ teilbar durch $(q+1)q$ und also nicht prim. Somit ist $\mathrm{GL}_n(K)$ nicht auflösbar; cf. Bemerkung 74.(1).

(5) Sei K ein endlicher Körper. Sei $\operatorname{char} K =: p > 0$. Sei $|K| = p^\alpha$, wobei $\alpha \geqslant 1$.

Sei $n \geqslant 1$. Sei

$$B \;:=\; \{\, (a_{i,j})_{i,j} \in \mathrm{GL}_n(K) \,:\, a_{i,j} = 0 \text{ für } n \geqslant i > j \geqslant 1 \,\} \;\leqslant\; \mathrm{GL}_n(K)$$

die Untergruppe der oberen Dreiecksmatrizen. Sei

$$U \;:=\; \{\, (a_{i,j})_{i,j} \in \mathrm{GL}_n(K) \,:\, a_{i,j} = 0 \text{ für } n \geqslant i > j \geqslant 1 \text{ und } a_{i,i} = 1 \text{ für } i \in [1,n] \,\} \;\leqslant\; B$$

darin die Untergruppe der unipotenten oberen Dreiecksmatrizen.

Es ist U der Kern des surjektiven Gruppenmorphismus

$$\begin{array}{rcl} B & \longrightarrow & \mathrm{U}(K)^{\times n} \\ (a_{i,j})_{i,j} & \longmapsto & (a_{i,i})_{i \in [1,n]}\,. \end{array}$$

Da $|U| = p^{\alpha n(n-1)/2}$, ist U nilpotent, folglich auflösbar; cf. Bemerkungen 75.(1) und 76. Es ist $\mathrm{U}(K)^{\times n}$ abelsch, folglich auflösbar. Also ist B auflösbar; cf. Aufgabe 32.(1).

Definition 78 Sei $U \leqslant G$.

Es heißt U eine *charakteristische Untergruppe* von G, geschrieben $U \operatorname{\blacktriangleleft} G$, wenn $\alpha(U) = U$ ist für $\alpha \in \mathrm{Aut}(G)$.

Wir schreiben $U \blacktriangleleft G$ für $(U \operatorname{\blacktriangleleft} G$ und $U < G)$.

Hierfür genügt es, wenn $\alpha(U) \leqslant U$ ist für $\alpha \in \mathrm{Aut}(G)$. Denn daraus folgt $U \leqslant \alpha^-(U)$ für $\alpha \in \mathrm{Aut}(G)$. Oder aber man verwendet die vorausgesetzte Endlichkeit von G.

Beispiel 79 Sei $V := \langle\, (1,2)(3,4)\,,\ (1,3)(2,4)\,\rangle \trianglelefteqslant \mathrm{S}_4$; cf. Beispiel 66. Es ist $V \simeq \mathrm{C}_2 \times \mathrm{C}_2$; cf. Aufgabe 2.(3).

Wir haben den inneren Automorphismus auf S_4 , der durch Konjugation mit $(1,2)$ gegeben ist. Dieser schränkt ein zu einem Automorphismus $\alpha \in \mathrm{Aut}(V)$. Sei $U := \langle (1,3)(2,4) \rangle \leqslant V$. Es ist

$$\alpha(U) \ = \ \langle\, {}^{(1,2)}(1,3)(2,4) \rangle \ = \ \langle (1,4)(2,3) \rangle \ \neq \ U \ .$$

Also ist $U \not\trianglelefteqslant V$, wohl aber $U \trianglelefteqslant V$.

Bemerkung 80

(1) Sei $U \leqslant G$. Da genau dann $U \trianglelefteqslant G$ ist, wenn $\alpha(U) = U$ ist für alle $\alpha \in \mathrm{Inn}(G)$, haben wir die Implikation $U \trianglelefteqslant G \Rightarrow U \trianglelefteqslant G$; cf. Aufgabe 23.

(2) Ist $U \trianglelefteqslant V \trianglelefteqslant G$, dann ist $U \trianglelefteqslant G$. Denn für $g \in G$ ist $\alpha : V \longrightarrow V,\ x \longmapsto {}^g x$ in $\mathrm{Aut}(V)$, sodaß ${}^g U = \alpha(U) = U$ folgt.

(3) Ist $U \trianglelefteqslant V \trianglelefteqslant G$, dann ist $U \trianglelefteqslant G$. Denn für $\beta \in \mathrm{Aut}(G)$ ist $\alpha := \beta|_V^V \in \mathrm{Aut}(V)$, sodaß $\beta(U) = \alpha(U) = U$ folgt.

(4) Es ist $\mathrm{Z}(G) \trianglelefteqslant G$. Denn für $\alpha \in \mathrm{Aut}(G)$ ist $\alpha(\mathrm{Z}(G)) \leqslant \mathrm{Z}(G)$; cf. Aufgabe 34.(3).

(5) Sind $U, V \trianglelefteqslant G$, dann ist $[U,V] \trianglelefteqslant G$. Denn für $\alpha \in \mathrm{Aut}(G)$ ist $\alpha([U,V]) = [\alpha(U), \alpha(V)] = [U,V]$; cf. Aufgabe 34.(1).

(6) Ist $U \trianglelefteqslant G$ und $U \leqslant V \leqslant G$ mit $V/U \trianglelefteqslant G/U$ gegeben, dann ist $V \trianglelefteqslant G$. Denn für $\alpha \in \mathrm{Aut}(G)$ ist $\bar\alpha : G/U \longrightarrow G/U,\ gU \longmapsto \bar\alpha(gU) := \alpha(g)U$ wegen $\alpha(U) = U$ wohldefiniert und also in $\mathrm{Aut}(G/U)$ enthalten. Wegen $V/U \trianglelefteqslant G/U$ ist $\alpha(V)/U = \bar\alpha(V/U) = V/U$ und also $\alpha(V) = V$.

(7) Ist $p > 0$ prim und ist $\mathrm{Syl}_p(G) = \{P\}$, dann ist $P \trianglelefteqslant G$, denn für $\alpha \in \mathrm{Aut}(G)$ ist $|\alpha(P)| = |P| = |G|[p]$, also $\alpha(P) \in \mathrm{Syl}_p(G) = \{P\}$, also $\alpha(P) = P$.

Definition 81

(1) Setze rekursiv $G^{(0)} := G$ und $G^{(i+1)} := (G^{(i)})^{(1)} = [G^{(i)}, G^{(i)}]$ für $i \geqslant 0$. Cf. auch Aufgabe 13.

(2) Setze rekursiv $G^{[0]} := G$ und $G^{[i+1]} := [G^{[i]}, G]$ für $i \geqslant 0$.

(3) Setze $G^{]0[} := 1$. Definiere rekursiv $G^{]i+1[} \leqslant G$ durch $G^{]i+1[}/G^{]i[} := \mathrm{Z}(G/G^{]i[})$ für $i \geqslant 0$; cf. Aufgabe 17.(3).

Bemerkung 82

(1) *Es ist* $G^{(1)} = G^{[1]} = [G,G]$. *Es ist* $G^{(2)} = [G^{(1)}, G^{(1)}]$. *Es ist* $G^{[2]} = [G^{(1)}, G]$. *Es ist* $G^{]1[} = \mathrm{Z}(G)$.

(2) *Es ist* $G^{(i)} \trianglelefteq G$ *und* $G^{[i]} \trianglelefteq G$ *und* $G^{]i[} \trianglelefteq G$ *für* $i \geqslant 0$.

(3) *Es ist* $G^{(i)} \leqslant G^{[i]}$ *für* $i \geqslant 0$.

(4) *Sei* $i \geqslant 0$. *Sei* $x \in G$. *Es ist* $x \in G^{]i+1[}$ *genau dann, wenn* $xG^{]i[} \in \mathrm{Z}(G/G^{]i[})$, *i.e. wenn* $[x, G] \subseteq G^{]i[}$ *ist.*

(5) *Es ist* $(G/\mathrm{Z}(G))^{]i[} = G^{]i+1[}/\mathrm{Z}(G)$ *für* $i \geqslant 0$.

(6) *Seien* i, $j \geqslant 0$. *Genau dann ist* $G^{[i]} \leqslant G^{]j+1[}$, *wenn* $G^{[i+1]} \leqslant G^{]j[}$ *ist.*

Beweis.

Ad (2). Es folgen $G^{(i)} \trianglelefteq G$ und $G^{[i]} \trianglelefteq G$ für $i \geqslant 0$ aus iterierter Anwendung von Bemerkung 80.(5).

Es folgt $G^{]i[} \trianglelefteq G$ für $i \geqslant 0$ aus iterierter Anwendung von Bemerkung 80.(4) unter Verwendung von Bemerkung 80.(6).

Ad (3). Induktion über $i \geqslant 0$. Aus $G^{(i)} \leqslant G^{[i]}$ folgt $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leqslant [G^{[i]}, G^{(i)}] \leqslant [G^{[i]}, G] = G^{[i+1]}$.

Ad (5). Schreibe $Z := \mathrm{Z}(G)$. Induktion über $i \geqslant 0$. Für $i = 0$ ist $(G/Z)^{]0[} = Z/Z = G^{]1[}/Z$. Sei die Gleichung für ein $i \geqslant 0$ gezeigt. Wir wollen sie für $i + 1$ zeigen.

Sei $x \in G$. Es ist $xZ \in (G/Z)^{]i+1[}$ dank (4) und Induktion genau dann, wenn $[xZ, G/Z] \subseteq (G/Z)^{]i[} = G^{]i+1[}/Z$ ist, i.e. wenn $[x, G] \subseteq G^{]i+1[}$ ist, i.e., dank (4), wenn $x \in G^{]i+2[}$ ist.

Ad (6). Gemäß (4) ist $G^{[i]} \leqslant G^{]j+1[}$ genau dann, wenn $G^{[i+1]} = [G^{[i]}, G] \leqslant G^{]j[}$ ist. ▫

Beispiel 83 Sei $B = \{ \left(\begin{smallmatrix} a & b \\ u & c \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_3) \,:\, u = 0 \} \leqslant \mathrm{GL}_2(\mathbf{F}_3)$; cf. Beispiel 77.(5). Kurz, $B = \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$.

Damit $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \in \mathrm{Z}(B)$ liegt, muß $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) = \left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ sein für x, $z \in \mathbf{F}_3^\times$ und $y \in \mathbf{F}_3$, i.e. $ay + bz = xb + yc$. Es erzwingt die Wahl $(x, y, z) = (1, 1, 1)$, daß $a + b = b + c$ ist; es erzwingt die Wahl $(x, y, z) = (-1, 1, 1)$, daß $a + b = -b + c$ ist; folglich ist $b = 0$ und also $a = c$. Mithin ist $B^{]1[} = \mathrm{Z}(B) = \langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \rangle$.

Schreibe $\overline{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)} := \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)\mathrm{Z}(B) \in B/\mathrm{Z}(B)$ für $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \in B$. Damit $\overline{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)} \in \mathrm{Z}(B/\mathrm{Z}(B))$ liegt, muß $\overline{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)}\,\overline{\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right)} = \overline{\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right)}\,\overline{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)}$ sein für x, $z \in \mathbf{F}_3^\times$ und $y \in \mathbf{F}_3$, i.e. $\overline{\left(\begin{smallmatrix} ax & ay+bz \\ 0 & cz \end{smallmatrix}\right)} = \overline{\left(\begin{smallmatrix} xa & xb+yz \\ 0 & zc \end{smallmatrix}\right)}$, i.e., wegen $xa \neq -xa$, $\left(\begin{smallmatrix} ax & ay+bz \\ 0 & cz \end{smallmatrix}\right) = \left(\begin{smallmatrix} xa & xb+yz \\ 0 & zc \end{smallmatrix}\right)$. Wie oben folgt $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \in \langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \rangle$, nur bedeutet dies nun $\mathrm{Z}(B/\mathrm{Z}(B)) = \mathrm{Z}(B)/\mathrm{Z}(B) = B^{]2[}/\mathrm{Z}(B)$ und also $B^{]2[} = B$. Dies wiederholt sich nun, sodaß wir

$$1 \;=\; B^{]0[} \;<\; B^{]1[} \;=\; B^{]2[} \;=\; B^{]3[} \;=\; \ldots$$

erhalten, wobei allerdings $B^{]1[} < B$ ist.

Satz 84 (Kommutatorreihe) *Weiterhin ist* G *eine endliche Gruppe.*

Die Aussagen $(1, 2)$ *sind äquivalent.*

(1) *Es ist G auflösbar.*

(2) *Es gibt ein $i \geqslant 0$ mit $G^{(i)} = 1$.*

Diesenfalls sei $m := \min\{\, i \geqslant 0 \,:\, G^{(i)} = 1 \,\}$; es heißt die Subnormalreihe $(G^{(i)})_{i\in[0,m]}$ die Kommutatorreihe *von G.*

Beweis.

Ad (1) $\Rightarrow$ (2). Sei $(U_i)_{i\in[0,s]}$ eine auflösende Reihe von G. Wir *behaupten* $G^{(i)} \overset{!}{\leqslant} U_i$ für $i \in [0,s]$. Induktion über $i \in [0,s]$. Es ist $G^{(0)} = G = U_0$. Sei nun $G^{(i)} \leqslant U_i$ für ein $i \in [0, s-1]$. Es ist U_i/U_{i+1} abelsch. Also ist $[x,y]U_{i+1} = [xU_{i+1}\,,\, yU_{i+1}] = 1\,U_{i+1}$ für $x,\, y \in U_i$. Es folgt $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leqslant [U_i\,, U_i] \leqslant U_{i+1}$. Dies zeigt die *Behauptung.* Für $i = s$ liefert diese $G^{(s)} \leqslant U_s = 1$, i.e. $G^{(s)} = 1$.

Ad (2) $\Rightarrow$ (1). Es ist $G^{(i+1)} \blacktriangleleft G$, also $G^{(i+1)} \trianglelefteqslant G^{(i)}$ für $i \geqslant 0$; cf. Bemerkung 82.(2). Es ist $G^{(i)}/G^{(i+1)}$ abelsch; cf. Aufgabe 13.(2). Also ist $(G^{(i)})_{i\in[0,m]}$ eine auflösende Reihe von G. ▫

Bemerkung 85 Sei G auflösbar.

Es ist in der Kommutatorreihe $(G^{(i)})_{i\in[0,m]}$ zwar $G^{(i)} \trianglelefteqslant G$ für $i \in [0,m]$, dafür aber $G^{(i)}/G^{(i+1)}$ i.a. nicht für jedes $i \in [0, m-1]$ zyklisch.

Es ist in einer Kompositionsreihe $(U_i)_{i\in[0,s]}$ zwar U_i/U_{i+1} zyklisch, zudem von Primordnung, dafür aber U_i i.a. nicht für jedes $i \in [0,s]$ ein Normalteiler von G.

Somit liefert weder die eine noch die andere Reihe ein Argument dafür, daß G überauflösbar sein sollte. Dies ist i.a. ja auch nicht der Fall; cf. Beispiel 77.(2).

Satz 86 (Zentralreihen) *Weiterhin ist G eine endliche Gruppe.*

Die Aussagen $(1,2,3)$ *sind äquivalent.*

(1) *Es ist G nilpotent.*

(2) *Es gibt ein $i \geqslant 0$ mit $G^{[i]} = 1$.*

(3) *Es gibt ein $j \geqslant 0$ mit $G^{]j[} = G$.*

Sei G nilpotent. Dann ist

$$u \;:=\; \min\{\, i \geqslant 0 \,:\, G^{[i]} = 1 \,\} \;=\; \min\{\, j \geqslant 0 \,:\, G^{]j[} = G \,\}\,;$$

es heißt die Subnormalreihe $(G^{[i]})_{i\in[0,u]}$ die absteigende Zentralreihe *von G;*
es heißt die Subnormalreihe $(G^{]u-i[})_{i\in[0,u]}$ die aufsteigende Zentralreihe *von G.*
Es ist $G^{[i]} \leqslant G^{]u-i[}$ für $i \in [0,u]$.

Beweis. Schreibe $Z := \mathrm{Z}(G)$.

Ad (1) $\Rightarrow$ (3). Induktion über $|G|$. Sei $|G| > 1$. Es ist $Z > 1$, also $|G/Z| < |G|$; cf. Bemerkung 75.(2). Es ist auch G/Z nilpotent; cf. Aufgabe 32.(7). Mit Induktion gibt es ein $j' \geqslant 0$ mit $(G/Z)^{]j'[} = G/Z$. Dank Bemerkung 82.(5) ist $(G/Z)^{]j'[} = G^{]j'+1[}/Z$. Insgesamt folgt $G = G^{]j'+1[}$.

Ad (3) $\Rightarrow$ (1). Induktion über $|G|$. Sei $|G| > 1$. Sei $t \geqslant 0$ minimal mit $G^{]t[} = G$ gegeben. Es ist $t \geqslant 1$. Es ist $G^{]1[} = Z > 1$. Es ist $(G/Z)^{]t-1[} = G^{]t[}/Z = G/Z$ dank Bemerkung 82.(5). Mit Induktion ist G/Z nilpotent. Also ist G nilpotent; cf. Aufgabe 32.(6).

Ad (2) $\Rightarrow$ (3). Sei s minimal mit $G^{[s]} = 1$. Wir *behaupten* $G^{[s-j]} \overset{!}{\leqslant} G^{]j[}$ für $j \in [0, s]$. Induktion über $j \in [0, s]$. Aus $G^{[s-j]} \leqslant G^{]j[}$ folgt $G^{[s-j-1]} \leqslant G^{]j+1[}$, sofern $j \in [0, s-1]$; cf. Bemerkung 82.(6). Dies zeigt die *Behauptung*. Für $j = s$ folgt $G = G^{[0]} \leqslant G^{]s[} \leqslant G$, also $G^{]s[} = G$. Insbesondere ist dann $\min\{\, i \geqslant 0 : G^{[i]} = 1 \,\} = s \geqslant \min\{\, j \geqslant 0 : G^{]j[} = G \,\}$.

Ad (3) $\Rightarrow$ (2). Sei t minimal mit $G^{]t[} = G$. Wir *behaupten* $G^{]t-i[} \overset{!}{\geqslant} G^{[i]}$ für $i \in [0, t]$. Induktion über $i \in [0, t]$. Aus $G^{]t-i[} \geqslant G^{[i]}$ folgt $G^{]t-i-1[} \geqslant G^{[i+1]}$, sofern $i \in [0, t-1]$; cf. Bemerkung 82.(6). Dies zeigt die *Behauptung*. Für $i = t$ folgt $1 = G^{]0[} \geqslant G^{[t]} \geqslant 1$, also $G^{[t]} = 1$. Insbesondere ist dann $\min\{\, j \geqslant 0 : G^{]j[} = G \,\} = t \geqslant \min\{\, i \geqslant 0 : G^{[i]} = 1 \,\}$.

Falls G nilpotent ist, so zeigt dies auch

$$\underbrace{\min\{\, i \geqslant 0 : G^{[i]} = 1 \,\}}_{=s} = \underbrace{\min\{\, j \geqslant 0 : G^{]j[} = G \,\}}_{=t} =: u$$

und $G^{[i]} \leqslant G^{]u-i[}$ für $i \in [0, u]$. ▫

Beispiel 87 (Fortsetzung) Im Lichte von Satz 86 wurde in Beispiel 83 gezeigt, daß die dortige Gruppe B nicht nilpotent ist, da $B^{]j[} < B$ für alle $j \geqslant 0$.

Lemma 88 *Sei p eine Primzahl. Sei $N \trianglelefteqslant G$.*

(1) *Wir haben die surjektive Abbildung*

$$\begin{array}{rcl} \mathrm{Syl}_p(G) & \xrightarrow{\rho_{G,N}} & \mathrm{Syl}_p(G/N) \\ Q & \longmapsto & (QN)/N \end{array}$$

(2) *Ist $N \leqslant \mathrm{Z}(G)$, so ist die Abbildung $\rho_{G,N}$ bijektiv.*

Beweis.

Ad (1). Sei $P \in \mathrm{Syl}_p(N)$; cf. Satz 38.(1). Sei $\tilde{Q} \in \mathrm{Syl}_p(G)$ mit $P \leqslant \tilde{Q}$; cf. Satz 38.(4).

Für die Wohldefiniertheit von $\rho_{G,N}$ haben wir für $Q \in \mathrm{Syl}_p(G)$ zu zeigen, daß auch $(QN)/N \overset{!}{\in} \mathrm{Syl}_p(G/N)$ ist; cf. auch Aufgabe 17.(2).

Sei $x \in G$ mit ${}^{x}Q = \tilde{Q}$; cf. Satz 38.(2). Es ist ${}^{xN}((QN)/N) = (xN)((QN)/N)(xN)^{-} = (x(QN)x^{-})/N = {}^{x}(QN)/N = ({}^{x}Q\,{}^{x}N)/N = (\tilde{Q}N)/N$. Somit können wir uns darauf beschränken, $(\tilde{Q}N)/N \overset{!}{\in} \mathrm{Syl}_p(G/N)$ zu zeigen.

Wegen $\tilde{Q} \cap N \leqslant \tilde{Q}$ ist $\tilde{Q} \cap N$ eine p-Gruppe. Wegen $P \leqslant \tilde{Q} \cap N \leqslant N$ und wegen $P \in \mathrm{Syl}_p(N)$ folgt $P = \tilde{Q} \cap N$. Somit ist $(\tilde{Q}N)/N \simeq \tilde{Q}/(\tilde{Q} \cap N) = \tilde{Q}/P$; cf. Aufgabe 12.(2). Folglich ist $|(\tilde{Q}N)/N| = |\tilde{Q}/P| = |\tilde{Q}|/|P| = |G|[p]/|N|[p] = |G/N|[p]$ und daher auch $(\tilde{Q}N)/N \in \mathrm{Syl}_p(G/N)$.

Zeigen wir die Surjektivität von $\rho_{G,N}$. Sei $K/N \in \mathrm{Syl}_p(G/N)$, wobei $N \leqslant K \leqslant G$; cf. Aufgabe 17.(1). Da auch $(\tilde{Q}N)/N \in \mathrm{Syl}_p(G/N)$ ist, gibt es ein $y \in G$ mit $K/N = {}^{yN}((\tilde{Q}N)/N) = ({}^{y}\tilde{Q}N)/N$; cf. Satz 38.(2). Da auch ${}^{y}\tilde{Q} \in \mathrm{Syl}_p(G)$ liegt, zeigt dies $K/N = \rho_{G,N}({}^{y}\tilde{Q})$.

Ad (2). Dank (1) genügt es, die Injektivität von $\rho_{G,N}$ zu zeigen.

Seien $Q, Q' \in \mathrm{Syl}_p(G)$ mit $QN/N = Q'N/N$ gegeben. Zu zeigen ist $Q \overset{!}{=} Q'$. Es ist $QN = Q'N$. Wegen $Q, Q' \leqslant QN \leqslant G$ sind auch $Q, Q' \in \mathrm{Syl}_p(QN)$. Folglich gibt es $q \in Q$ und $n \in N$ mit ${}^{qn}Q = Q'$; cf. Satz 38.(2). Wegen $N \leqslant \mathrm{Z}(G)$ ist aber ${}^{qn}Q = {}^{q}Q = Q$. Also ist $Q' = Q$. ▫

Satz 89 (Sylowzerlegung nilpotenter Gruppen)

Weiterhin ist G eine endliche Gruppe.

Schreibe $\pi(G) := \{\, p \in \mathbf{Z}_{>0} \,:\, p \text{ prim}, \, |G| \equiv_p 0 \,\}$.

Sei $\ell := |\pi(G)|$. *Schreibe* $\pi(G) = \{\, p_i \,:\, i \in [1,\ell] \,\}$.

Für alle $i \in [1,\ell]$ *wählen wir ein* $Q_i \in \mathrm{Syl}_{p_i}(G)$ *; cf. Satz* 38.(1).

Die folgenden Aussagen $(1,2,3,4)$ *sind äquivalent.*

(1) *Es ist G nilpotent.*

(2) *Es ist* $|\,\mathrm{Syl}_p(G)| = 1$ *für* $p \in \pi(G)$.

(3) *Wir haben den Gruppenisomorphismus* $\prod_{i\in[1,\ell]} Q_i \xrightarrow{\sim} G$, $(q_i)_i \longmapsto q_1 \cdot q_2 \cdot \ldots \cdot q_\ell$.

(4) *Es ist* $G \simeq \prod_{i\in[1,\ell]} Q_i$.

Beweis.

Ad (4) $\Rightarrow$ (1). Als p_i-Gruppe ist Q_i nilpotent für alle $i \in [1,\ell]$; cf. Bemerkung 75.(1). Ferner ist ein direktes Produkt nilpotenter Gruppen nilpotent; cf. Aufgabe 35.(4), iteriert angewandt. Also ist G isomorph zu einer nilpotenten Gruppe, mithin selbst nilpotent.

Ad (1) $\Rightarrow$ (2). Sei $(U_j)_{j\in[0,s]}$ eine nilpotent auflösende Reihe von G, i.e. sei $U_0 = G$, sei $U_s = 1$, sei $U_j \trianglelefteq G$ für $j \in [0,s]$ und sei $U_j/U_{j+1} \leqslant \mathrm{Z}(G/U_{j+1})$ für $i \in [0,s-1]$.

Sei $i \in [1,\ell]$.

Wir wollen mit Induktion zeigen, daß G/U_j genau eine p_i-Sylowgruppe hat für $j \in [0,s]$. Dies trifft für $j=0$ zu. Sei $j \in [0,s-1]$ und habe G/U_j genau eine p_i-Sylowgruppe. Wir haben zu zeigen, daß G/U_{j+1} genau eine p_i-Sylowgruppe hat.

Da $U_j/U_{j+1} \leqslant \mathrm{Z}(G/U_{j+1})$ ist und da $(G/U_{j+1})/(U_j/U_{j+1}) \simeq G/U_j$ ist, folgt dies mit Lemma 88.(2).

Für $j=s$ zeigt dies nun insbesondere, daß $|\operatorname{Syl}_{p_i}(G)| = 1$ ist.

Ad (2) $\Rightarrow$ (3). Nun ist $\operatorname{Syl}_{p_i}(G) = \{Q_i\}$ und also $Q_i \trianglelefteq G$ für $i \in [1,\ell]$; cf. Satz 38.(2).

Wir *behaupten,* es ist $|Q_1Q_2\cdot\ldots\cdot Q_i| = |Q_1||Q_2|\cdot\ldots\cdot|Q_i|$ und $(Q_1\cdot\ldots\cdot Q_{i-1})\cap Q_i = 1$ für $i \in [0,\ell]$. Induktion über $i \in [0,\ell]$. Für $i=0$ erhalten wir in beiden Gleichungen auf beiden Seiten 1. Sei $i \in [0,\ell-1]$ gegeben. Sei $|Q_1\cdot\ldots\cdot Q_i| = |Q_1|\cdot\ldots\cdot|Q_i|$ bekannt. Zunächst sind $|Q_1\cdot\ldots\cdot Q_i| = |Q_1|\cdot\ldots\cdot|Q_i|$ und $|Q_{i+1}|$ teilerfremd, woraus wir $(Q_1\cdot\ldots\cdot Q_i)\cap Q_{i+1} = 1$ ersehen. Weiter folgt

$$|Q_1\cdot\ldots\cdot Q_i\,Q_{i+1}| \overset{\text{A. 12.(1)}}{=} \frac{|Q_1\cdot\ldots\cdot Q_i||Q_{i+1}|}{|(Q_1\cdot\ldots\cdot Q_i)\cap Q_{i+1}|} = |Q_1\cdot\ldots\cdot Q_i||Q_{i+1}| = |Q_1|\cdot\ldots\cdot|Q_i||Q_{i+1}| .$$

Dies zeigt die *Behauptung.*

Seien $i,\ j \in [1,\ell]$ mit $i \neq j$ gegeben. Da für $q_i \in Q_i$ und $q_j \in Q_j$ sich $[q_i\,,\,q_j] = {}^{q_i^-}(q_j^-)q_j = q_i^{-\,{}^{q_j^-}}q_i \in Q_i \cap Q_j = 1$ ergibt, ist $[Q_i\,,\,Q_j] = 1$.

Damit und mit obiger Behauptung erhalten wir dank Aufgabe 2.(3) nun den injektiven Gruppenmorphismus

$$\begin{array}{ccc} \prod_{i\in[1,\ell]} Q_i & \overset{f}{\rightarrowtail} & G \\ (q_i)_i & \longmapsto & q_1q_2\cdot\ldots\cdot q_\ell\ . \end{array}$$

Schließlich ist

$$|\textstyle\prod_{i\in[1,\ell]} Q_i| = \prod_{i\in[1,\ell]} |Q_i| = \prod_{i\in[1,\ell]} |G|[p_i] = |G| .$$

Also ist f ein Gruppenisomorphismus.

Ad (3) $\Rightarrow$ (4). Dies gilt a fortiori. ▫

3.3 Semidirekte Produkte

Definition 90 Sei H eine Gruppe. Sei N eine Gruppe. Sei $\alpha : H \longrightarrow \operatorname{Aut}(N)$ ein Gruppenmorphismus. Schreibe auch $(\alpha(h))(n) =: {}^hn$ für $h \in H$ und $n \in N$. Beachte ${}^h(nn') = {}^hn\,{}^hn'$ und ${}^{hh'}n = {}^h({}^{h'}n)$ für $n,\ n' \in N$ und $h,\ h' \in H$.

Wir definieren auf der Menge $N \times H$ eine Multiplikation durch

$$(n,h)(n',h') = (n,h) \underset{\alpha}{\cdot} (n',h') := (n\,{}^hn', hh') .$$

für $n,\, n' \in N$ und $h,\, h' \in H$.

Da dann

$$(n,h)(1,1) \;=\; (n,h)$$

und

$$\begin{array}{rcccl} ((n,h)(n',h'))(n'',h'') & = & (n\ {}^{h}n', hh')(n'',h'') & = & (n\ {}^{h}n'\ {}^{hh'}n'', hh'h'') \\ & = & (n,h)(n'\ {}^{h'}n'', h'h'') & = & (n,h)((n',h')(n'',h'')) \end{array}$$

sowie

$$(n,h)({}^{h^-}(n^-), h^-) \;=\; (1,1)$$

ist für $n,\, n',\, n'' \in N$ und $h,\, h',\, h'' \in H$, wird die Menge $N \times H$ ausgestattet mit $(\,\underset{\alpha}{\cdot}\,)$ dank Aufgabe 1 zu einer Gruppe, genannt *(äußeres) semidirektes Produkt* von N mit H mittels α und geschrieben

$$N \underset{\alpha}{\rtimes} H\ .$$

Oft schreiben wir kurz $N \rtimes H := N \underset{\alpha}{\rtimes} H$.

E.g. ist ${}^{(1,h)}(n,1) = (1,h)(n,1)(1,h^-) = ({}^{h}n, 1)$ für $n \in N$ und $h \in H$.

Wir haben die kurz exakte Sequenz

$$\begin{array}{ccccc} N & \overset{\iota}{\rightarrowtail} & N \underset{\alpha}{\rtimes} H & \overset{\rho}{\twoheadrightarrow} & H \\ n & \longmapsto & (n,1) & & \\ & & (n,h) & \longmapsto & h\ . \end{array}$$

Wir haben den Gruppenmorphismus $\sigma : H \longrightarrow N \underset{\alpha}{\rtimes} H$, $h \longmapsto (1,h)$. Es ist $\rho \circ \sigma = \mathrm{id}_H$.

Bemerkung 91 Seien H und N Gruppen. Es ist $N \underset{!}{\rtimes} H = N \times H$. In diesem Sinne verallgemeinert das semidirekte Produkt das direkte Produkt; cf. Aufgabe 2.(1).

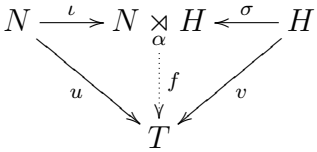
Lemma 92 (Universelle Eigenschaft des semidirekten Produktes)

Sei H eine Gruppe. Sei N eine Gruppe. Sei $\alpha : H \longrightarrow \mathrm{Aut}(N)$ ein Gruppenmorphismus. Schreibe wiederum auch $(\alpha(h))(n) =: {}^{h}n$ für $h \in H$ und $n \in N$.

Beachte ${}^{\sigma(h)}\iota(n) = \iota({}^{h}n)$ für $h \in H$ und $n \in N$, wie in Definition 90 angemerkt.

Sei T eine Gruppe. Sei $u : N \longrightarrow T$ ein Gruppenmorphismus. Sei $v : H \longrightarrow T$ ein Gruppenmorphismus. Sei ${}^{v(h)}u(n) = u({}^{h}n)$ für $h \in H$ und $n \in N$.

Dann gibt es genau einen Gruppenmorphismus $f : N \underset{\alpha}{\rtimes} H \longrightarrow T$ mit $f \circ \iota = u$ und $f \circ \sigma = v$.



Für diesen ist $f(n,h) = u(n) \cdot v(h)$ für $n \in N$ und $h \in H$.

Beweis.

Eindeutigkeit. Sei $\tilde{f} : N \underset{\alpha}{\rtimes} H \longrightarrow T$ ein Gruppenmorphismus mit $\tilde{f} \circ \iota = u$ und $\tilde{f} \circ \sigma = v$.

Für $n \in N$ und $h \in H$ ist dann notwendig $\tilde{f}(n,h) = \tilde{f}((n,1)\cdot(1,h)) = \tilde{f}(n,1)\cdot\tilde{f}(1,h) = (\tilde{f}\circ\iota)(n)\cdot(\tilde{f}\circ\sigma)(h) = u(n)\cdot v(h)$.

Existenz. Sei $f(n,h) = u(n)\cdot v(h)$ für $n \in N$ und $h \in H$. Dann ist $(f\circ\iota)(n) = f(n,1) = u(n)$, also $f\circ\iota = u$, und $(f\circ\sigma)(h) = f(1,h) = v(h)$, also $f\circ\sigma = v$.

Zu zeigen bleibt, daß f ein Gruppenmorphismus ist. Seien (n,h), $(\tilde{n},\tilde{h}) \in N \underset{\alpha}{\rtimes} H$. Dann ist

$$\begin{aligned} f((n,h)\cdot(\tilde{n},\tilde{h})) &= f(n\,{}^h\tilde{n}, h\tilde{h}) \\ &= u(n\,{}^h\tilde{n})\cdot v(h\tilde{h}) \\ &= u(n)\cdot u({}^h\tilde{n})\cdot v(h)\cdot v(\tilde{h}) \\ &= u(n)\cdot {}^{v(h)}u(\tilde{n})\cdot v(h)\cdot v(\tilde{h}) \\ &= u(n)\cdot v(h)\cdot u(\tilde{n})\cdot v(\tilde{h}) \\ &= f(n,h)\cdot f(\tilde{n},\tilde{h})\ . \end{aligned}$$

□

Lemma 93 *Sei G eine Gruppe. Sei $N \trianglelefteq G$. Sei $H \leqslant G$.*

Setze $\alpha : H \longrightarrow \mathrm{Aut}(N)$, $h \longmapsto (n \longmapsto {}^hn = hnh^-)$. Es ist α ein Gruppenmorphismus.

Wir haben den Gruppenmorphismus

$$\begin{array}{ccccc} N & \underset{\alpha}{\rtimes} & H & \xrightarrow{\varphi} & G \\ (n & , & h) & \longmapsto & nh \end{array}$$

Es ist φ surjektiv genau dann, wenn $NH = G$ ist.

Es ist φ injektiv genau dann, wenn $N \cap H = 1$ ist.

Ist $N \cap H = 1$ und $NH = G$, so ist φ ein Isomorphismus. Diesenfalls heißt H ein Komplement *zu N in G, sowie G ein* (inneres) semidirektes Produkt *von N mit H.*

Beweis. Es ist α wohldefiniert, denn für $h \in H$ ist die Abbildung $N \longrightarrow N$, $n \longmapsto hnh^-$ in der Tat ein Automorphismus von N. Es ist α ein Gruppenmorphismus, denn für h, h' wird für $n \in N$ wird $(\alpha(hh'))(n) = {}^{hh'}n = {}^h({}^{h'}n) = (\alpha(h)\circ\alpha(h'))(n)$.

Die Existenz des angegebenen Gruppenmorphismus φ folgt mit Lemma 92, angewandt auf die beiden Inklusionsabbildungen $N \hookrightarrow G$ und $H \hookrightarrow G$.

Es ist φ surjektiv genau dann, wenn $NH = G$ ist.

Es ist φ injektiv genau dann, wenn $\mathrm{Kern}(\varphi) = 1$ ist. Wir haben $\mathrm{Kern}(\varphi) = 1 \overset{!}{\Leftrightarrow} N\cap H = 1$ zu zeigen.

Ad $\Rightarrow$. Sei $\mathrm{Kern}(\varphi) = 1$. Sei $x \in N \cap H$. Dann ist $\varphi(x,x^-) = xx^- = 1$ und also $(x,x^-) = (1,1)$, i.e. $x = 1$. Somit ist $N \cap H = 1$.

Ad $\Leftarrow$. Sei $N \cap H = 1$. Sei $(n,h) \in \mathrm{Kern}(\varphi)$. Dann ist $1 = \varphi(n,h) = nh$, also $n = h^- \in N \cap H = 1$, also $(n,h) = (1,1)$. Somit ist $\mathrm{Kern}(\varphi) = 1$. ▫

Cf. Aufgabe 2.(4).

Bemerkung 94 *Sei G eine Gruppe.*

Sei $N \trianglelefteq G$. Sei H ein Komplement zu N in G. Sei $x \in G$.

(1) *Es ist auch ${}^xH$ ein Komplement zu N in G.*

(2) *Wir haben den Gruppenisomorphismus $\psi : H \xrightarrow{\sim} G/N$, $h \longmapsto hN$.*

Beweis.

Ad (1). Es ist $N\,{}^xH = {}^xN\,{}^xH = {}^x(NH) = G$.

Es ist $N \cap {}^xH = {}^xN \cap {}^xH = {}^x(N \cap H) = 1$.

Ad (2). Es ist ψ ein Gruppenmorphismus. Es ist ψ surjektiv, da für $g \in G$ wegen $G = NH = HN$ es $h \in H$ und $n \in N$ mit $g = hn$ und also mit $gN = hnN = hN$ gibt. Es ist ψ injektiv, da $\mathrm{Kern}(\psi) = H \cap N = 1$ ist. ▫

Beispiel 95

(1) Es hat $\langle (1,2,3) \rangle \trianglelefteq \mathrm{S}_3$ das Komplement $\langle (1,2) \rangle$. So ist S_3 isomorph zum semidirekten Produkt $\langle (1,2,3) \rangle \underset{\alpha}{\rtimes} \langle (1,2) \rangle$, wobei $\alpha : \langle (1,2) \rangle \longrightarrow \mathrm{Aut}(\langle (1,2,3) \rangle)$, $(1,2) \longmapsto ((1,2,3)^i \mapsto {}^{(1,2)}(1,2,3)^i = (1,2,3)^{-i})$, wobei $i \in [0,2]$.

Schreiben wir $\mathrm{C}_3 = \langle\, a \,:\, a^3 \,\rangle$ und $\mathrm{C}_2 = \langle\, b \,:\, b^3 \,\rangle$, so wird mit $\beta : \mathrm{C}_2 \longrightarrow \mathrm{Aut}(\mathrm{C}_3)$, $a \longmapsto (b \mapsto b^-)$ auch

$$\begin{array}{rcl} \mathrm{C}_3 \underset{\beta}{\rtimes} \mathrm{C}_2 & \xrightarrow{\sim} & \mathrm{S}_3 \\ (a^i, b^j) & \longmapsto & (1,2,3)^i \circ (1,2)^j \ , \quad \text{wobei } i \in [0,2] \text{ und } j \in [0,1]. \end{array}$$

Kurz, $\mathrm{S}_3 \simeq \mathrm{C}_3 \rtimes \mathrm{C}_2$.

Beachte, daß $\langle (1,2,3) \rangle$ außer dem Komplement $\langle (1,2) \rangle$ auch das Komplement $\langle (1,3) \rangle$ besitzt.

(2) Es hat $V := \langle \overbrace{(1,2)(3,4)}^{=:a}, \overbrace{(1,3)(2,4)}^{=:b} \rangle \trianglelefteq \mathrm{A}_4$ das Komplement $\langle \overbrace{(1,2,3)}^{=:c} \rangle$. So ist A_4 isomorph zu $V \underset{\alpha}{\rtimes} \langle c \rangle$, wobei $\alpha : \langle c \rangle \longrightarrow \mathrm{Aut}(V)$, $c \longmapsto (a \mapsto {}^ca = ab, b \mapsto {}^cb = a)$.

Kurz, $\mathrm{A}_4 \simeq (\mathrm{C}_2 \times \mathrm{C}_2) \rtimes \mathrm{C}_3$.

(3) Es hat $V := \langle \overbrace{(1,2)(3,4)}^{=:a}, \overbrace{(1,3)(2,4)}^{=:b} \rangle \trianglelefteq \mathrm{S}_4$ das Komplement $\mathrm{S}_3 = \langle \overbrace{(1,2,3)}^{=:c}, \overbrace{(1,2)}^{=:d} \rangle$, denn $V \cap \mathrm{S}_3 = 1$ und $|V||\mathrm{S}_3| = |\mathrm{S}_4|$, woraus $|V\mathrm{S}_3| = |V||\mathrm{S}_3|/|V \cap \mathrm{S}_3| = |\mathrm{S}_4|$ und also $V\mathrm{S}_3 = \mathrm{S}_4$ folgt. So ist S_4 isomorph zu $V \underset{\alpha}{\rtimes} \mathrm{S}_3$, wobei $\alpha : \mathrm{S}_3 \longrightarrow \mathrm{Aut}(V)$, $c \longmapsto (a \mapsto {}^c a = ab, b \mapsto {}^c b = a)$, $d \longmapsto (a \mapsto {}^d a = a, b \mapsto {}^d b = ab)$.

Kurz, $\mathrm{S}_4 \simeq V \rtimes \mathrm{S}_3 \overset{(1)}{\simeq} (\mathrm{C}_2 \times \mathrm{C}_2) \rtimes (\mathrm{C}_3 \rtimes \mathrm{C}_2)$.

(4) Betrachte $\mathrm{D}_8 = \langle\, a, b \,:\, a^4, b^2, (ab)^2 \,\rangle$; cf. Beispiel 56. Es hat $\langle a \rangle \trianglelefteq \mathrm{D}_8$ das Komplement $\langle b \rangle$. So ist D_8 isomorph zu $\langle a \rangle \underset{\alpha}{\rtimes} \langle b \rangle$, wobei $\alpha : \langle b \rangle \longrightarrow \mathrm{Aut}(\langle a \rangle)$, $b \longmapsto (a \mapsto {}^b a = a^-)$.

Kurz, $\mathrm{D}_8 \simeq \mathrm{C}_4 \rtimes \mathrm{C}_2$.

(5) Schreibe $\mathrm{C}_7 = \langle\, c \,:\, c^7 \,\rangle$ und $\mathrm{C}_3 = \langle\, x \,:\, x^3 \,\rangle$. Es ist

$$\begin{array}{rcl} \mathrm{Aut}(\mathrm{C}_7) \;=\; \{\, \alpha_i : c \mapsto c^i \,:\, i \in [1,6] \,\} & \xrightarrow{\sim} & \mathrm{U}(\mathbf{Z}/7\mathbf{Z}) \;=\; \langle 3 + 7\mathbf{Z} \rangle \;\simeq\; \mathrm{C}_6 \\ \alpha_i & \longmapsto & i + 7\mathbf{Z}\,. \end{array}$$

Also ist $\mathrm{Aut}(\mathrm{C}_7) = \langle \alpha_3 \rangle$ zyklisch von Ordnung 6.

Es ist $\beta : \mathrm{C}_3 \longrightarrow \mathrm{Aut}(\mathrm{C}_7)$, $x \longmapsto \alpha_3^2 = \alpha_2$ ein Gruppenmorphismus. Wir können das semidirekte Produkt $G := \mathrm{C}_7 \underset{\beta}{\rtimes} \mathrm{C}_3$ bilden. Darin ist

$$(c^i, x^k)(c^j, x^\ell) \;=\; (c^i \cdot (\beta(x^k))(c^j), x^k \cdot x^\ell) \;=\; (c^{i+j\cdot 2^k},\, x^{k+\ell})$$

für $i,\, k,\, j,\, \ell \in \mathbf{Z}_{\geqslant 0}$.

(6) Schreibe $\mathrm{C}_4 = \langle\, a \,:\, a^4 \,\rangle$. Die Untergruppen von C_4 sind 1, $\langle a^2 \rangle$ und C_4.

Es hat $\langle a^2 \rangle \trianglelefteq \mathrm{C}_4$ kein Komplement.

Lemma 96 *Sei $N \overset{i}{\rightarrowtail} G \overset{r}{\twoheadrightarrow} H$ eine kurz exakte Sequenz von Gruppen.*

Sei $H \overset{s}{\longrightarrow} G$ ein Gruppenmorphismus mit $r \circ s = \mathrm{id}_H$.

Wir haben den Gruppenmorphismus $\beta : H \longrightarrow \mathrm{Aut}(i(N))$, $h \longmapsto (i(n) \mapsto {}^{s(h)}(i(n)))$, da $i(N) \trianglelefteq G$.

Schreibe $i' := i|^{i(N)} : N \xrightarrow{\sim} i(N)$. Somit ist $i(n) := i'(n)$ für $n \in N$. Wir haben den Gruppenisomorphismus $\gamma : \mathrm{Aut}(i(N)) \xrightarrow{\sim} \mathrm{Aut}(N)$, $w \longmapsto i'^- \circ w \circ i'$.

Setze $\alpha := \gamma \circ \beta : H \longrightarrow \mathrm{Aut}(N)$.

(1) *Es ist $s(H)$ ein Komplement zum Normalteiler $i(N)$ in G.*

(2) *Wir haben den Gruppenisomorphismus*

$$\begin{array}{rcl} N \underset{\alpha}{\rtimes} H & \overset{f}{\xrightarrow{\sim}} & G \\ (n, h) & \longmapsto & i(n) \cdot s(h) \end{array}$$

(3) *Folgendes Diagramm kommutiert.*

$$\begin{array}{ccccc} N & \xrightarrow{\iota} & N \underset{\alpha}{\rtimes} H & \xrightarrow{\rho} & H \\ \downarrow{\scriptstyle \mathrm{id}_N} & & \downarrow{\scriptstyle \wr f} & & \downarrow{\scriptstyle \mathrm{id}_H} \\ N & \xrightarrow{i} & G & \xrightarrow{r} & H \end{array}$$

Beweis.

Ad (1). Wir zeigen $i(N)s(H) \stackrel{!}{=} G$. Für $g \in G$ ist $g = (g \cdot sr(g)^-) \cdot sr(g)$ und $r(g \cdot sr(g)^-) = r(g) \cdot rsr(g)^- = 1$, also $g \cdot sr(g)^- = i(n)$ für ein $n \in N$.

Wir zeigen $i(N) \cap s(H) = 1$. Sei $g \in i(N) \cap s(H)$. Schreibe $g = s(h)$. Da $g \in i(N)$ liegt, ist $r(g) = 1$. Insgesamt ist also $g = s(h) = srs(h) = sr(g) = s(1) = 1$.

Ad (2). Es ist $i({}^h n) = i((\alpha(h))(n)) = i((\gamma(\beta(h)))(n)) = i((i'^- \circ \beta(h) \circ i'^-)(n)) = i'(i'^-({}^{s(h)}(i(n)))) = {}^{s(h)}(i(n))$ für $h \in H$ und $n \in N$. Die Existenz des angegebenen Gruppenmorphismus f folgt also aus der universellen Eigenschaft in Lemma 92, angewandt auf i und s.

Es ist f injektiv, da für $n \in N$ und $h \in H$ aus $i(n) \cdot s(h) = 1$ auch $i(n^-) = s(h) \in i(N) \cap s(H) \stackrel{(1)}{=} 1$ folgt, mithin $n = 1$ und $h = r(s(h)) = r(1) = 1$.

Es ist f surjektiv, da $\mathrm{Im}(f) = i(N) \cdot s(H) = G$ nach (1).

Ad (3). Es ist $f \circ \iota = i$, da $f(\iota(n)) = f(n, 1) = i(n)$ für $n \in N$. Es ist $r \circ f = \rho$, da $r(f(n, h)) = r(i(n) \cdot s(h)) = h = \rho(n, h)$ für $(n, i) \in N \underset{\alpha}{\rtimes} H$. ▫

Definition 97 Sei H eine Gruppe. Sei $m \geqslant 1$. Sei $\beta : H \longrightarrow \mathrm{S}_m$ ein Gruppenmorphismus. Schreibe $(\beta(h))(i) =: h \cdot i = hi$ für $h \in H$ und $i \in [1, m]$.

Sei K eine Gruppe. Setze

$$\begin{array}{ccc} H & \xrightarrow{\alpha} & \mathrm{Aut}(K^{\times m}) \\ h & \longmapsto & ((k_i)_i \mapsto {}^h(k_i)_i = (\alpha(h))(k_i)_i := (k_{h^-i})_i) \ . \end{array}$$

Sei

$$K \wr_\beta H \ := \ K^{\times m} \underset{\alpha}{\rtimes} H$$

das *Kranzprodukt* von K mit H vermittels β. Wir schreiben oft auch kurz $K \wr H := K \wr_\beta H$.

Es ist α in der Tat ein Gruppenmorphismus, denn für h, $h' \in H$ und $(k_i)_i \in K^m$ folgt

$$(\alpha(h) \circ \alpha(h'))((k_i)_i) \ = \ (\alpha(h))(k_{h'-i})_i \ = \ (k_{h'-h^-i})_i \ = \ (k_{(hh')^-i})_i \ = \ (\alpha(hh'))((k_i)_i) \ ,$$

und also $\alpha(h) \circ \alpha(h') = \alpha(hh')$.

Beispiel 98

Sei $N := \langle (1,2,3),\ (4,5,6),\ (7,8,9) \rangle \leqslant \mathrm{S}_9$. Sei $H := \langle (1,4,7)(2,5,8)(3,6,9) \rangle \leqslant \mathrm{S}_9$.

Schreibe $\mathrm{C}_3 = \langle\, c \,:\, c^3 \,\rangle$. Dank Aufgabe 2.(3) haben wir den injektiven Gruppenmorphismus

$$\begin{array}{rcl} \mathrm{C}_3^{\times 3} & \xrightarrow{u} & \mathrm{S}_9 \\ (c^{i_1}, c^{i_2}, c^{i_3}) & \longmapsto & (1,2,3)^{i_1}(4,5,6)^{i_2}(7,8,9)^{i_3}\ , \quad \text{wobei } (i_1\,,\, i_2\,,\, i_3) \in \mathbf{Z}^{\times 3}. \end{array}$$

Wir haben den injektiven Gruppenmorphismus

$$\begin{array}{rcl} \mathrm{C}_3 & \xrightarrow{v} & \mathrm{S}_9 \\ c^k & \longmapsto & ((1,4,7)(2,5,8)(3,6,9))^k\ , \quad \text{wobei } k \in \mathbf{Z}. \end{array}$$

Wir haben den Gruppenmorphismus $\beta : \mathrm{C}_3 \longrightarrow \mathrm{S}_3\,,\ c^k \longmapsto (1,2,3)^k$, wobei $k \in \mathbf{Z}$; so wird $[1,3]$ zu einer C_3-Menge.

Es ist

$$\begin{array}{rcl} {}^{v(c)}u(c^{i_1}, c^{i_2}, c^{i_3}) & = & {}^{(1,4,7)(2,5,8)(3,6,9)}((1,2,3)^{i_1}(4,5,6)^{i_2}(7,8,9)^{i_3}) \\ & = & (4,5,6)^{i_1}(7,8,9)^{i_2}(1,2,3)^{i_3} \\ & = & (1,2,3)^{i_3}(4,5,6)^{i_1}(7,8,9)^{i_2} \\ & = & u(c^{i_3}, c^{i_1}, c^{i_2}) \\ & = & u(c^{i_{c^-\cdot 1}}, c^{i_{c^-\cdot 2}}, c^{i_{c^-\cdot 3}}) \\ & = & {}^{c}u(c^{i_1}, c^{i_2}, c^{i_3}) \end{array}$$

und damit auch

$${}^{v(c^k)}u(c^{i_1}, c^{i_2}, c^{i_3}) \ = \ {}^{c^k}u(c^{i_1}, c^{i_2}, c^{i_3})$$

für $k \in \mathbf{Z}$ im Sinne von Definition 97. Die universelle Eigenschaft des semidirekten Produkts aus Lemma 92 gibt also den Gruppenmorphismus

$$\mathrm{C}_3 \wr_\beta \mathrm{C}_3 \ = \ \mathrm{C}_3^{\times 3} \underset{\alpha}{\rtimes} \mathrm{C}_3 \quad \xrightarrow{f} \quad \mathrm{S}_9\ .$$

Dieser ist injektiv, da $N \cap H = 1$. Somit ist

$$\mathrm{C}_3 \wr_\beta \mathrm{C}_3 \xrightarrow[\sim]{f|^{NH}} NH \ = \ \langle (1,2,3),\ (4,5,6),\ (7,8,9),\ (1,4,7)(2,5,8)(3,6,9) \rangle \ \in \ \mathrm{Syl}_3(\mathrm{S}_9)\ ,$$

denn $3^3 \cdot 3 \ = \ |\mathrm{C}_3 \wr_\beta \mathrm{C}_3| \ = \ |NH| = |\mathrm{S}_9|[3]$.

Kurz, die 3-Sylowgruppen von S_9 sind von der Form $\mathrm{C}_3 \wr \mathrm{C}_3$.

3.4 Schur-Zassenhaus

3.4.1 Die ersten beiden Cohomologiegruppen

Wir geben uns mit einer abgekürzten Version der Cohomologietheorie von Gruppen zufrieden. Cf. auch [**5**].

Sei H eine Gruppe.

Sei A eine abelsche Gruppe. Sei $\alpha : H \longrightarrow \mathrm{Aut}(A)$ ein Gruppenmorphismus.

Wir schreiben $(\alpha(h))(a) =: {}^h a$ für $h \in H$ und $a \in A$.

Definition 99 Sei

$$\mathrm{Z}^1(H,A) := \{\, d : H \longrightarrow A \,:\, \text{es ist } {}^h d(h') \cdot d(hh')^- \cdot d(h) = 1 \text{ für } h,\, h' \in H \,\}$$
die Menge der *Derivationen* oder 1-*Cozykel*,

$$\mathrm{B}^1(H,A) := \{\, d_b : H \longrightarrow A,\ h \longmapsto {}^h b \cdot b^- \,:\, b \in A \,\}$$
die Menge der *inneren Derivationen* oder 1-*Coränder*,

$$\mathrm{Z}^2(H,A) := \{\, z : H \times H \longrightarrow A \,:\, \text{es ist } {}^h z(h',h'') \cdot z(hh',h'')^- \cdot z(h,h'h'') \cdot z(h,h')^- = 1 \text{ für } h,\, h',\, h'' \in H \,\}$$
die Menge der 2-*Cozykel*,

$$\mathrm{B}^2(H,A) := \{\, z_c : H \times H \longrightarrow A,\ (h,h') \longmapsto {}^h c(h') \cdot c(hh')^- \cdot c(h) \,:\, c : H \longrightarrow A \,\}$$
die Menge der 2-*Coränder*

von H mit Koeffizienten in A bezüglich α.

Bemerkung 100 Ist M eine Menge und B eine Gruppe, dann ist die Menge ${}_{\mathrm{Abb}}(M,B)$ der Abbildungen von M nach B eine abelsche Gruppe unter punktweiser Multiplikation, i.e. für $u,\, v \in {}_{\mathrm{Abb}}(M,B)$ setzen wir

$$u \cdot v \,:\, M \longrightarrow B\,, \quad m \longmapsto (uv)(m) \,=\, (u \cdot v)(m) \,:=\, u(m) \cdot v(m)\,.$$

Das Einselement ist gegeben durch $1 : M \longrightarrow B$, $m \longmapsto 1$. Das zu $u \in {}_{\mathrm{Abb}}(M,B)$ inverse Element ist gegeben durch $u^- : M \longrightarrow B$, $m \longmapsto u^-(m) := u(m)^-$.

Vorsicht, mit u^- ist hierbei nicht die Umkehrabbildung gemeint.

Ist B abelsch, dann ist ${}_{\mathrm{Abb}}(M,B)$ abelsch.

Bemerkung 101 Ist $d \in \mathrm{Z}^1(H,A)$, dann ist ${}^1 d(1) \cdot d(1 \cdot 1)^- \cdot d(1) = 1$, also $d(1) = 1$. Somit ist für $h \in H$ auch $1 = d(h^- h) = {}^{h^-} d(h) \cdot d(h^-)$ und somit $d(h^-) = ({}^{h^-} d(h))^-$.

Bemerkung 102

(1) *Es ist* $\mathrm{B}^1(H,A) \leqslant \mathrm{Z}^1(H,A) \leqslant {}_{\mathrm{Abb}}(H,A)$.

(2) *Es ist* $\mathrm{B}^2(H,A) \leqslant \mathrm{Z}^2(H,A) \leqslant {}_{\mathrm{Abb}}(H \times H, A)$.

Beweis.

Ad (1). Es ist 1 eine Derivation. Sind d und $\tilde{d}$ gegebene Derivationen, dann ist auch $d\tilde{d}^-$ eine Derivation, da

$$\begin{aligned} {}^h(d\tilde{d}^-)(h') \cdot (d\tilde{d}^-)(hh')^- \cdot (d\tilde{d}^-)(h) &= {}^h(d(h') \cdot \tilde{d}(h')^-) \cdot (d(hh') \cdot \tilde{d}(hh')^-)^- \cdot d(h) \cdot \tilde{d}(h)^- \\ &= {}^h d(h') \cdot d(hh')^- \cdot d(h) \cdot {}^h\tilde{d}(h') \cdot \tilde{d}(hh')^- \cdot \tilde{d}(h) \\ &= 1 \cdot 1 \,=\, 1 \end{aligned}$$

ist für $h,\, h' \in H$. Somit ist $\mathrm{Z}^1(H,A) \leqslant {}_{\mathrm{Abb}}(H,A)$.

Es ist $d_1 = 1$. Sind $b,\, \tilde{b} \in A$ gegeben, so wird

$$\begin{aligned}(d_b d_{\tilde{b}}^-)(h) &= d_b(h) \cdot d_{\tilde{b}}(h)^- \\ &= {}^h b \cdot b^- \cdot ({}^h\tilde{b} \cdot \tilde{b}^-)^- \\ &= {}^h(b\tilde{b}^-) \cdot (b\tilde{b}^-)^- \\ &= d_{b\tilde{b}^-}(h)\end{aligned}$$

für $h \in H$, i.e. $d_b d_{\tilde{b}}^- = d_{b\tilde{b}^-}$. Somit ist $\mathrm{B}^1(H,A) \leqslant {}_{\mathrm{Abb}}(H,A)$.

Sei $b \in A$ gegeben. Es ist

$$\begin{aligned}{}^h d_b(h') \cdot d_b(hh')^- \cdot d_b(h) &= {}^h({}^{h'}b \cdot b^-) \cdot ({}^{hh'}b \cdot b^-)^- \cdot ({}^h b \cdot b^-) \\ &= {}^{hh'}b \cdot {}^h b^- \cdot {}^{hh'}b^- \cdot b \cdot {}^h b \cdot b^- \\ &= 1\,.\end{aligned}$$

Also ist $d_b \in \mathrm{Z}^1(H,A)$. Somit ist $\mathrm{B}^1(H,A) \leqslant \mathrm{Z}^1(H,A)$.

Ad (2). Es ist 1 ein 2-Cozykel. Sind z und $\tilde{z}$ gegebene 2-Cozykel, dann ist auch $z\tilde{z}^-$ ein 2-Cozykel, da

$$\begin{aligned}&{}^h(z\tilde{z}^-)(h',h'') \cdot (z\tilde{z}^-)(hh',h'')^- \cdot (z\tilde{z}^-)(h,h'h'') \cdot (z\tilde{z}^-)(h,h')^- \\ =\;& {}^h(z(h',h'') \cdot \tilde{z}(h,h')^-))\cdot (z(hh',h'') \cdot \tilde{z}(hh',h'')^-)^- \cdot z(h,h'h'') \cdot \tilde{z}(h,h'h'')^- \cdot (z(h,h') \cdot \tilde{z}(h,h')^-)^- \\ =\;& {}^h z(h',h'') \cdot z(hh',h'')^- \cdot z(h,h'h'') \cdot z(h,h')^- \cdot {}^h\tilde{z}(h',h'') \cdot \tilde{z}(hh',h'')^- \cdot \tilde{z}(h,h'h'') \cdot \tilde{z}(h,h')^- \\ =\;& 1 \cdot 1 \;=\; 1\end{aligned}$$

ist für $h,\, h',\, h'' \in H$. Somit ist $\mathrm{Z}^2(H,A) \leqslant {}_{\mathrm{Abb}}(H \times H, A)$.

Es ist $z_1 = 1$. Sind $c,\, \tilde{c} : H \longrightarrow A$ gegeben, so wird

$$\begin{aligned}(z_c z_{\tilde{c}}^-)(h,h') &= z_c(h,h') \cdot z_{\tilde{c}}(h,h')^- \\ &= {}^h c(h') \cdot c(hh')^- \cdot c(h) \cdot ({}^h\tilde{c}(h') \cdot \tilde{c}(hh')^- \cdot \tilde{c}(h))^- \\ &= {}^h(c(h') \cdot \tilde{c}(h')^-) \cdot (c(hh') \cdot \tilde{c}(hh')^-)^- \cdot c(h) \cdot \tilde{c}(h)^- \\ &= {}^h(c\tilde{c}^-)(h') \cdot (c\tilde{c}^-)(hh')^- \cdot (c\tilde{c}^-)(h) \\ &= z_{c\tilde{c}^-}(h,h')\end{aligned}$$

für $h,\, h' \in H$, i.e. $z_c z_{\tilde{c}}^- = z_{c\tilde{c}^-}$. Somit ist $\mathrm{B}^2(H,A) \leqslant {}_{\mathrm{Abb}}(H \times H, A)$.

Sei $c : H \longrightarrow A$ gegeben. Es ist

$$\begin{aligned}&{}^h z_c(h',h'') \cdot z_c(hh',h'')^- \cdot z_c(h,h'h'') \cdot z_c(h,h')^- \\ =\;& {}^h({}^{h'}c(h'') \cdot c(h'h'')^- \cdot c(h')) \cdot ({}^{hh'}c(h'') \cdot c(hh'h'')^- \cdot c(hh'))^- \\ &\cdot ({}^h c(h'h'') \cdot c(hh'h'')^- \cdot c(h))({}^h c(h') \cdot c(hh')^- \cdot c(h))^- \\ =\;& {}^{hh'}c(h'') \cdot {}^h c(h'h'')^- \cdot {}^h c(h') \cdot {}^{hh'}c(h'')^- \cdot c(hh'h'') \cdot c(hh')^- \\ &\cdot {}^h c(h'h'') \cdot c(hh'h'')^- \cdot c(h) \cdot {}^h c(h')^- \cdot c(hh') \cdot c(h)^- \\ =\;& 1\,.\end{aligned}$$

Also ist $z_c \in \mathrm{Z}^2(H,A)$. Somit ist $\mathrm{B}^2(H,A) \leqslant \mathrm{Z}^2(H,A)$. ▫

Definition 103 Sei

$$\begin{aligned} \mathrm{H}^1(H,A) &:= \mathrm{Z}^1(H,A)/\mathrm{B}^1(H,A) \quad \text{die } \textit{erste Cohomologiegruppe}, \\ \mathrm{H}^2(H,A) &:= \mathrm{Z}^2(H,A)/\mathrm{B}^2(H,A) \quad \text{die } \textit{zweite Cohomologiegruppe} \end{aligned}$$

von H mit Koeffizienten in A bezüglich α.

Bemerkung 104 Sei $\alpha = ! : H \longrightarrow \mathrm{Aut}(A)$, i.e. ${}^h a = a$ für $h \in H$ und $a \in A$.

(1) Eine Derivation von H mit Koeffizienten in A bezüglich ! ist ein Gruppenmorphismus von H nach A.

Für $b \in A$ ist $d_b(h) = {}^h b \cdot b^- = 1$ für $h \in H$, also $d_b = 1$. Somit ist $\mathrm{B}^1(H,A) = 1$.

Insgesamt ist $\mathrm{H}^1(H,A) = \{\, d : H \longrightarrow A \,:\, d \text{ ist Gruppenmorphismus} \,\}$.

(2) Eine Abbildung $z : H \times H \longrightarrow A$ ist ein 2-Cozykel von H mit Koeffizienten in A bezüglich ! genau dann, wenn

$$z(h', h'') \cdot z(h, h'h'') \;=\; z(hh', h'') \cdot z(h, h')$$

ist für h, h', $h'' \in H$.

Beispiel 105 Sei p prim. Sei $H = \mathrm{C}_p = \langle\, h \,:\, h^p \,\rangle$. Sei $A = \mathrm{C}_p = \langle\, a \,:\, a^p \,\rangle$.

Sei $\alpha = ! : H \longrightarrow \mathrm{Aut}(A)$, i.e. ${}^h a = a$.

(1) Es ist $d_{a^j}(h^i) = {}^{h^i}(a^j) \cdot (a^j)^- = 1$ für $i,\, j \in \mathbf{Z}$ und also $\mathrm{B}^1(H,A) = 1$.

Da eine Derivation $d : H \longrightarrow A$ gerade ein Gruppenmorphismus ist, erhalten wir $\mathrm{Z}^1(H,A) = \{\, d_i : H \longrightarrow A \,:\, d_i(h) := a^i \,\} = \langle d_1 \rangle \simeq \mathrm{C}_p$.

Folglich ist $\mathrm{H}^1(H,A) \simeq \mathrm{C}_p$.

(2) Sei $z \in \mathrm{Z}^2(H,A)$. Schreibe $z(h^i, h^j) =: a^{\zeta(i,j)}$ mit $\zeta(i,j) \in [0, p-1]$ für $i,\, j \in \mathbf{Z}$. Dann ist $\zeta(j,k) - \zeta(i+j,k) + \zeta(i,j+k) - \zeta(i,j) \equiv_p 0$ für $i,\, j,\, k \in \mathbf{Z}$. Insbesondere ist $\zeta(0,0) - \zeta(i,0) + \zeta(i,0) - \zeta(i,0) = 0$ und also $\zeta(0,0) = \zeta(i,0)$ für $i \in \mathbf{Z}$ und genauso $\zeta(0,0) = \zeta(0,k)$ für $k \in \mathbf{Z}$.

Sei nun $p = 2$.

Der Gruppenmorphismus

$$\begin{array}{rccc} \varphi \;:\; \mathrm{Z}^2(H,A) & \longrightarrow & \mathrm{C}_2 \;\times\; \mathrm{C}_2 \\ z & \longmapsto & (a^{\zeta(0,0)} \;,\; a^{\zeta(1,1)-\zeta(0,0)}) \end{array}$$

ist bijektiv, da zum einen jede konstante Abbildung von $H \times H$ nach A in $\mathrm{Z}^2(H,A)$ liegt und zum anderen die Bedingung $\zeta(j,k) - \zeta(i+j,k) + \zeta(i,j+k) - \zeta(i,j) \equiv_2 0$

an ζ unter Berücksichtigung obiger Bemerkung redundant ist für $i = 0$ oder $j = 0$ oder $k = 0$ oder $(i, j, k) = (1, 1, 1)$.

Sei $c : H \longrightarrow A$, $h^i \longrightarrow c(h^i) =: a^{\gamma(i)}$ mit $\gamma(i) \in \{0, 1\}$ für $i \in \mathbf{Z}$. Es ist $z_c(h^i, h^j) = a^{\gamma(j)-\gamma(i+j)+\gamma(i)}$ für $i,\ j \in \mathbf{Z}$. Hierbei ist $\gamma(0)-\gamma(0+0)+\gamma(0) \equiv_2 \gamma(0)$ und $\gamma(1) - \gamma(1 + 1) + \gamma(1) \equiv_2 \gamma(0)$ und also

$$\varphi(\mathrm{B}^2(H, A)) \ = \ \mathrm{C}_2 \times 1 \ .$$

Es folgt $\mathrm{H}^2(H, A) \simeq (\mathrm{C}_2 \times \mathrm{C}_2)/(\mathrm{C}_2 \times 1) \simeq \mathrm{C}_2$.

(3) Sei e.g. $H = 1$. Es ist $\mathrm{H}^1(1, A) = 1$; cf. Bemerkung 104.(1).

Es ist $\mathrm{H}^2(1, A) = 1$. Für eine Abbildung $c : 1 \longrightarrow A$ wird $z_c(1, 1) = c(1)$, sodaß $\mathrm{B}^2(1, A)$ ist die Menge aller Abbildungen von 1×1 nach A ist, woraus $\mathrm{B}^2(1, A) = \mathrm{Z}^2(1, A) = {}_{\mathrm{Abb}}(1 \times 1, A)$ folgt.

Lemma 106 *Sei $K \leqslant H$ eine Untergruppe von endlichem Index $[H : K]$.*

Sei $1 \in T \subseteq H$ mit $\bigsqcup_{t\in T} Kt = H$. Für $h \in H$ schreiben wir $h = \kappa(h) \cdot \tau(h)$ mit $\kappa(h) \in K$ und $\tau(h) \in T$.

Wir bilden die Gruppen Z^i, B^i und H^i für H bezüglich $\alpha : H \longrightarrow \mathrm{Aut}(A)$, für K bezüglich $\alpha|_K : K \longrightarrow \mathrm{Aut}(A)$, wobei $i \in \{1, 2\}$.

(1) *Wir haben die Gruppenmorphismen*

$$\begin{array}{rcl} \mathrm{Z}^1(K, A) & \longleftrightarrow & \mathrm{Z}^1(H, A) \\ d & \longmapsto & \left(d\restriction_K^H : H \to A, h \mapsto \prod_{t\in T} {}^{t^-}d(\,\kappa(th)\,) \right) \\ \tilde{d}|_K & \longleftarrow\!\shortmid & \tilde{d} \end{array}$$

(2) *Wir haben die Gruppenmorphismen*

$$\begin{array}{rcl} \mathrm{H}^1(K, A) & \longleftrightarrow & \mathrm{H}^1(H, A) \\ d\mathrm{B}^1(K, A) & \overset{\mathrm{Cores}\uparrow_K^H}{\longmapsto} & d\restriction_K^H \mathrm{B}^1(H, A) \\ \tilde{d}|_K \mathrm{B}^1(K, A) & \overset{\mathrm{Res}\downarrow_K^H}{\longleftarrow\!\shortmid} & \tilde{d}\mathrm{B}^1(H, A) \ . \end{array}$$

Es ist

$$(\mathrm{Cores}\uparrow_K^H \circ \mathrm{Res}\downarrow_K^H)(\tilde{d}\mathrm{B}^1(H, A)) \ = \ (\tilde{d}\mathrm{B}^1(H, A))^{[H:K]}$$

für $\tilde{d} \in \mathrm{Z}^1(H, A)$.

(3) *Wir haben die Gruppenmorphismen*

$$\begin{array}{rcl} \mathrm{Z}^2(K, A) & \longleftrightarrow & \mathrm{Z}^2(H, A) \\ z & \longmapsto & \left(z\restriction_K^H : H \times H \to A, (h, h') \mapsto \prod_{t\in T} {}^{t^-}z(\,\kappa(th)\,,\, \kappa(th)^-\kappa(thh')\,) \right) \\ \tilde{z}|_{K\times K} & \longleftarrow\!\shortmid & \tilde{z} \end{array}$$

(4) *Wir haben die Gruppenmorphismen*

$$\begin{array}{rcl} \mathrm{H}^2(K,A) & \longleftrightarrow & \mathrm{H}^2(H,A) \\ z\mathrm{B}^2(K,A) & \overset{\mathrm{Cores}\uparrow_K^H}{\longmapsto} & z\uparrow_K^H \mathrm{B}^2(H,A) \\ \tilde{z}|_{K\times K}\mathrm{B}^2(K,A) & \overset{\mathrm{Res}\downarrow_K^H}{\longmapsto} & \tilde{z}\mathrm{B}^2(H,A)\ . \end{array}$$

Es ist

$$(\mathrm{Cores}\uparrow_K^H \circ \mathrm{Res}\downarrow_K^H)(\tilde{z}\mathrm{B}^2(H,A)) \ = \ (\tilde{z}\mathrm{B}^2(H,A))^{[H:K]}$$

für $\tilde{z} \in \mathrm{Z}^2(H,A)$.

Die Formeln für $\mathrm{Cores}\uparrow_K^H$ habe ich dem Lemma in [**5,** §2.5.4] entnommen.

Beweis. Es ist $\kappa(t) = 1$ und $\tau(t) = t$ für $t \in T$. Es ist $\kappa(k) = k$ und $\tau(k) = 1$ für $k \in K$. Es ist $\kappa(kh) = k\kappa(h)$ und $\tau(kh) = \tau(h)$ für $k \in K$ und $h \in H$.

Ad (1). Liegt $\tilde{d} \in \mathrm{Z}^1(H,A)$, so liegt a fortiori $\tilde{d}|_K \in \mathrm{Z}^1(K,A)$. Da die Abbildung $\tilde{d} \longmapsto \tilde{d}|_K$ punktweise Multiplikation respektiert, ist sie ein Gruppenmorphismus.

Sei umgekehrt $d \in \mathrm{Z}^1(K,A)$ gegeben. Wir haben $d\uparrow_K^H \overset{!}{\in} \mathrm{Z}^1(H,A)$ zu zeigen.

Beachte, daß für $k,\ k' \in K$ sich ${}^k d(k^- k') \cdot d(k')^- \cdot d(k) = 1$ ergibt durch Anwendung der 1-Cozykel-Bedingung auf $(k, k^- k')$.

Seien nun $h,\ h' \in H$ gegeben. Zunächst ist $th^- = \kappa(th^-)\cdot\tau(th^-)$, also $t = \kappa(th^-)\cdot\tau(th^-)h$ und auch $1 = \kappa(t) = \kappa(th^-) \cdot \kappa(\tau(th^-)h)$ für $t \in T$, wegen $\bigsqcup_{t\in T} Kth^- = H$ somit

$$\begin{array}{rcl} {}^h d\uparrow_K^H(h') & = & {}^h\big(\prod_{t\in T} {}^{t^-}d(\,\kappa(th')\,)\big) \\ & = & \prod_{t\in T} {}^{(th^-)^-}d(\,\kappa(th')\,) \\ & = & \prod_{t\in T} {}^{(\kappa(th^-)\cdot\tau(th^-))^-}d(\,\kappa(\kappa(th^-)\cdot\tau(th^-)hh')\,) \\ & = & \prod_{t\in T} {}^{\tau(th^-)^-\cdot\kappa(th^-)^-}d(\,\kappa(th^-)\cdot\kappa(\tau(th^-)hh')\,) \\ & = & \prod_{t\in T} {}^{\tau(th^-)^-\cdot\kappa(\tau(th^-)h)}d(\,\kappa(\tau(th^-)h)^-\kappa(\tau(th^-)hh')\,) \\ & = & \prod_{t\in T} {}^{t^-\cdot\kappa(th)}d(\,\kappa(th)^-\kappa(thh')\,)\ . \end{array}$$

Also wird

$$\begin{array}{rl} & {}^h d\uparrow_K^H(h') \cdot d\uparrow_K^H(hh')^- \cdot d\uparrow_K^H(h) \\ = & \big(\prod_{t\in T} {}^{t^-\cdot\kappa(th)}d(\,\kappa(th)^-\kappa(thh')\,)\big) \cdot \big(\prod_{t\in T} {}^{t^-}d(\,\kappa(thh')\,)\big)^- \cdot \big(\prod_{t\in T} {}^{t^-}d(\,\kappa(th)\,)\big) \\ = & \prod_{t\in T} {}^{t^-}\big({}^{\kappa(th)}d(\,\kappa(th)^-\kappa(thh')\,) \cdot d(\,\kappa(thh')\,)^- \cdot d(\,\kappa(th)\,)\big) \\ = & 1\ . \end{array}$$

Da auch die Abbildung $d \longmapsto d\uparrow_K^H$ punktweise Multiplikation respektiert, ist sie ein Gruppenmorphismus.

Ad (2). Es ist zu zeigen, daß für $\tilde{d} \in \mathrm{B}^1(H,A)$ auch $\tilde{d}|_K \in \mathrm{B}^1(K,A)$ liegt. Wähle ein $\tilde{b} \in A$ mit $\tilde{d}(h) = {}^h\tilde{b} \cdot \tilde{b}^-$ für $h \in H$. Dann ist auch $\tilde{d}(k) = {}^k\tilde{b} \cdot \tilde{b}^-$ für $k \in K$ und also $\tilde{d}|_K \in \mathrm{B}^1(K,A)$.

Es ist zu zeigen, daß für $d \in \mathrm{B}^1(K,A)$ auch $d\uparrow_K^H \in \mathrm{B}^1(H,A)$ liegt. Wähle ein $b \in A$ mit $d(k) = {}^kb \cdot b^-$ für $k \in K$. Sei $h \in H$ gegeben. Da $th = \kappa(th) \cdot \tau(th)$ und also $h\tau(th)^- = t^-\kappa(th)$, wird wegen $\bigsqcup_{t\in T} Kth = H$ somit

$$\begin{aligned} d\uparrow_K^H(h) &= \textstyle\prod_{t\in T} {}^{t^-}d(\,\kappa(th)\,) \\ &= \textstyle\prod_{t\in T} {}^{t^-}\big({}^{\kappa(th)}b \cdot b^-\big) \\ &= \big(\textstyle\prod_{t\in T} {}^{t^-\kappa(th)}b\big) \cdot \big(\textstyle\prod_{t\in T} {}^{t^-}b\big)^- \\ &= {}^h\big(\textstyle\prod_{t\in T} {}^{\tau(th)^-}b\big) \cdot \big(\textstyle\prod_{t\in T} {}^{t^-}b\big)^- \\ &= {}^h\big(\textstyle\prod_{t\in T} {}^{t^-}b\big) \cdot \big(\textstyle\prod_{t\in T} {}^{t^-}b\big)^- \\ &= {}^h\tilde{b} \cdot \tilde{b}^- \,, \end{aligned}$$

wobei $\tilde{b} := \prod_{t\in T} {}^{t^-}b \in A$.

Sei $\tilde{d} \in \mathrm{Z}^1(H,A)$. Es bleibt $(\mathrm{Cores}\uparrow_K^H \circ \mathrm{Res}\downarrow_K^H)(\tilde{d}\mathrm{B}^1(H,A)) \stackrel{!}{=} (\tilde{d}\mathrm{B}^1(H,A))^{[H:K]}$ zu zeigen.

Sei $h \in H$ gegeben. Dann wird $th = \kappa(th) \cdot \tau(th)$, also

$${}^t\tilde{d}(h) \cdot \tilde{d}(t) \;=\; \tilde{d}(th) \;=\; \tilde{d}(\kappa(th) \cdot \tau(th)) \;=\; {}^{\kappa(th)}\tilde{d}(\tau(th)) \cdot \tilde{d}(\kappa(th)) \,.$$

Dank $\bigsqcup_{t\in T} Kth = H$ wird also

$$\begin{aligned} \tilde{d}|_K\uparrow_K^H(h) &= \textstyle\prod_{t\in T} {}^{t^-}\tilde{d}(\,\kappa(th)\,) \\ &= \textstyle\prod_{t\in T} \big(\tilde{d}(h) \cdot ({}^{t^-\kappa(th)}\tilde{d}(\tau(th)))^- \cdot {}^{t^-}\tilde{d}(t)\big) \\ &= \tilde{d}(h)^{|T|} \cdot \big(\textstyle\prod_{t\in T} {}^{h\tau(th)^-}\tilde{d}(\tau(th))\big)^- \cdot \big(\textstyle\prod_{t\in T} {}^{t^-}\tilde{d}(t)\big) \\ &= \tilde{d}(h)^{|T|} \cdot {}^h\big(\textstyle\prod_{t\in T} {}^{\tau(th)^-}\tilde{d}(\tau(th))\big)^- \cdot \big(\textstyle\prod_{t\in T} {}^{t^-}\tilde{d}(t)\big) \\ &= \tilde{d}(h)^{|T|} \cdot {}^h\big(\textstyle\prod_{t\in T} {}^{t^-}(\tilde{d}(t)^-)\big) \cdot \big(\textstyle\prod_{t\in T} {}^{t^-}(\tilde{d}(t)^-)\big)^- \\ &= \tilde{d}(h)^{[H:K]} \cdot {}^h\tilde{b} \cdot \tilde{b}^- \end{aligned}$$

wobei $\tilde{b} := \prod_{t\in T} {}^{t^-}(\tilde{d}(t)^-) \in A$.

Die Abbildung $\mathrm{Cores}\uparrow_K^H$ auf H^1 hängt übrigens nicht von der Wahl von T ab.

Sei hierzu $T' = \{\, k_t t \,:\, t \in T \,\}$ mit $k_t \in K$ für $t \in T$ gewählt. Für $h \in H$ sei $h =: \kappa'(h) \cdot \tau'(h)$ mit $\kappa'(h) \in K$ und $\tau'(h) \in T'$. Dann wird $\kappa'(h) = \kappa'(\kappa(h)\cdot\tau(h)) = \kappa'(\kappa(h)k^-_{\tau(h)} \cdot k_{\tau(h)}\tau(h)) = \kappa(h)k^-_{\tau(h)}$, da $\kappa(h)k^-_{\tau(h)} \in K$ und $k_{\tau(h)}\tau(h) \in T'$.

Sei $d \in \mathrm{Z}^1(K,A)$. Es wird für $h \in H$ auch $\bigsqcup_{t\in T} Kth = H$ und also, dank Bemerkung 101,

$$\begin{aligned}
\textstyle\prod_{t'\in T'} {}^{t'^-}d(\kappa'(t'h)) &= \textstyle\prod_{t\in T} {}^{t^-k_t^-}d(\kappa'(k_t th)) \\
&= \textstyle\prod_{t\in T} {}^{t^-k_t^-}d(k_t\kappa'(th)) \\
&= \textstyle\prod_{t\in T} {}^{t^-k_t^-}d(k_t\kappa(th)k_{\tau(th)}^-) \\
&= \textstyle\prod_{t\in T} {}^{t^-k_t^-}\big({}^{k_t\kappa(th)}d(k_{\tau(th)}^-)\cdot {}^{k_t}d(\kappa(th))\cdot d(k_t)\big) \\
&= \textstyle\prod_{t\in T} {}^{t^-}\big({}^{\kappa(th)}d(k_{\tau(th)}^-)\cdot d(\kappa(th))\cdot {}^{k_t^-}d(k_t)\big) \\
&= \big(\textstyle\prod_{t\in T} {}^{t^-\kappa(th)}d(k_{\tau(th)}^-)\big)\cdot\big(\textstyle\prod_{t\in T} {}^{t^-}d(\kappa(th))\big)\cdot\big(\textstyle\prod_{t\in T} {}^{t^-k_t^-}d(k_t)\big) \\
&= \big(\textstyle\prod_{t\in T} {}^{h\tau(th)^-}d(k_{\tau(th)}^-)\big)\cdot\big(\textstyle\prod_{t\in T} {}^{t^-k_t^-}d(k_t)\big)\cdot\big(\textstyle\prod_{t\in T} {}^{t^-}d(\kappa(th))\big) \\
&= {}^{h}\big(\textstyle\prod_{t\in T} {}^{\tau(th)^-k_{\tau(th)}^-}d(k_{\tau(th)})\big)^-\cdot\big(\textstyle\prod_{t\in T} {}^{t^-k_t^-}d(k_t)\big)\cdot\big(\textstyle\prod_{t\in T} {}^{t^-}d(\kappa(th))\big) \\
&= {}^{h}\big(\textstyle\prod_{t\in T} {}^{t^-k_t^-}d(k_t)\big)^-\cdot\big(\textstyle\prod_{t\in T} {}^{t^-k_t^-}d(k_t)\big)\cdot\big(\textstyle\prod_{t\in T} {}^{t^-}d(\kappa(th))\big) \\
&= {}^{h}\tilde{b}\cdot\tilde{b}^-\cdot\big(\textstyle\prod_{t\in T} {}^{t^-}d(\kappa(th))\big)\,,
\end{aligned}$$

wobei $\tilde{b} := \big(\prod_{t\in T} {}^{t^-k_t^-}d(k_t)\big)^- \in A$.

Ad (3). Siehe Aufgabe 47.(1).

Ad (4). Siehe Aufgabe 47.(2).

3.4.2 Schur

Sei H eine Gruppe. Sei A eine abelsche Gruppe.

Lemma 107 (und Definition)

Sei $A \overset{i}{\bullet\!\!\rightarrow} G \overset{r}{\twoheadrightarrow} H$ eine kurz exakte Sequenz von Gruppen.

Sei $\beta : H \longrightarrow \mathrm{Aut}(i(A))$, $h \longmapsto (\beta(h) : i(a) \mapsto {}^{g}i(a))$, wobei $g \in G$ mit $r(g) = h$ gewählt werde. Es ist β ein Gruppenmorphismus.

Sei $i' := i|^{i(A)} : A \xrightarrow{\sim} i(A)$. Sei $\gamma : \mathrm{Aut}(i(A)) \longrightarrow \mathrm{Aut}(A)$, $\varphi \longmapsto i'^- \circ \varphi \circ i'$.

Es ist auch $\alpha := \gamma \circ \beta : H \longrightarrow \mathrm{Aut}(A)$ ein Gruppenmorphismus. Wir schreiben oft $(\alpha(h))(a) =: {}^{h}a$ für $h \in H$ und $a \in A$; es wird

$$i({}^{h}a) \;=\; {}^{g}i(a)$$

für jedes $g \in G$ mit $r(g) = h$.

Wir sagen, es ist α von der kurz exakten Sequenz $A \overset{i}{\bullet\!\!\rightarrow} G \overset{r}{\twoheadrightarrow} H$ induziert.

Beweis. Für die Wohldefiniertheit der Abbildung $\alpha(h)$ seien $g, \tilde{g} \in G$ mit $r(g) = r(\tilde{g}) = h$ gegeben. Sei $a \in A$ gegeben. Da $i(A) \trianglelefteq G$, ist ${}^{g}i(a) \in i(A)$.

Wir haben ${}^{g}i(a) \overset{!}{=} {}^{\tilde{g}}i(a)$ zu zeigen. Es ist $r(\tilde{g}^-g) = r(\tilde{g})^- \cdot r(g) = 1$, also $\tilde{g}^-g = i(b)$ für ein $b \in A$. Es wird $g = \tilde{g}\cdot i(b)$ und also

$${}^{g}i(a) \;=\; {}^{\tilde{g}\cdot i(b)}i(a) \;=\; {}^{\tilde{g}}i({}^{b}a) \;=\; {}^{\tilde{g}}i(a)\,,$$

da A abelsch ist.

Es ist $\beta(h)$ ein Automorphismus von $i(A)$ für $h \in H$.

Wir haben zu zeigen, daß β ein Gruppenmorphismus ist. Seien h, $h' \in H$ gegeben. Wir haben $\beta(hh') \stackrel{!}{=} \beta(h) \circ \beta(h')$ zu zeigen. Seien hierzu g, $g' \in G$ mit $r(g) = h$ und $r(g') = h'$ gewählt. Dann ist auch $r(gg') = r(g) \cdot r(g') = hh'$. Somit wird in der Tat

$$(\beta(hh'))(i(a)) \;=\; {}^{gg'}i(a) \;=\; {}^{g}({}^{g'}i(a)) \;=\; (\beta(h) \circ \beta(h'))(i(a))$$

für $a \in A$.

Da γ ein Gruppenmorphismus ist, gilt dies auch für $\alpha = \gamma \circ \beta$. Für $h \in H$, für $g \in G$ mit $r(g) = h$ und für $a \in A$ wird

$$\begin{aligned} i({}^{h}a) \;&=\; i'((\alpha(h))(a)) \;=\; i'(((\gamma \circ \beta)(h))(a)) \\ &=\; i'((i'^{-} \circ \beta(h) \circ i')(a)) \;=\; i'(i'^{-}({}^{g}i(a))) \;=\; {}^{g}i(a)\,. \end{aligned}$$

□

Im Unterschied zur Situation von Lemma 96 ist nun kein Gruppenmorphismus $G \stackrel{s}{\longleftarrow} H$ mit $r \circ s = \mathrm{id}_H$ gegeben, dafür ist nun aber die linksstehende Gruppe abelsch – was ebenfalls die Wohldefiniertheit von α sichert.

Beispiel 108 Sei $A \trianglelefteq G$. Sei $A \overset{i}{\bullet\!\!\rightarrow} G$ die Inklusion $\mathrm{id}_G|_A$. Sei $G \overset{r}{\twoheadrightarrow} G/A$, $g \longmapsto gA$. Dies gibt die kurz exakte Sequenz $A \overset{i}{\bullet\!\!\rightarrow} G \overset{r}{\twoheadrightarrow} G/A$. Diese induziert einen Gruppenmorphismus $\alpha : G/A \longrightarrow \mathrm{Aut}(A)$; cf. Lemma 107.

Lemma 109 *Sei $A \overset{i}{\bullet\!\!\rightarrow} G \overset{r}{\twoheadrightarrow} H$ eine kurz exakte Sequenz von Gruppen, mit A abelsch.*

Diese induziert einen Gruppenmorphismus $\alpha : H \longrightarrow \mathrm{Aut}(A)$; cf. Lemma 107.

Sei $\mathrm{H}^1(H, A)$ genommen bezüglich α.

Sei ein Gruppenmorphismus $G \stackrel{s}{\longleftarrow} H$ mit $r \circ s = \mathrm{id}_H$ gegeben.

Die folgenden Aussagen $(1, 2)$ sind äquivalent.

(1) *Es ist $\mathrm{H}^1(H, A) = 1$.*

(2) *Für alle Gruppenmorphismen $G \stackrel{\tilde{s}}{\longleftarrow} H$ mit $r \circ \tilde{s} = \mathrm{id}_H$ gibt es ein $b \in A$ mit ${}^{i(b)}s(h) = \tilde{s}(h)$ für $h \in H$.*

Beweis.

Ad (1) $\Rightarrow$ (2). Sei ein Gruppenmorphismus $G \stackrel{\tilde{s}}{\longleftarrow} H$ mit $r \circ \tilde{s} = \mathrm{id}_H$ gegeben. Es ist $r(s(h)\tilde{s}(h)^{-}) = hh^{-} = 1$ für $h \in H$, sodaß es eine Abbildung $d : H \longrightarrow A$ gibt mit

$i(d(h)) := s(h)\tilde{s}(h)^-$ für $h \in H$. Es ist $d \in \mathrm{Z}^1(H,A)$, denn für $h,\, h' \in H$ ist $r(\tilde{s}(h)) = h$ und also

$$\begin{aligned} i({}^h d(h') \cdot d(hh')^- \cdot d(h)) &= i({}^h d(h')) \cdot i(d(hh')^-) \cdot i(d(h)) \\ &= {}^{\tilde{s}(h)} i(d(h')) \cdot i(d(hh'))^- \cdot i(d(h)) \\ &= {}^{\tilde{s}(h)} s(h')\tilde{s}(h')^- \cdot (s(hh')\tilde{s}(hh')^-)^- \cdot s(h)\tilde{s}(h)^- \\ &= \tilde{s}(h)s(h')\tilde{s}(h')^-\tilde{s}(h)^- \cdot \tilde{s}(h)\tilde{s}(h')s(h')^-s(h)^- \cdot s(h)\tilde{s}(h)^- \\ &= 1\,. \end{aligned}$$

Wegen $\mathrm{H}^1(H,A) = 1$ ist $d \in \mathrm{B}^1(H,A)$. Somit können wir ein $b \in A$ wählen mit $d(h) = {}^h b \cdot b^-$ für $h \in H$. Es folgt

$$s(h) \cdot \tilde{s}(h)^- = i(d(h)) = i({}^h b \cdot b^-) = i({}^h b) \cdot i(b)^- = {}^{s(h)} i(b) \cdot i(b)^- = s(h) \cdot i(b) \cdot s(h)^- \cdot i(b)^-$$

und also

$$ {}^{i(b)} s(h) \;=\; \tilde{s}(h) $$

für $h \in H$.

Ad (2) $\Rightarrow$ (1). Wir haben $\mathrm{H}^1(H,A) \stackrel{!}{=} 1$ zu zeigen, i.e. $\mathrm{Z}^1(H,A) \stackrel{!}{=} \mathrm{B}^1(H,A)$.

Sei $d \in \mathrm{Z}^1(H,A)$ gegeben. Wir haben $d \stackrel{!}{\in} \mathrm{B}^1(H,A)$ zu zeigen.

Setze $\tilde{s}(h) := i(d(h))^- \cdot s(h)$ für $h \in H$. Dann ist $G \xleftarrow{\tilde{s}} H$ ein Gruppenmorphismus mit $r \circ \tilde{s} = \mathrm{id}_H$, denn für $h,\, h' \in H$ ist $(r \circ \tilde{s})(h) = r(i(d(h))^- \cdot s(h)) = 1 \cdot r(s(h)) = h$ und

$$\begin{aligned} \tilde{s}(hh') &= i(d(h))^- \cdot s(h) \cdot i(d(h'))^- \cdot s(h') \\ &= i(d(h))^- \cdot {}^{s(h)} i(d(h'))^- \cdot s(h) \cdot s(h') \\ &= i(d(h))^- \cdot i({}^h d(h'))^- \cdot s(h) \cdot s(h') \\ &= i(d(hh'))^- \cdot s(hh') \\ &= \tilde{s}(hh')\,. \end{aligned}$$

Sei $b \in A$ gewählt mit ${}^{i(b)} s(h) = \tilde{s}(h)$ für $h \in H$. Dann ist

$$ i(b) \cdot s(h) \cdot i(b)^- \;=\; {}^{i(b)} s(h) \;=\; \tilde{s}(h) \;=\; i(d(h))^- \cdot s(h)\,, $$

also

$$ i(d(h)) \;=\; s(h) \cdot i(b) \cdot s(h)^- \cdot i(b)^- \;=\; {}^{s(h)} i(b) \cdot i(b)^- \;=\; i({}^h b \cdot b^-) $$

und somit

$$ d(h) \;=\; {}^h b \cdot b^- $$

für $h \in H$. ▫

Korollar 110 *Sei G eine Gruppe. Sei $A \trianglelefteq G$ ein abelscher Normalteiler. Sei K ein Komplement zu A in G.*

Sei $\mathrm{H}^1(G/A, A)$ *genommen bezüglich* $\alpha : G/A \longrightarrow \mathrm{Aut}(A)$ *wie in Beispiel* 108.

Die folgenden Aussagen $(1, 2)$ *sind äquivalent.*

(1) *Es ist* $\mathrm{H}^1(G/A, A) = 1$.

(2) *Für alle Komplemente* $\tilde{K}$ *zu* A *in* G *gibt es ein* $g \in G$ *mit* ${}^gK = \tilde{K}$.

Beweis. Sei $A \overset{i}{\bullet\!\!\rightarrow} G$ die Inklusion $\mathrm{id}_G|_A$. Sei $G \overset{r}{\twoheadrightarrow} G/A$, $g \longmapsto gA$. Dies gibt die kurz exakte Sequenz $A \overset{i}{\bullet\!\!\rightarrow} G \overset{r}{\twoheadrightarrow} G/A$.

Wir haben den Gruppenisomorphismus $\psi := r|_K : K \longrightarrow G/A$, $k \longmapsto kA$; cf. Bemerkung 94.(2). Sei $s := \mathrm{id}_G|_K \circ \psi^- : G/A \longrightarrow G$, $gA \longmapsto \psi^-(gA)$. Es ist s ein Gruppenmorphismus mit Bild K und mit $r \circ s = \mathrm{id}_{G/A}$, denn $(r \circ s)(xA) = r(\psi^-(xA)) = \psi(\psi^-(xA)) = xA$ für $x \in G$.

Ad (1) $\Rightarrow$ (2). Sei $\tilde{K}$ ein Komplement zu A in G.

Sei $\tilde{s} : G/A \longrightarrow G$ ein Gruppenmorphismus mit Bild $\tilde{K}$ und mit $r \circ \tilde{s} = \mathrm{id}_{G/A}$.

Lemma 109 liefert ein $b \in A$ mit ${}^{i(b)}s(xA) = \tilde{s}(xA)$ für $x \in G$ und also ${}^{i(b)}K = \tilde{K}$.

Ad (2) $\Rightarrow$ (1). Gemäß Lemma 109 genügt es, für jeden Gruppenmorphismus $\tilde{s} : G/A \longrightarrow G$ mit $r \circ \tilde{s} = \mathrm{id}_{G/A}$ ein $b \in A$ zu finden mit ${}^{i(b)}s(xA) = \tilde{s}(xA)$ für $x \in G$.

Es ist $\tilde{K} := \mathrm{Im}(\tilde{s})$ ein Komplement zu A in G; cf. Lemma 96. Dank (2) können wir $g \in G$ mit ${}^gK = \tilde{K}$ wählen. Schreibe $g = (g \cdot s(gA)^-) \cdot s(gA)$. Dann ist $s(gA) \in K$, sowie $r(g \cdot s(gA)^-) = gA \cdot (gA)^- = 1$ und also $(g \cdot s(gA)^-) = i(b)$ für ein $b \in A$. Es ist $\tilde{K} = {}^gK = {}^{i(b)\cdot s(gA)}K = {}^{i(b)}K$. Für $x \in G$ ist also ${}^{i(b)}s(xA) = \tilde{s}(x'A)$ für ein $x' \in G$. Es bleibt $xA \overset{!}{=} x'A$ zu zeigen. In der Tat wird

$$x'A \;=\; r(\tilde{s}(x'A)) \;=\; r({}^{i(b)}s(xA)) \;=\; {}^{r(i(b))}r(s(xA)) \;=\; {}^{1}(xA) \;=\; xA\,.$$

□

Beispiel 111 Sei $p > 0$ prim. Sei $G = \langle a, b : a^p, b^p, [a,b]\rangle \simeq \mathrm{C}_p \times \mathrm{C}_p$. Es hat $\langle a\rangle \trianglelefteq G$ das Komplement $\langle b\rangle$ und das Komplement $\langle ab\rangle$. Da G abelsch ist, sind diese Komplemente nicht konjugiert. Der im Sinne von Lemma 107 induzierte Gruppenmorphismus $G/\langle a\rangle \longrightarrow \mathrm{Aut}(\langle b\rangle)$ ist wegen G abelsch gleich $!$. Cf. Aufgabe 41.(2).

Folglich ist $\mathrm{H}^1(\mathrm{C}_p\,, \mathrm{C}_p) > 1$, genommen bezüglich $! : \mathrm{C}_p \longrightarrow \mathrm{Aut}(\mathrm{C}_p)$.

In der Tat ist $\mathrm{H}^1(\mathrm{C}_p\,, \mathrm{C}_p) \simeq \mathrm{C}_p$; cf. Beispiel 105.(1).

Lemma 112 *Sei* $\alpha : H \longrightarrow \mathrm{Aut}(A)$ *ein Gruppenmorphismus. Sei* $\mathrm{H}^2(H, A)$ *genommen bezüglich* α.

Die folgenden Aussagen $(1, 2)$ *sind äquivalent.*

(1) *Es ist* $\mathrm{H}^2(H, A) = 1$.

(2) *Für jede kurz exakte Sequenz von Gruppen* $A \overset{i}{\bullet\!\!\rightarrow} G \overset{r}{\twoheadrightarrow} H$, *die* α *induziert im Sinne von Lemma* 107, *gibt es einen Gruppenmorphismus* $s : H \longrightarrow G$ *mit* $r \circ s = \mathrm{id}_H$.

Diesenfalls sind wir also in der Situation von Lemma 96. Insbesondere ist G dann ein semidirektes Produkt aus A und H.

Beweis.

Ad (1) $\Rightarrow$ (2). Sei $A \overset{i}{\bullet\!\!\rightarrow} G \overset{r}{\twoheadrightarrow} H$ eine kurz exakte Sequenz von Gruppen. Sei $\mathfrak{s} : H \longrightarrow G$ eine Abbildung mit $r \circ \mathfrak{s} = \mathrm{id}_H$, wählbar, da r surjektiv ist ([2]). Für $h, h' \in H$ ist $r(\mathfrak{s}(h) \cdot \mathfrak{s}(h') \cdot \mathfrak{s}(hh')^-) = h \cdot h' \cdot (hh')^- = 1$, sodaß wir $z(h, h') \in A$ durch $i(z(h, h')) := \mathfrak{s}(h) \cdot \mathfrak{s}(h') \cdot \mathfrak{s}(hh')^-$ definieren können. Dies liefert die Abbildung $z : H \times H \longrightarrow A$.

Wir *behaupten* $z \in \mathrm{Z}^2(H, A)$. Für h, h', $h'' \in H$ wird

$$\begin{array}{rl} & i(z(h,h')^- \cdot {}^h z(h',h'') \cdot z(h,h'h'') \cdot z(hh',h'')^-) \\ \overset{\text{L. }107}{=} & i(z(h,h'))^- \cdot {}^{\mathfrak{s}(h)} i(z(h',h'')) \cdot i(z(h,h'h'')) \cdot i(z(hh',h''))^- \\ = & \big(\mathfrak{s}(hh') \cdot \mathfrak{s}(h')^- \cdot \mathfrak{s}(h)^-\big) \cdot \big(\mathfrak{s}(h) \cdot \mathfrak{s}(h') \cdot \mathfrak{s}(h'') \cdot \mathfrak{s}(h'h'')^- \cdot \mathfrak{s}(h)^-\big) \\ & \cdot \big(\mathfrak{s}(h) \cdot \mathfrak{s}(h'h'') \cdot \mathfrak{s}(hh'h'')^-\big) \cdot \big(\mathfrak{s}(hh'h'') \cdot \mathfrak{s}(h'')^- \cdot \mathfrak{s}(hh')^-\big) \\ = & 1 \, . \end{array}$$

Die *Behauptung* folgt hieraus dank i injektiv.

Wegen $\mathrm{H}^2(H, A) = 1$ ist nun $\mathrm{Z}^2(H, A) = \mathrm{B}^2(H, A)$. Also ist $z \in \mathrm{B}^2(H, A)$. Wähle eine Abbildung $c : H \longrightarrow A$ mit $z(h, h') = {}^h c(h') \cdot c(hh')^- \cdot c(h)$ für h, $h' \in H$. Schreibe $c' := i \circ c$. Es folgt

$$\mathfrak{s}(h) \cdot \mathfrak{s}(h') \cdot \mathfrak{s}(hh')^- \;=\; i(z(h,h')) \;=\; {}^{\mathfrak{s}(h)} c'(h') \cdot c'(hh')^- \cdot c'(h)$$

und also

$$\mathfrak{s}(hh') \;=\; c'(h)^- \cdot c'(hh') \cdot {}^{\mathfrak{s}(h)} c'(h')^- \cdot \mathfrak{s}(h) \cdot \mathfrak{s}(h')$$

für h, $h' \in H$.

Sei $s : H \longrightarrow G$, $h \longmapsto s(h) := c'(h)^- \cdot \mathfrak{s}(h)$.

Es ist $(r \circ s)(h) = r(c'(h)^- \cdot \mathfrak{s}(h)) = r(i(c(h)^-) \cdot r(\mathfrak{s}(h)) = 1 \cdot h = h$ für $h \in H$ und also $r \circ s = \mathrm{id}_H$.

Wir haben zu zeigen, daß s ein Gruppenmorphismus ist. Seien h, $h', \in H$ gegeben. Es wird

$$\begin{array}{rcl} s(hh') & = & c'(hh')^- \cdot \mathfrak{s}(hh') \\ & = & c'(hh')^- \cdot c'(h)^- \cdot c'(hh') \cdot {}^{\mathfrak{s}(h)} c'(h')^- \cdot \mathfrak{s}(h) \cdot \mathfrak{s}(h') \\ & = & c'(h)^- \cdot \mathfrak{s}(h) \cdot c'(h')^- \cdot \mathfrak{s}(h)^- \cdot \mathfrak{s}(h) \cdot \mathfrak{s}(h') \\ & = & c'(h)^- \cdot \mathfrak{s}(h) \cdot c'(h')^- \cdot \mathfrak{s}(h') \\ & = & s(h) \cdot s(h') \, . \end{array}$$

Ad (2) $\Rightarrow$ (1). Wir haben $\mathrm{H}^2(H, A) \overset{!}{=} 1$ zu zeigen, i.e. $\mathrm{Z}^2(H, A) \overset{!}{=} \mathrm{B}^2(H, A)$.

Sei $z \in \mathrm{Z}^2(H, A)$ gegeben. Wir haben $z \overset{!}{\in} \mathrm{B}^2(H, A)$ zu zeigen.

[2] Dies verwendet das Auswahlaxiom.

Sei $G := A \times H$ als Menge. Sei hierauf durch

$$(a,h)\cdot(a',h') \;:=\; (a\,{}^h a' z(h,h'), hh')$$

für $a,\, a' \in A$ und $h,\, h' \in H$ eine Multiplikation erklärt.

Diese Multiplikation ist assoziativ, da

$$\begin{aligned}((a,h)\cdot(a',h'))\cdot(a'',h'') &= (a\,{}^h a'\, z(h,h'), hh')\cdot(a'',h'')\\ &= (a\,{}^h a'\,{}^{hh'} a\, z(h,h')\, z(hh',h''), hh'h'')\\ &= (a\,{}^h a'\,{}^{hh'} a''\,{}^h z(h',h'')\, z(h,h'h''), hh'h'')\\ &= (a,h)\cdot(a'\,{}^{h'} a''\, z(h',h''), h'h'')\\ &= (a,h)\cdot((a',h')\cdot(a'',h''))\end{aligned}$$

für $a,\, a',\, a'' \in A$ und $h,\, h',\, h'' \in H$.

Es ist ${}^h z(1,1)\cdot z(h\cdot 1,1)^-\cdot z(h,1\cdot 1)\cdot z(h,1)^- = 1$ und also $z(h,1) = {}^h z(1,1)$ für $h \in H$. Also wird

$$(a,h)\cdot(z(1,1)^-,1) \;=\; (a\,{}^h z(1,1)^-\, z(h,1)\,,\, h) = (a,h)$$

und

$$(a,h)\cdot({}^{h^-}(a^-\, z(1,1)^-\, z(h,h^-)^-)\,,\, h^-) \;=\; (a\, a^-\, z(1,1)^-\, z(h,h^-)^-\, z(h,h^-), 1) \;=\; (z(1,1)^-,1)$$

für $a \in A$ und $h \in H$.

Somit ist G eine Gruppe, mit dem neutralen Element $1_G = (z(1,1)^-,1)$ und mit dem inversen Element $(a,h)^- = ({}^{h^-}(a^-\, z(1,1)^-\, z(h,h^-)^-)\,,\, h^-)$ für $(a,h) \in G$; cf. Aufgabe 1.

Wir haben die kurz exakte Sequenz von Gruppen

$$\begin{array}{ccccc} A & \overset{i}{\bullet\!\!\rightarrow} & G & \overset{r}{\twoheadrightarrow} & H\\ a & \longmapsto & (a\, z(1,1)^-,1) & & \\ & & (a,h) & \longmapsto & h\,. \end{array}$$

Denn es ist die Abbildung i injektiv, es ist $i(a)\cdot i(a') = (a\, z(1,1)^-,1)\cdot(a'\, z(1,1)^-,1) = (a\, z(1,1)^-\, a'\, z(1,1)^-\, z(1,1), 1\cdot 1) \;=\; (a\, a'\, z(1,1)^-,1) = i(aa')$ für $a,\, a' \in A$, es ist die Abbildung r surjektiv, es ist $r((a,h)\cdot(a,h')) = r(a\,{}^h a'\, z(h,h'), hh') = hh' = r(a,h)\cdot r(a,h')$ für $(a,h),\, (a,h') \in G$ und es ist

$$\mathrm{Im}(i) \;=\; \{\,(a\, z(1,1)^-,1) \,:\, a \in A\,\} \;=\; \{\,(\tilde a,1) \,:\, \tilde a \in A\,\} \;=\; \mathrm{Kern}(r)\,.$$

Diese kurz exakte Sequenz induziere den Gruppenmorphismus $\tilde\alpha : H \longrightarrow \mathrm{Aut}(A)$ im Sinne von Lemma 109. Für $a \in A$ und $h \in H$ ist $r(1,h) = h$ und also

$$\begin{aligned} i((\tilde\alpha(h))(a)) &= {}^{(1,h)} i(a)\\ &= (1,h)(a\, z(1,1)^-,1)(1,h)^-\\ &= ({}^h a\,{}^h z(1,1)^- z(h,1), h)({}^{h^-}(z(1,1)^-\, z(h,h^-)^-)\,,\, h^-)\\ &= ({}^h a, h)({}^{h^-}(z(1,1)^-\, z(h,h^-)^-)\,,\, h^-)\\ &= ({}^h a\, z(1,1)^-\, z(h,h^-)^-\, z(h,h^-)\,,\, 1)\\ &= ({}^h a\, z(1,1)^-,\, 1)\\ &= i({}^h a)\\ &= i((\alpha(h))(a))\,. \end{aligned}$$

Es folgt $\tilde{\alpha} = \alpha$.

Dank (2) gibt es also einen Gruppenmorphismus $G \overset{s}{\longleftarrow} H$ mit $r \circ s = \mathrm{id}_H$, i.e. mit $s(h) = (c(h)^-, h)$ für eine Abbildung $c : H \longrightarrow A$. Für $h,\ h' \in H$ wird mithin

$$\begin{aligned}(c(hh')^-, hh') &= s(hh') \\ &= s(h) \cdot s(h') \\ &= (c(h)^-, h) \cdot (c(h')^-, h') \\ &= (c(h)^- \ {}^h c(h')^- \ z(h,h'), h')\end{aligned}$$

und infolgedessen

$$z(h,h') = {}^h c(h') \cdot c(hh')^- \cdot c(h) \ .$$

Somit ist $z \in \mathrm{B}^2(H, A)$. ▫

Korollar 113 *Sei G eine Gruppe. Sei $A \trianglelefteq G$ ein abelscher Normalteiler.*

Sei $\mathrm{H}^2(G/A, A)$ genommen bezüglich $\alpha : G/A \longrightarrow \mathrm{Aut}(A)$ wie in Beispiel 108.

Ist $\mathrm{H}^2(G/A, A) = 1$, dann hat A in G ein Komplement.

Beweis. Sei $\mathrm{H}^2(G/A, A) = 1$.

Sei $A \overset{i}{\longrightarrow} G$ die Inklusion $\mathrm{id}_G|_A$. Sei $G \overset{r}{\longrightarrow} G/A$, $g \longmapsto gA$. Dies gibt die kurz exakte Sequenz $A \overset{i}{\rightarrowtail} G \overset{r}{\twoheadrightarrow} G/A$.

Dank Lemma 112 gibt es einen Gruppenmorphismus $s : G/A \longrightarrow G$ mit $r \circ s = \mathrm{id}_{G/A}$.

Es ist $s(G/A)$ ein Komplement zu A in G; cf. Lemma 96.(1). ▫

Beispiel 114 Sei $G = \langle\, a \ : \ a^4 \,\rangle \simeq \mathrm{C}_4$. Es hat $\langle a^2 \rangle$ in C_4 kein Komplement; cf. Beispiel 95.(6). Der im Sinne von Lemma 107 induzierte Gruppenmorphismus $G/\langle a^2 \rangle \longrightarrow \mathrm{Aut}(\langle a^2 \rangle)$ ist wegen G abelsch (oder wegen $\mathrm{Aut}(\langle a^2 \rangle) = 1$) gleich !.

Folglich ist $\mathrm{H}^2(\mathrm{C}_2\,,\, \mathrm{C}_2) > 1$, genommen bezüglich $! : \mathrm{C}_2 \longrightarrow \mathrm{Aut}(\mathrm{C}_2)$.

In der Tat ist $\mathrm{H}^2(\mathrm{C}_2\,,\, \mathrm{C}_2) \simeq \mathrm{C}_2$; cf. Beispiel 105.(2).

Bemerkung 115 *Sei H eine endliche Gruppe. Sei A eine endliche abelsche Gruppe. Sei $\alpha : H \longrightarrow \mathrm{Aut}(A)$ ein Gruppenmorphismus. Seien $\mathrm{H}^1(H, A)$ und $\mathrm{H}^2(H, A)$ genommen bezüglich α.*

(1) *Für $\delta \in \mathrm{H}^1(H, A)$ ist $\delta^{\exp(A)} = 1$.*

(2) *Für $\delta \in \mathrm{H}^1(H, A)$ ist $\delta^{|H|} = 1$.*

(3) *Für $\zeta \in \mathrm{H}^2(H, A)$ ist $\zeta^{\exp(A)} = 1$.*

(4) *Für $\zeta \in \mathrm{H}^2(H, A)$ ist $\zeta^{|H|} = 1$.*

Beweis.

Ad (1). Dies gilt in ${}_{\mathrm{Abb}}(H, A)$, also in der Untergruppe $\mathrm{Z}^1(H, A)$, also in der Faktorgruppe $\mathrm{H}^1(H, A)$.

Ad (2). Für $\delta \in \mathrm{H}^1(H, A)$ ist

$$\delta^{|H|} \overset{\text{L. 106.(2)}}{=} (\mathrm{Cores}\uparrow_1^H \circ \mathrm{Res}\downarrow_1^H)(\delta) \;=\; 1\,,$$

letzteres, da $\mathrm{H}^1(1, A) = 1$; cf. Beispiel 105.(3).

Ad (3). Dies gilt in ${}_{\mathrm{Abb}}(H \times H, A)$, also in der Untergruppe $\mathrm{Z}^2(H, A)$, also in der Faktorgruppe $\mathrm{H}^2(H, A)$.

Ad (4). Für $\zeta \in \mathrm{H}^2(H, A)$ ist

$$\zeta^{|H|} \overset{\text{L. 106.(4)}}{=} (\mathrm{Cores}\uparrow_1^H \circ \mathrm{Res}\downarrow_1^H)(\zeta) \;=\; 1\,,$$

letzteres, da $\mathrm{H}^2(1, A) = 1$; cf. Beispiel 105.(3). ▫

Lemma 116 (Schur) *Sei G eine endliche Gruppe.*

Sei $A \trianglelefteq G$ ein abelscher Normalteiler. Seien $|A|$ und $|G/A|$ teilerfremd.

(1) *Es hat A in G ein Komplement.*

(2) *Seien K und $\tilde{K}$ Komplemente zu A in G. Dann gibt es ein $g \in G$ mit $\tilde{K} = {}^gK$.*

Beweis. Sei $\alpha : G/A \longrightarrow \mathrm{Aut}(A)$ wie in Beispiel 108. Seien $\mathrm{H}^1(H, A)$ und $\mathrm{H}^2(H, A)$ genommen bezüglich α.

Zeigen wir zunächst $\mathrm{H}^1(G/A, A) \overset{!}{=} 1$. Sei $\delta \in \mathrm{H}^1(G/A, A)$. Wir müssen $|\langle\delta\rangle| \overset{!}{=} 1$ zeigen. Es ist $\delta^{\exp(A)} = 1$, also auch $\delta^{|A|} = 1$; cf. Bemerkung 115.(1). Es ist $\delta^{|G/A|} = 1$; cf. Bemerkung 115.(2). Folglich teilt $|\langle\delta\rangle|$ sowohl $|A|$ als auch $|G/A|$. Da $|A|$ und $|G/A|$ teilerfremd sind, folgt $|\langle\delta\rangle| = 1$.

Genauso folgt $\mathrm{H}^2(H, A) = 1$ unter Verwendung von Bemerkung 115.(3, 4).

Ad (1). Da $\mathrm{H}^2(G/A, A) = 1$, hat dank Korollar 113 der abelsche Normalteiler A in G ein Komplement.

Ad (2). Da $\mathrm{H}^1(G/A, A) = 1$, gibt es dank Korollar 110 ein $g \in G$ mit $\tilde{K} = {}^gK$. ▫

3.4.3 Zassenhaus

Lemma 117 (Frattini) *Sei G eine endliche Gruppe. Sei $N \trianglelefteq G$.*

Sei p prim. Sei $P \in \mathrm{Syl}_p(N)$.

Dann ist $\mathrm{N}_G(P) \cdot N = G$.

Beweis. Es ist $\mathrm{Syl}_p(N)$ eine transitive N-Menge; cf. Satz 38.(2). Sei $g \in G$. Sei $P \in \mathrm{Syl}_p(N)$. Wegen $N \trianglelefteq G$ ist auch ${}^gP \in \mathrm{Syl}_p(N)$. Folglich gibt es ein $n \in N$ mit ${}^gP = {}^nP$. Also ist $n^- g \in \mathrm{N}_G(P)$ und somit $g \in \mathrm{N}_G(P) \cdot N$. ▫

Lemma 117 kann auch aus Aufgabe 6.(1) gefolgert werden.

Bemerkung 118 *Sei G eine Gruppe. Seien H, K, $L \leqslant G$. Sei $H \leqslant L$. Dann ist*

$$H(K \cap L) \;=\; HK \cap L$$

als Teilmengen von G.

Beweis. Seien $h \in H$ und $k \in K \cap L$. Dann liegt hk in HK und wegen $h \in L$ und $k \in L$ auch in L.

Seien umgekehrt $h \in H$ und $k \in K$ mit $hk \in L$ gegeben. Dann liegt $k = h^-(hk)$ in L, da h^- in L enthalten ist, und somit ist $hk \in H(K \cap L)$. ▫

Definition 119 Sei G eine endliche Gruppe.

Ein Normalteiler $N \trianglelefteq G$ mit $|N|$ teilerfremd zu $|G/N|$ heißt ein *Hall-Normalteiler* oder *hallsch* in G.

Bemerkung 120 *Sei G eine endliche Gruppe. Sei $N \trianglelefteq G$ hallsch. Sei $K \leqslant G$.*

Es ist genau dann K ein Komplement zu N in G, wenn $|K| = |G/N|$ ist.

Beweis.

Ad $\Rightarrow$. Es ist $K \simeq G/N$, also $|K| = |G/N|$; cf. Bemerkung 94.(2).

Ad $\Leftarrow$. Es ist $|N \cap K|$ ein Teiler von $|N|$ und von $|K| = |G/N|$. Folglich ist $N \cap K = 1$. Daher ist auch $|NK| = |N| \cdot |K|/|N \cap K| = |N| \cdot |G/N|/1 = |G|$; cf. Aufgabe 12.(1). ▫

Satz 121 (Schur, Zassenhaus) *Sei G eine endliche Gruppe.*

Sei $N \trianglelefteq G$ ein Hall-Normalteiler, es seien also $|N|$ und $|G/N|$ teilerfremd.

(1) *Es hat N in G ein Komplement.*

(2) *Sei N auflösbar oder G/N auflösbar.*

Sind K und $\tilde{K}$ Komplemente zu N in G, so gibt es ein $g \in G$ mit $\tilde{K} = {}^gK$.

Cf. Bemerkung 94.

Beweis.

Ad (1). *Annahme,* es gibt eine endliche Gruppe, die einen Hall-Normalteiler besitzt, für welchen (1) nicht gilt. Sei G eine solche endliche Gruppe minimaler Ordnung. Sei $N \trianglelefteq G$ ein Hall-Normalteiler, welcher kein Komplement besitzt. Insbesondere ist $N > 1$.

Sei $p \in \pi(N)$. Sei $P \in \mathrm{Syl}_p(N)$; cf. Satz 38.(1). Wir behaupten $P \overset{!}{\trianglelefteq} G$. Sei im Gegenteil *angenommen,* es ist $\mathrm{N}_G(P) < G$. Es ist $G = \mathrm{N}_G(P) \cdot N$; cf. Lemma 117. Es ist $\mathrm{N}_N(P) = N \cap \mathrm{N}_G(P)$ hallsch in $\mathrm{N}_G(P)$, da $|\mathrm{N}_N(P)|$ ein Teiler von $|N|$ ist und $|\mathrm{N}_G(P)/(N \cap \mathrm{N}_G(P))| = |\mathrm{N}_G(P) \cdot N/N| = |G/N|$ ist; cf. Aufgabe 12.(2). Wegen der Minimalität von $|G|$ existiert ein Komplement K zu $\mathrm{N}_N(P)$ in $\mathrm{N}_G(P)$, isomorph zu G/N. Da N hallsch in G ist und da $|K| = |G/N|$ ist, ist K ein Komplement zu N in G; cf. Bemerkung 120.(1). Wir haben einen *Widerspruch.* Also ist $P \trianglelefteq G$.

Schreibe $Z := \mathrm{Z}(P)$. Es ist $Z > 1$; beachte $P > 1$ und Aufgabe 31.(1). Es ist $Z \blacktriangleleft P \trianglelefteq G$ und also $Z \trianglelefteq G$; cf. Bemerkung 80.(4, 2). Es ist $|N/Z|$ teilerfremd zu $|(G/Z)/(N/Z)| = |G/N|$, also $N/Z \trianglelefteq G/Z$ hallsch. Wegen der Minimalität von $|G|$ hat N/Z ein Komplement L/Z in G/Z, wobei $Z \leqslant L \leqslant G$; cf. Aufgabe 17.(1). Es ist also $|N/Z||L/Z| = |G/Z|$, i.e. $|N||L| = |G||Z|$.

Es ist $Z \trianglelefteq L$ hallsch, da $|Z|$ ein Teiler von $|N|$ ist und dies teilerfremd zu $|G/N| = |L/Z|$ ist. Da Z abelsch ist, hat Z ein Komplement M in L; cf. Lemma 116.(1). Insbesondere ist $|M| = |L/Z| = |G/N|$; cf. Bemerkung 94.(2). Da N hallsch in G ist, ist M ein Komplement zu N in G; cf. Bemerkung 120.(1). Wir haben einen *Widerspruch.*

Ad (2).

Fall: Normalteiler auflösbar. Annahme, es gibt eine endliche Gruppe mit einem auflösbaren Hall-Normalteiler mit zwei nicht zueinander konjugierten Komplementen. Sei G eine solche Gruppe minimaler Ordnung. Sei darin N ein auflösbarer Hall-Normalteiler mit zwei nicht zueinander konjugierten Komplementen K und L. Wäre $N = 1$, so wäre $K = G = L$, was nicht der Fall ist. Also ist $N > 1$. Somit ist $N^{(1)} < N$; cf. Satz 84. Aus $N^{(1)} \blacktriangleleft N \trianglelefteq G$ folgt ferner $N^{(1)} \trianglelefteq G$; cf. Bemerkung 80.(5, 2).

Schreibe $\bar{G} := G/N^{(1)}$, $\bar{N} := N/N^{(1)}$, $\bar{K} := KN^{(1)}/N^{(1)}$, $\bar{L} := LN^{(1)}/N^{(1)}$. Also $\bar{N} \trianglelefteq \bar{G}$ und $\bar{K}, \bar{L} \leqslant \bar{G}$. Wegen $K \cap N^{(1)} = 1$ und $L \cap N^{(1)} = 1$ ist $K \xrightarrow{\sim} \bar{K}$, $k \longmapsto kN^{(1)}$, insgesamt also $K \simeq \bar{K} \simeq G/N$; cf. Bemerkung 94.(2). Genauso ist $L \simeq \bar{L} \simeq G/N$. Ferner ist $|\bar{N}|$ ein Teiler von $|N|$ und dies wiederum teilerfremd zu $|G/N| = |\bar{G}/\bar{N}|$. Also ist $\bar{N} \trianglelefteq \bar{G}$ hallsch, und es sind $\bar{K}$ und $\bar{L}$ beides Komplemente zu $\bar{N}$ in $\bar{G}$; cf. Bemerkung 120.(1). Da $\bar{N}$ abelsch ist nach Aufgabe 13.(2), können wir ein $y \in G$ wählen mit, so wir $\bar{y} := yN^{(1)}$ schreiben, ${}^{\bar{y}}\bar{K} = \bar{L}$, i.e. mit $({}^{y}K)N^{(1)} = LN^{(1)} =: G'$. Es ist $|G'| = |L| \cdot |N^{(1)}|/|L \cap N^{(1)}| = |L| \cdot |N^{(1)}| < |L| \cdot |N| = |G|$.

Nun ist $N^{(1)}$ ein auflösbarer Normalteiler von G, also auch von G'; cf. Satz 84. Es ist $|N^{(1)}|$ ein Teiler von $|N|$, und dies teilerfremd zu $|G/N| = |{}^{y}K| = |L| = |G'/N^{(1)}|$. Also ist $N^{(1)} \trianglelefteq G'$ hallsch, und es sind ${}^{y}K$ und L Komplemente zu $N^{(1)}$ in G'; cf. Bemerkung 120.(1). Wegen der Minimalität von $|G|$ folgt nun, daß es ein $x \in G'$ gibt mit $L = {}^{x}({}^{y}K) = {}^{xy}K$, wobei $xy \in G$. Wir haben einen *Widerspruch.*

Fall: Faktorgruppe auflösbar. Annahme, es gibt eine endliche Gruppe mit einem Hall-Normalteiler mit auflösbarer Faktorgruppe und zwei nicht zueinander konjugierten Komplementen. Sei G eine solche Gruppe minimaler Ordnung. Sei $N \trianglelefteqslant G$ hallsch mit G/N auflösbar, und seien K und L nicht zueinander konjugierte Komplemente von N in G. Wäre $N = G$, so wäre $K = 1 = L$, was nicht der Fall ist. Also ist $N < G$. Es ist $(G/N)^{(1)} < G/N$, i.e. $G^{(1)}N < G$; cf. Satz 84, Aufgabe 13.(1). Da $G/G^{(1)}N$ eine abelsche Gruppe ungleich 1 ist, hat sie eine normale Untergruppe von primem Index; cf. Aufgaben 13.(4) und 3.(4). Somit gibt es ein $N \leqslant NG^{(1)} \leqslant M \lhd G$ mit $|G/M| =: p > 1$ prim; cf. Aufgabe 17.(3). Wäre $N = M$, so wären K, $L \in \mathrm{Syl}_p(G)$ und also gemäß Satz 38.(2) zueinander konjugiert, was nicht der Fall ist. Also ist $N < M$. Insgesamt ist $N \lhd M$.

Da $N \trianglelefteqslant G$ hallsch ist, ist auch $N \trianglelefteqslant M$ hallsch. Es ist $N \cap (K \cap M) = 1$ und $N(K \cap M) = NK \cap M = G \cap M = M$; cf. Bemerkung 118. Also ist $K \cap M$ ein Komplement zu N in M. Genauso ist $L \cap M$ ein Komplement zu N in M. Insbesondere ist M/N als Untergruppe von G/N auflösbar; cf. Aufgabe 32.(2). Wegen der Minimalität von $|G|$ gibt es ein $m \in M$ mit $U := L \cap M = {}^m(K \cap M) = {}^mK \cap M$. Es ist $U \simeq M/N$ und also $U > 1$; cf. Bemerkung 94.(2). Es ist $U \trianglelefteqslant L$, i.e. $L \leqslant \mathrm{N}_G(U)$. Genauso ist ${}^mK \leqslant \mathrm{N}_G(U)$.

Subfall $\mathrm{N}_G(U) < G$. Es ist $N \cap \mathrm{N}_G(U) =: N' \trianglelefteqslant \mathrm{N}_G(U)$. Es ist $L \cap N' = 1$ und $LN' = L(N \cap \mathrm{N}_G(U)) = LN \cap \mathrm{N}_G(U) = \mathrm{N}_G(U)$; cf. Bemerkung 118. Genauso ist ${}^mK \cap N' = 1$ und $({}^mK) \cdot N' = \mathrm{N}_G(U)$. Also sind L und ${}^mK$ Komplemente zu N' in $\mathrm{N}_G(U)$. Da $N' \leqslant N$, ist $|N'|$ teilerfremd zu $|\mathrm{N}_G(U)/N'| = |L|$. Somit ist $N' \trianglelefteqslant \mathrm{N}_G(U)$ hallsch. Ferner ist $\mathrm{N}_G(U)/N' \simeq L \simeq G/N$ auflösbar; cf. Bemerkung 94.(2). Wegen der Minimalität von $|G|$ gibt es ein $x \in \mathrm{N}_G(U) \leqslant G$ mit $L = {}^x({}^mK) = {}^{xm}K$. Da $xm \in G$, haben wir diesenfalls einen *Widerspruch.*

Subfall $\mathrm{N}_G(U) = G$. Es ist $U \trianglelefteqslant G$. Es ist $N \cap U = N \cap (L \cap M) = 1$. Also ist $N \xrightarrow{\sim} NU/U$, $n \longmapsto nU$. Es ist $NU/U \trianglelefteqslant G/U$ hallsch, da $|NU/U| = |N|$ und $|(G/U)/(NU/U)| = |G/NU| = |G|/(|N| \cdot |U|/|N \cap U|) = |G/N|/|U|$ teilerfremd sind; cf. Aufgabe 12.(2). Da ferner $|L/U| = |{}^mK/U| = |G/N|/|U| = |(G/U)/(NU/U)|$, sind L/U und ${}^mK/U$ Komplemente zu NU/U in G/U; cf. Bemerkung 120.(1). Insbesondere ist $(G/U)/(NU/U) \simeq L/U$ als Faktorgruppe von $L \simeq G/N$ auflösbar; cf. Aufgabe 32.(2). Wegen der Minimalität von $|G|$ gibt es ein $y \in G$ mit $L/U = {}^{yU}({}^mK/U)$, i.e. mit $L = {}^{ym}K$. Da $ym \in G$, haben wir diesenfalls einen *Widerspruch.* □

> Der Satz von Feit und Thompson (Pac. J. Math. 13, 1963) besagt, daß eine Gruppe ungerader Ordnung auflösbar ist. Könnten wir diesen Satz hier zeigen, würden wir wissen, daß die Auflösbarkeitsbedingung in Satz 121.(2) weggelassen werden darf.

Beispiel 122 Sei G eine endliche Gruppe. Sei $p \in \pi(G)$. Sei $\mathrm{Syl}_p(G) = \{P\}$. Dann ist $P \trianglelefteqslant G$ hallsch. Dank Satz 121 hat P also ein Komplement in G, und alle solchen Komplemente sind konjugiert in G; cf. Bemerkungen 75.(1) und 76.

Falls $\pi(G) = \{p, q\}$ ist mit $p \neq q$, so ist ein Komplement zu P dasselbe wie eine q-Sylowgruppe von G ; cf. Bemerkung 120. Diesenfalls können wir die Existenz eines Komplements zu P in G also auch aus Satz 38.(1) folgern; ferner folgt die Tatsache, daß zwei Komplemente zu P in G dort zueinander konjugiert sind, dann auch aus Satz 38.(2).

Kapitel 4

Kleine Untergruppen

4.1 Die Frattiniuntergruppe

Sei G eine endliche Gruppe.

Definition 123 Sei $\mathrm{U}_{\max}(G) := \{\, U < G \,:\, \text{es gibt kein } V \text{ mit } U < V < G \,\}$ die Menge der maximalen echten Untergruppen von G.

Sei

$$\Phi(G) \;:=\; \bigcap_{U \in \mathrm{U}_{\max}(G)} U$$

die *Frattiniuntergruppe* von G.

Bemerkung 124

(1) *Es ist* $\Phi(G) \trianglelefteq G$.

(2) *Sei* $V \leqslant G$ *mit* $V\Phi(G) = G$ *gegeben. Dann ist* $V = G$.

Beweis.

Ad (1). Sei $\beta \in \mathrm{Aut}(G)$. Sei $U \in \mathrm{U}_{\max}(G)$. Dann ist $\mathrm{U}_{\max}(G) \longrightarrow \mathrm{U}_{\max}(G)$, $U \longmapsto \beta(U)$ eine Bijektion. Also ist $\beta(\Phi(G)) = \bigcap_{U \in \mathrm{U}_{\max}(G)} \beta(U) = \bigcap_{\tilde{U} \in \mathrm{U}_{\max}(G)} \tilde{U} = \Phi(G)$.

Ad (2). *Annahme*, es ist $V < G$. Dann gibt es ein $U \in \mathrm{U}_{\max}(G)$ mit $V \leqslant U < G$. Es ist auch $\Phi(G) \leqslant U$. Also ist $V\Phi(G) \leqslant U < G$ und wir haben einen *Widerspruch.* ▫

Lemma 125 *Es ist* $\Phi(G)$ *nilpotent.*

Beweis. Sei $p \in \pi(\Phi(G))$ und $P \in \mathrm{Syl}_p(\Phi(G))$ gegeben. Wir haben $P \trianglelefteqslant \Phi(G)$ zu zeigen; cf. Satz 89.

Es ist $\mathrm{N}_G(P)\Phi(G) = G$; cf. Lemma 117. Also ist $\mathrm{N}_G(P) = G$; cf. Bemerkung 124.(2). Also ist $P \trianglelefteqslant G$ und somit $P \trianglelefteqslant \Phi(G)$. ▫

Lemma 126 *Es ist* $\Phi(G/\Phi(G)) = 1$.

In diesem Sinne ist es möglich, die Frattinigruppe aus einer Gruppe zu entfernen.

Beweis. Es ist $\mathrm{U}_{\max}(G/\Phi(G)) = \{\, U/\Phi(G) \,:\, U \in \mathrm{U}_{\max}(G) \,\}$, da jede Untergruppe $U \in \mathrm{U}_{\max}(G)$ die Frattiniuntergruppe $\Phi(G)$ enthält; cf. Aufgabe 17.(1). Also wird

$$\begin{aligned} \Phi(G/\Phi(G)) &= \textstyle\bigcap_{U\in \mathrm{U}_{\max}(G)}(U/\Phi(G)) \\ &= (\textstyle\bigcap_{U\in \mathrm{U}_{\max}(G)} U)/\Phi(G) \\ &= \Phi(G)/\Phi(G) \\ &= 1\,. \end{aligned}$$

□

Lemma 127 *Sei* $p > 0$ *prim. Sei* P *eine* p*-Gruppe.*
Schreibe $P^p := \langle\, x^p \,:\, x \in P \,\rangle$.

(1) *Es ist* $P^p \trianglelefteq P$.

(2) *Es ist* $\Phi(P) = P^{(1)}P^p$.

(3) *Falls* $p = 2$ *ist, ist* $\Phi(P) = P^2$.

(4) *Sei* $U \leqslant P$. *Es ist* $\Phi(U) \leqslant \Phi(P)$.

(5) *Sei* $N \trianglelefteq P$. *Es ist* $\Phi(P/N) = \Phi(P)N/N$.

(6) *Sei* $|P/\Phi(P)| =: p^n$, *wobei* $n \geqslant 0$. *Dann ist* $n = \min\{\, |S| \,:\, S \subseteq P,\ \langle S\rangle = P \,\}$.

Cf. Aufgabe **??**.

Beweis.
Ad (1). Sei $\beta \in \mathrm{Aut}(P)$. Es ist

$$\beta(P^p) \;=\; \langle\, \beta(x^p) \,:\, x \in P \,\rangle \;=\; \langle\, \beta(x)^p \,:\, x \in P \,\rangle \;=\; \langle\, \tilde{x}^p \,:\, \tilde{x} \in P \,\rangle \;=\; P^p\,.$$

Ad (2).

Ad $\geqslant$. Sei $U \in \mathrm{U}_{\max}(G)$. Zu zeigen ist $P^{(1)}P^p \overset{!}{\leqslant} U$, i.e. $P^{(1)} \overset{!}{\leqslant} U$ und $P^p \overset{!}{\leqslant} U$.
Es ist $U < \mathrm{N}_P(U) \leqslant P$; cf. Aufgabe 40.(1). Da U maximale echte Untergruppe von P ist, folgt $\mathrm{N}_P(U) = P$, i.e. $U \trianglelefteq P$. Abermals wegen dieser Maximalität darf die p-Gruppe P/U keine Untergruppe echt zwischen 1 und P/U besitzen; cf. Aufgabe 17.(1). Aber P/U enthält ein Element und also auch eine Untergruppe von Ordnung p; cf. Aufgabe 7.(1).

Somit ist $|P/U| = p$, i.e. $P/U \simeq \mathrm{C}_p$. Folglich ist $P^{(1)} \leqslant U$; cf. Aufgabe 13.(4). Sei $x \in P$. Es ist $x^p U = (xU)^p = 1U$, i.e. $x^p \in U$. Somit ist auch $P^p \leqslant U$.

Ad $\leqslant$. Schreibe $Q := P^{(1)}P^p$. Es ist P/Q eine endliche abelsche Gruppe, in welcher jedes Element Ordnung 1 oder Ordnung p hat; cf. Aufgabe 13.(4). Folglich können wir einen Isomorphismus $\mathrm{C}_p^{\times \ell} \xrightarrow{\sim} P/Q$ wählen, wobei $\ell \geqslant 0$; cf. Aufgabe 3.(4). Sei c_i ein Erzeuger des i-ten direkten Faktors und $d_i Q$ sein Bild unter diesem Isomorphismus.

Sei $x \in P \smallsetminus Q$. Wir haben $x \notin \Phi(P)$ zu zeigen. Dafür ist zu zeigen, daß es ein $U \in \mathrm{U}_{\max}(P)$ mit $x \notin U$ gibt. Schreibe $xQ = \prod_{i \in [1,\ell]} (d_i Q)^{t_i}$ mit $t_i \in [0, p-1]$. Es gibt ein $j \in [0, p-1]$ mit $t_i \neq 0$. Sei $Q \trianglelefteq U \trianglelefteq P$ mit $U/Q := \langle\, d_i \,:\, i \in [1,\ell] \smallsetminus \{j\} \,\rangle$; cf. Aufgabe 17.(1, 2). Es ist $xQ \notin U/Q$ und also $x \notin U$. Es ist $|P/U| = |(P/Q)/(U/Q)| = p$ und also $U \in \mathrm{U}_{\max}(P)$.

Ad (3). Dank (2) bleibt $P^{(1)} \leqslant P^2$ zu zeigen. Seien $x,\, y \in P$. Es ist $[x,y] \overset{!}{\in} P^2$ zu zeigen. Tatsächlich wird

$$P^2 \;\ni\; (x^- y^- x)^2 (x^-)^2 (xy)^2 \;=\; x^- y^{-2} x x^{-2} xyxy \;=\; x^- y^- xy \;=\; [x,y]\,.$$

Ad (4). Wir wenden (2) auf U und P an. Aus $U^p \leqslant P^p$ und $U^{(1)} \leqslant P^{(1)}$ folgt

$$\Phi(U) \;=\; U^{(1)}U^p \;\leqslant\; P^{(1)}P^p \;=\; \Phi(P)\,.$$

Ad (5). Wir wenden (2) auf P und P/N an. Es wird

$$\Phi(P/N) \;=\; (P/N)^{(1)}(P/N)^p \;=\; (P^{(1)}N/N)(P^pN/N) \;=\; P^{(1)}P^pN/N \;=\; \Phi(P)N/N\,;$$

cf. Aufgabe 13.(1).

Ad (6). Wir *behaupten*

$$\min\{\,|S| \,:\, S \subseteq P,\ \langle S\rangle = P\,\} \;\overset{!}{=}\; \min\{\,|T| \,:\, T \subseteq P/\Phi(P),\ \langle T\rangle = P/\Phi(P)\,\}\,.$$

Ad $\geqslant$. Ist $S \subseteq P$ mit $\langle S\rangle = P$ gegeben, dann ist mit $T := \{\, s\Phi(P) \,:\, s \in S\,\}$ zum einen $|S| \geqslant |T|$, zum anderen $T \subseteq P/\Phi(P)$ mit $\langle T\rangle = P/\Phi(P)$.

Ad $\leqslant$. Ist $T \subseteq P/\Phi(P)$ mit $\langle T\rangle = P/\Phi(P)$ gegeben, dann wählen wir $S \subseteq P$ mit $T := \{\, s\Phi(P) \,:\, s \in S\,\}$ und $|T| = |S|$. Wegen $P/\Phi(P) = \langle T\rangle = \langle\, s\Phi(P) \,:\, s \in S\,\rangle$ folgt nun $\langle S\rangle\Phi(P) = P$ und also $\langle S\rangle = P$; cf. Bemerkung 124.(2).

Dies zeigt die *Behauptung.*

Zu zeigen ist nun also $n \overset{!}{=} \min\{\,|T| \,:\, T \subseteq P/\Phi(P),\ \langle T\rangle = P/\Phi(P)\,\}$.

Es ist $P/\Phi(P) = P/(P^{(1)}P^p) \simeq \mathrm{C}_p^{\times n}$; cf. Argument zu (2). Diese Gruppe ist isomorph zur additiven Gruppe des $\mathbf{F}_p$-Vektorraums $\mathbf{F}_p^n$. Unter einem solchen Isomorphismus entspricht eine erzeugende Teilmenge einer $\mathbf{F}_p$-linear erzeugenden Teilmenge von $\mathbf{F}_p^n$. Dank Linearer Algebra ist also

$$\begin{aligned} & \min\{\,|T| \,:\, T \subseteq P/\Phi(P),\ P/\Phi(P) = \langle T\rangle\,\} \\ = \;& \min\{\,|T'| \,:\, T' \subseteq \mathbf{F}_p^n,\ T' \text{ ist } \mathbf{F}_p\text{-linear erzeugende Teilmenge von } \mathbf{F}_p^n\,\} \\ = \;& n\,. \end{aligned}$$

□

Beispiel 128

(1) Es ist $\Phi(\mathrm{S}_3) = 1$, da bereits die maximalen echten Untergruppen $\langle (1,2,3) \rangle$ und $\langle (1,2) \rangle$ den Schnitt 1 haben.

(2) Betrachte $\mathrm{D}_8 = \langle\, a, b \,:\, a^4, b^2, (ab)^2 \,\rangle$; cf. Beispiel 56. Es ist $\mathrm{D}_8^2 = \Phi(\mathrm{D}_8)$; cf. Lemma 127.(3). Es ist $\langle a^2 \rangle \leqslant \mathrm{D}_8^2$. Es ist $\langle a^2 \rangle \trianglelefteqslant \mathrm{D}_8$ und $\mathrm{D}_8/\langle a^2 \rangle \simeq \mathrm{C}_2 \times \mathrm{C}_2$, mithin $\mathrm{D}_8^2 \leqslant \langle a^2 \rangle$. Insgesamt ist $\Phi(\mathrm{D}_8) = \langle a^2 \rangle$.

(3) Betrachte S_4 . Es ist S_3 eine maximale echte Untergruppe von S_4 ; cf. Beispiel 30. Es hat S_4 nur die Normalteiler A_4 , $\langle\, (1,2)(3,4),\ (1,3)(2,4) \,\rangle$ und 1 ; cf. Vorbemerkung in Lösung zu Aufgabe 30.(2). Davon liegt nur 1 in S_3 . Also ist $\Phi(\mathrm{S}_4) = 1$; cf. Bemerkung 124.(1).

(4) Sei p prim. Betrachte $G = \langle\, a \,:\, a^{p^3} \,\rangle \simeq \mathrm{C}_{p^3}$. Es ist $\Phi(G) = \langle a^{p^2} \rangle$; cf. Lemma 127.(2). In der Tat ist $\langle a^{p^2} \rangle$ die einzige maximale Untergruppe von G.

4.2 Eine Bemerkung

Bemerkung 129 Sei G eine Gruppe. Sei $H \trianglelefteqslant G$.

Der Gruppenmorphismus

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(H) \\ g & \longmapsto & (h \longmapsto {}^g h) \end{array}$$

hat den Kern $\mathrm{C}_G(H) \trianglelefteqslant G$. Er induziert somit den injektiven Gruppenmorphismus

$$\begin{array}{ccc} G/\mathrm{C}_G(H) & \xrightarrow{\ \iota\ } & \mathrm{Aut}(H) \\ g\mathrm{C}_G(H) & \longmapsto & (h \longmapsto {}^g h) \end{array}$$

Falls

$$\mathrm{C}_G(H) \ \leqslant\ H$$

ist, dann ist $\mathrm{C}_G(H) = \mathrm{C}_G(H) \cap H = \mathrm{C}_H(H) = \mathrm{Z}(H)$. Wir können unseren injektiven Gruppenmorphismus also

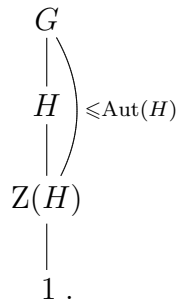
$$\begin{array}{ccc} G/\mathrm{Z}(H) & \xrightarrow{\ \iota\ } & \mathrm{Aut}(H) \\ g\mathrm{Z}(H) & \longmapsto & (h \longmapsto {}^g h)\ . \end{array}$$

schreiben.

Um G zu kennen, genügt es diesenfalls also, $\mathrm{Z}(H)$ zu kennen, das Bild $\mathrm{Im}(\iota) \leqslant \mathrm{Aut}(H)$ zu kennen und die kurz exakte Sequenz

$$\mathrm{Z}(H) \ \hookrightarrow\ G \ \overset{r}{\twoheadrightarrow}\ \mathrm{Im}(\iota)$$

zu untersuchen, wobei $r(g) := \iota(g\mathrm{Z}(H))$ für $g \in G$. Symbolisch wird



4.3 Die Fittinguntergruppe

Sei G eine endliche Gruppe. Schreibe $k := |\pi(G)|$ und $\pi(G) = \{\, p_i \,:\, i \in [1,k] \,\}$.

Definition 130 Für $p \in \pi(G)$ sei

$$\mathrm{O}_p(G) \;:=\; \bigcap_{P \in \mathrm{Syl}_p(G)} P \;.$$

Sei

$$\mathrm{F}(G) \;:=\; \mathrm{O}_{p_1}(G) \cdot \ldots \cdot \mathrm{O}_{p_k}(G)$$

die *Fittinguntergruppe* von G.

Bemerkung 131

(1) *Sei $p \in \pi(G)$. Es ist $\mathrm{O}_p(G) \trianglelefteq G$.*

(2) *Es ist $\mathrm{F}(G) \trianglelefteq G$.*

(3) *Es ist $\mathrm{F}(G)$ das terminale Element von $\{\, N \trianglelefteqslant G \,:\, N$ ist nilpotent$\,\}$.*
Kurz, für $N \trianglelefteqslant G$ ist N genau dann nilpotent, wenn $N \leqslant \mathrm{F}(G)$ ist.

(4) *Es ist $\Phi(G) \leqslant \mathrm{F}(G)$.*

Beweis.

Ad (1). Sei $\beta \in \mathrm{Aut}(G)$. Es ist $\mathrm{Syl}_p(G) \longrightarrow \mathrm{Syl}_p(G)$, $P \longmapsto \beta(P)$ wohldefiniert und bijektiv. Damit folgt

$$\beta(\mathrm{O}_p(G)) \;=\; \bigcap_{P \in \mathrm{Syl}_p(G)} \beta(P) \;=\; \bigcap_{\tilde{P} \in \mathrm{Syl}_p(G)} \tilde{P} \;=\; \mathrm{O}_p(G) \;.$$

Ad (2). Allgemein ist in einer Gruppe H mit $N,\ \tilde{N} \trianglelefteq H$ auch $N\tilde{N} \trianglelefteq H$, da für $\beta \in \mathrm{Aut}(H)$ sich $\beta(N\tilde{N}) = \beta(N) \cdot \beta(\tilde{N}) = N\tilde{N}$ ergibt; cf. Aufgabe 12.(2, 3).

Daher folgt $\mathrm{F}(G) \blacktriangleleft G$ aus (1).

Ad (3). Wir *behaupten,* daß $\mathrm{F}(G)$ nilpotent ist. Sei $p \in \pi(G)$. Wir müssen zeigen, daß $|\operatorname{Syl}_p(\mathrm{F}(G))| \overset{!}{=} 1$ ist; cf. Satz 89. Es genügt zu zeigen, daß es eine p-Sylowgruppe in $\mathrm{F}(G)$ gibt, die normal in $\mathrm{F}(G)$ liegt; cf. Satz 38.(2).

Sei o.E. $p = p_k$; cf. Aufgabe 12.(2). Schreibe $\mathrm{F}'(G) := \mathrm{O}_{p_1}(G) \cdot \ldots \cdot \mathrm{O}_{p_{k-1}}(G)$. Es ist $|\mathrm{F}'(G)|$ ein Teiler von $|\mathrm{O}_{p_1}(G)| \cdot \ldots \cdot |\mathrm{O}_{p_{k-1}}(G)|$, wie eine iterierte Anwendung von Aufgabe 12.(2) ergibt, und also nicht durch p teilbar. Somit ist $\mathrm{F}(G)/\mathrm{O}_p(G) = \mathrm{F}'(G)\mathrm{O}_p(G)/\mathrm{O}_p(G) \simeq \mathrm{F}'(G)/(\mathrm{F}'(G) \cap \mathrm{O}_p(G))$ von Ordnung teilerfremd zu p ; cf. Aufgabe 12.(2). Also ist $\mathrm{O}_p(G)$ eine p-Sylowgruppe von $\mathrm{F}(G)$. Aus $\mathrm{O}_p(G) \trianglelefteqslant G$ folgt $\mathrm{O}_p(G) \trianglelefteqslant \mathrm{F}(G)$; cf. (1). Dies zeigt die *Behauptung* ; cf. Satz 89.

Sei andererseits $N \trianglelefteqslant G$ mit N nilpotent gegeben. Wir haben $N \overset{!}{\leqslant} \mathrm{F}(G)$ zu zeigen.

Es ist $|\operatorname{Syl}_p(N)| = 1$ für $p \in \pi(N)$ und auch für $p \in \pi(G) \smallsetminus \pi(N)$; cf. Satz 89. Schreibe also $\operatorname{Syl}_p(N) = \{Q_p\}$ für $p \in \pi(G)$. Es ist $\prod_{i\in[1,k]} Q_{p_i} \xrightarrow{\sim} N$, $(q_i)_i \longmapsto q_1 \cdot \ldots \cdot q_k$; cf. Satz 89. Insbesondere ist $N = Q_{p_1} \cdot \ldots \cdot Q_{p_k}$.

Sei $p \in \pi(G)$. Wir haben nun $Q_p \overset{!}{\leqslant} \mathrm{F}(G)$ zu zeigen. Es genügt, $Q_p \overset{!}{\leqslant} \mathrm{O}_p(G)$ zu zeigen. Es ist $Q_p = \mathrm{O}_p(N) \blacktriangleleft N \trianglelefteqslant G$ und also $Q_p \trianglelefteqslant G$; cf. Bemerkung 131.(1). Es ist $Q_p \leqslant P$ für ein $P \in \operatorname{Syl}_p(G)$; cf. Satz 38.(4). Für jedes $\tilde{P} \in \operatorname{Syl}_p(G)$ gibt es ein $g \in G$ mit $\tilde{P} = {}^gP$, cf. Satz 38.(2), es wird also $Q_p = {}^gQ_p \leqslant {}^gP = \tilde{P}$. Somit ist in der Tat $Q_p \leqslant \bigcap_{\tilde{P}\in\operatorname{Syl}_p(G)} \tilde{P} = \mathrm{O}_p(G)$.

Ad (4). Es ist $\Phi(G)$ nilpotent; cf. Lemma 125. Es ist $\Phi(G) \trianglelefteqslant G$; cf. Bemerkung 124.(1). Also ist $\Phi(G) \leqslant \mathrm{F}(G)$; cf. (3). ▫

Beispiel 132

(1) Es ist $\mathrm{O}_2(\mathrm{S}_3) = 1$. Es ist $\mathrm{O}_3(\mathrm{S}_3) = \langle (1,2,3) \rangle = \mathrm{A}_3$. Also ist $\mathrm{F}(\mathrm{S}_3) = \mathrm{A}_3$. Es ist $\mathrm{F}(\mathrm{S}_3/\mathrm{F}(\mathrm{S}_3)) > 1$. Cf. auch Beispiel 128.(1) und Lemma 126.

(2) Es ist $\mathrm{O}_2(\mathrm{S}_4) = \langle\, (1,2)(3,4),\, (1,3)(2,4) \,\rangle =: V$. Es ist $\mathrm{O}_3(\mathrm{S}_4) = 1$. Also ist $\mathrm{F}(\mathrm{S}_4) = V$. Cf. auch Beispiel 128.(3).

(3) Sei $n \geqslant 5$. Unter den Normalteilern 1, A_n , S_n von S_n ist nur 1 nilpotent; cf. Aufgabe 20.(3), Beispiel 77.(3). Also ist $\mathrm{F}(\mathrm{S}_n) = 1$; cf. Bemerkung 131.(3).

(4) Sei N nilpotent. Es ist $\mathrm{F}(N) = N$, da $\mathrm{F}(N)$ der terminale nilpotente Normalteiler von N ist; cf. Bemerkung 131.(3). Cf. auch Lemma 127.(2).

Lemma 133 *Sei G eine endliche Gruppe. Schreibe $C := \mathrm{C}_G(\mathrm{F}(G))$.*

(1) *Ist G auflösbar und ist $\mathrm{F}(G) = 1$, dann ist auch $G = 1$.*

(2) *Es ist $\mathrm{F}\big(C/(C \cap \mathrm{F}(G))\big) = 1$.*

Beweis.

Ad (1). *Annahme,* es ist $G > 1$. Also gibt es ein $i \geqslant 0$ mit $G^{(i)} > 1$ und $G^{(i+1)} = 1$; cf. Satz 84. Somit ist $G^{(i)}$ ein abelscher Normalteiler von G; cf. Bemerkung 82.(2). Also ist $1 < G^{(i)} \leqslant \mathrm{F}(G)$; cf. Bemerkung 131.(3), Bemerkung 76. Wir haben einen *Widerspruch.*

Ad (2). Schreibe $\mathrm{F}(C/(C \cap \mathrm{F}(G))) =: U/(C \cap \mathrm{F}(G))$ mit $C \cap \mathrm{F}(G) \trianglelefteqslant U \trianglelefteqslant C$; cf. Aufgabe 17.(1, 2). Wir haben $U \overset{!}{\leqslant} \mathrm{F}(G)$ zu zeigen. Dank Bemerkung 131.(3) genügt es hierfür zu zeigen, daß U ein nilpotenter Normalteiler von G ist.

Es ist $C = \mathrm{C}_G(\mathrm{F}(G)) \trianglelefteqslant G$, da $\mathrm{F}(G) \trianglelefteqslant G$ ist; cf. Bemerkungen 18 und 131.(2).

Es ist $U/(C \cap \mathrm{F}(G)) \blacktriangleleft C/(C \cap \mathrm{F}(G)) \trianglelefteqslant G/(C \cap \mathrm{F}(G))$; cf. Bemerkung 131.(2). Also ist $U/(C \cap \mathrm{F}(G)) \trianglelefteqslant G/(C \cap \mathrm{F}(G))$; cf. Bemerkung 80.(2). Somit ist $U \trianglelefteqslant G$.

Für $x \in C \cap \mathrm{F}(G) \leqslant \mathrm{F}(G)$ ist für $u \in U \leqslant C = \mathrm{C}_G(\mathrm{F}(G))$ dann ${}^{u}x = x$, aber auch $x \in U$, also insgesamt $x \in \mathrm{Z}(U)$. Somit ist $C \cap \mathrm{F}(G) \leqslant \mathrm{Z}(U)$.

Es ist $U/(C \cap \mathrm{F}(G)) = \mathrm{F}(C/(C \cap \mathrm{F}(G)))$ nilpotent; cf. Bemerkung 131.(3).

Hieraus folgt U nilpotent; cf. Aufgabe 32.(6). ▫

Satz 134 (Zentralisator der Fittinguntergruppe)

Sei G eine auflösbare endliche Gruppe.

Es ist $\mathrm{C}_G(\mathrm{F}(G)) \leqslant \mathrm{F}(G)$.

Damit sind wir in der Situation, die in Bemerkung 129 beschrieben wird.

Beweis. Schreibe $C := \mathrm{C}_G(\mathrm{F}(G))$. Es ist $\mathrm{F}(G) \trianglelefteqslant G$; cf. Bemerkung 131.(2). Also ist $C \trianglelefteqslant G$; cf. Bemerkung 18.

Es genügt, $C/(C \cap \mathrm{F}(G)) \overset{!}{=} 1$ zu zeigen.

Da G auflösbar ist, gilt dies auch für C und damit für $C/(C \cap \mathrm{F}(G))$; cf. Aufgabe 32.(2). Somit genügt es, $\mathrm{F}(C/(C \cap \mathrm{F}(G))) \overset{!}{=} 1$ zu zeigen; cf. Lemma 133.(1). Dies aber folgt mit Lemma 133.(2). ▫

Beispiel 135 Betrachte S_4. Es ist S_4 auflösbar; cf. Aufgabe 30, Bemerkung 74.(1). Es ist $\mathrm{F}(\mathrm{S}_4) = \langle \underbrace{(1,2)(3,4)}_{=:a}, \underbrace{(1,3)(2,4)}_{=:b} \rangle =: V$; cf. Beispiel 132.(2).

Es ist $\mathrm{C}_{\mathrm{S}_4}(V) \leqslant V$; cf. Satz 134. Da V abelsch ist, ist also $\mathrm{C}_{\mathrm{S}_4}(V) = \mathrm{Z}(V) = V$. Somit ist V der Kern des Gruppenmorphismus

$$\begin{array}{ccc} \mathrm{S}_4 & \longrightarrow & \mathrm{Aut}(V) \\ \sigma & \longmapsto & (v \mapsto {}^{\sigma}v) \end{array}$$

Wir haben den Isomorphismus

$$\begin{array}{rcl} \mathrm{GL}_2(\mathbf{F}_2) & \xrightarrow{\sim} & \mathrm{Aut}(V) \\ \left(\begin{smallmatrix} i+2\mathbf{Z} & j+2\mathbf{Z} \\ k+2\mathbf{Z} & \ell+2\mathbf{Z} \end{smallmatrix}\right) & \longmapsto & (a \mapsto a^i b^k,\ b \mapsto a^j b^\ell)\ . \end{array}$$

Insbesondere ist $|\mathrm{Aut}(V)| = 6$. Somit ist der induzierte injektive Gruppenmorphismus

$$\begin{array}{rcl} \mathrm{S}_4/V & \xrightarrow{\iota} & \mathrm{Aut}(V) \\ \sigma V & \longmapsto & (\upsilon \mapsto {}^{\sigma}\upsilon) \end{array}$$

auch sujektiv, zusammen also ein Isomorphismus. Cf. Bemerkung 129.

In der Tat ist $\mathrm{GL}_2(\mathbf{F}_2) \simeq \mathrm{S}_3$; cf. Aufgabe 19.(3). Es folgt $\mathrm{S}_4/V \simeq \mathrm{S}_3$. Cf. Aufgabe 23.(3).

4.4 Die erweiterte Fittinguntergruppe

Wir folgen [**4,** §6.5].

Sei G eine endliche Gruppe. Wir werden wiederholt und kommentarlos von Aufgabe 12.(2) Gebrauch machen.

Lemma 136 *Sei $N \trianglelefteq G$ mit N abelsch und mit G/N perfekt.*

Dann ist $G^{(1)}$ perfekt.

Beweis. Es ist $G/N = (G/N)^{(1)} = G^{(1)}N/N \simeq G^{(1)}/(G^{(1)} \cap N)$; cf. Aufgabe 13.(1).

Also ist $G^{(1)}/(G^{(1)} \cap N) = (G^{(1)}/(G^{(1)} \cap N))^{(1)} = (G^{(2)}(G^{(1)} \cap N))/(G^{(1)} \cap N)$; cf. Aufgabe 13.(1).

Es folgt

$$G \ = \ G^{(1)}N \ = \ G^{(2)}(G^{(1)} \cap N)N \ = \ G^{(2)}N$$

und also $G/G^{(2)} = (G^{(2)}N)/G^{(2)} \simeq N/(N \cap G^{(2)})$. Da N abelsch ist, folgt $G^{(1)} \leqslant G^{(2)}$; cf. Aufgabe 13.(4). Insgesamt ist also $G^{(1)} = G^{(2)}$. ▫

Definition 137 Es heißt G *quasieinfach,* wenn G perfekt ist und $G/\mathrm{Z}(G)$ einfach ist.

Insbesondere ist $G/\mathrm{Z}(G)$ dann nichtabelsch, da ansonsten G auflösbar und > 1 und also nicht perfekt wäre; cf. Aufgabe 32.(1), Satz 84.

Somit ist G dann nichtauflösbar; cf. Aufgabe 32.(2), Bemerkung 74.(1).

Beispiel 138 Sei F ein Körper. Sei $n \geqslant 2$. Sei $(n, |F|) \notin \{\, (2,2),\ (2,3) \,\}$.

Es ist $\mathrm{SL}_n(F)$ quasieinfach; cf. Aufgabe 18.(1, 2), Satz 49.

Definition 139 Sei $H \leqslant G$. Es heißt H *subnormal* in G, geschrieben $H \trianglelefteq\trianglelefteq G$, wenn es $s \geqslant 0$ und $U_i \leqslant G$ für $i \in [0, s]$ gibt mit

$$H \;=\; U_s \;\trianglelefteq\; U_{s-1} \;\trianglelefteq\; \ldots \;\trianglelefteq\; U_1 \;\trianglelefteq\; U_0 \;=\; G\,.$$

Bemerkung 140 *Sei G quasieinfach. Sei $H \trianglelefteq\trianglelefteq G$. Dann ist $H \leqslant \mathrm{Z}(G)$ oder $H = G$.*

Beweis. Es ist auch $H\mathrm{Z}(G) \trianglelefteq\trianglelefteq G$ und also $H\mathrm{Z}(G)/\mathrm{Z}(G) \trianglelefteq\trianglelefteq G/\mathrm{Z}(G)$. Da aber $G/\mathrm{Z}(G)$ einfach ist, ist $H\mathrm{Z}(G) = \mathrm{Z}(G)$ oder $H\mathrm{Z}(G) = G$. Ersterenfalls ist $H \leqslant \mathrm{Z}(G)$. Letzterenfalls ist $H\mathrm{Z}(G) = G$, also $H \trianglelefteq H\mathrm{Z}(G) = G$ und $G/H = H\mathrm{Z}(G)/H \simeq \mathrm{Z}(G)/H \cap \mathrm{Z}(G)$ abelsch, was $G = G^{(1)} \leqslant H \leqslant G$ und also $H = G$ zur Folge hat; cf. Aufgabe 13.(4). ▫

Bemerkung 141 *Sei $H \trianglelefteq\trianglelefteq G$. Dann ist* $\mathrm{F}(H) \leqslant \mathrm{F}(G)$.

Beweis. Dank möglicher Iteration genügt es, die Aussage im Falle $H \trianglelefteq G$ zu zeigen.

Aus $\mathrm{F}(H) \blacktriangleleft H \trianglelefteq G$ folgt $\mathrm{F}(H) \trianglelefteq G$; cf. Bemerkungen 131.(2) und 80.(2). Da zudem $\mathrm{F}(H)$ nilpotent ist, folgt $\mathrm{F}(H) \leqslant \mathrm{F}(G)$; cf. Bemerkung 131.(3). ▫

Definition 142

Es heißt $K \leqslant G$ eine *Komponente* von G, wenn K quasieinfach und $K \trianglelefteq\trianglelefteq G$ ist.

Sei $\mathrm{Komp}(G) := \{\, K \leqslant G \,:\, K \text{ ist Komponente von } G \,\}$.

Bemerkung 143 *Sei $K \in \mathrm{Komp}(G)$.*

(1) *Sei $K \leqslant H \leqslant G$. Dann ist $K \in \mathrm{Komp}(H)$.*

(2) *Sei $K \not\leqslant N \trianglelefteq G$. Dann ist $KN/N \in \mathrm{Komp}(G/N)$.*

(3) *Ist $G \trianglelefteq\trianglelefteq \tilde{G}$, dann ist $K \in \mathrm{Komp}(\tilde{G})$.*

Beweis.

Ad (1). Zu zeigen ist $K \trianglelefteq\trianglelefteq H$. Aber ist $K = U_s \trianglelefteq \ldots \trianglelefteq U_0 = G$, dann ist auch $K = K \cap H = U_s \cap H \trianglelefteq \ldots \trianglelefteq U_0 \cap H = G \cap H = H$.

Ad (2). Zu zeigen ist zum einen $KN/N \trianglelefteq\trianglelefteq G/N$, i.e. $KN \trianglelefteq\trianglelefteq G$; cf. Aufgabe 17.(3). Aber ist $K = U_s \trianglelefteq \ldots \trianglelefteq U_0 = G$, dann ist auch $KN = U_sN \trianglelefteq \ldots \trianglelefteq U_0N = GN = N$; beachte hierbei für $i \in [1, s]$, für $u_i \in U_i$ und $n \in N$, daß ${}^{n}u_i = u[u^-, n] \in U_iN$ ist.

Zum zweiten ist zu zeigen, daß KN/N perfekt ist. Aber $KN/N \simeq K/(K \cap N)$ und $(K/(K \cap N))^{(1)} = K^{(1)}(K \cap N)/(K \cap N) = K(K \cap N)/(K \cap N) = K/(K \cap N)$; cf. Aufgabe 13.(1).

Da $KN/N \simeq K/(K \cap N)$, ist zum dritten zu zeigen, daß $(K/(K \cap N))/\mathrm{Z}(K/(K \cap N))$ einfach ist. Schreibe $\mathrm{Z}(K/(K \cap N)) = Z/(K \cap N)$ mit $K \cap N \trianglelefteq Z \trianglelefteq K$. Es ist $\mathrm{Z}(K) \leqslant Z$.

Also ist $Z = \mathrm{Z}(K)$ oder $Z = K$; cf. Bemerkung 140. Letzterenfalls *wäre* $K/(K \cap N)$ abelsch. Da aber $K/(K \cap N)$ perfekt ist, zöge dies $K/(K \cap N) = 1$ nach sich, also $K \leqslant N$, was *nicht* der Fall ist. Somit ist $Z = \mathrm{Z}(K)$.

Es folgt, daß $(K/(K \cap N))/\mathrm{Z}(K/(K \cap N)) = (K/(K \cap N))/(\mathrm{Z}(K)/(K \cap N)) \simeq K/\mathrm{Z}(K)$ eine einfache Gruppe ist. □

Ad (3). Subnormalität ist transitiv. □

Lemma 144 *Seien $Z \leqslant \mathrm{Z}(G) \leqslant G$. Sei $E \leqslant G$. Sei $EZ/Z \in \mathrm{Komp}(G/Z)$.*

Dann ist $E^{(1)} \in \mathrm{Komp}(G)$.

Beweis. Aus $EZ/Z \trianglelefteqslant\trianglelefteqslant G/Z$ folgt $E^{(1)} \trianglelefteqslant E \trianglelefteqslant EZ \trianglelefteqslant\trianglelefteqslant G$.

Da EZ/Z perfekt ist, ist $EZ/Z = (EZ/Z)^{(1)} = E^{(1)}Z/Z$; cf. Aufgabe 13.(1).

Da EZ/Z perfekt ist, gilt dies auch für $(EZ)^{(1)} = E^{(1)}$; cf. Lemma 136.

Bleibt zu zeigen, daß $E^{(1)}/\mathrm{Z}(E^{(1)})$ einfach ist. Sei $\mathrm{Z}(E^{(1)}) \trianglelefteqslant N \trianglelefteqslant E^{(1)}$. Es ist zu zeigen, daß $N = E^{(1)}$ oder $\mathrm{Z}(E^{(1)}) = N$ ist; cf. Aufgabe 17.(3).

Es ist $NZ \trianglelefteqslant E^{(1)}Z$ und also $NZ/Z \trianglelefteqslant E^{(1)}Z/Z = EZ/Z$. Da EZ/Z quasieinfach ist, folgt $NZ/Z \leqslant \mathrm{Z}(EZ/Z)$ oder $NZ/Z = EZ/Z$; cf. Bemerkung 140.

Letzerenfalls ist $N \leqslant E^{(1)} \leqslant E \leqslant NZ$, also $N(Z \cap E^{(1)}) = NZ \cap E^{(1)} = E^{(1)}$; cf. Bemerkung 118. Da $E^{(1)}/N = N(Z \cap E^{(1)})/N \simeq (Z \cap E^{(1)})/(Z \cap E^{(1)} \cap N)$ abelsch ist, folgt $E^{(1)} = E^{(2)} \leqslant N \leqslant E^{(1)}$, also $N = E^{(1)}$; cf. Aufgabe 13.(4).

Ersterenfalls ist $NZ/Z \leqslant \mathrm{Z}(EZ/Z) = \mathrm{Z}(E^{(1)}Z/Z)$ und also $[N, E^{(1)}] \leqslant Z$. Daher ist $[[N, E^{(1)}], E^{(1)}] = 1$. Da $E^{(1)}$ perfekt ist, folgt $[N, E^{(1)}] = 1$; cf. Aufgabe **??**.(3). I.e. es ist $N \leqslant \mathrm{Z}(E^{(1)})$. Insgesamt ist $\mathrm{Z}(E^{(1)}) = N$. □

Lemma 145 *Sei $K \in \mathrm{Komp}(G)$. Sei $L \trianglelefteqslant\trianglelefteqslant G$.*

Dann ist $K \leqslant L$ oder $[K, L] = 1$.

Beweis. Annahme, es gibt eine endliche Gruppe, die eine Komponente und einen Subnormalteiler so enthält, daß die Komponente nicht im Subnormalteiler liegt und daß der Kommutator dieser beiden nicht vertauscht. Wähle eine solche Gruppe G minimaler Ordnung, darin dann $K \in \mathrm{Komp}(G)$ und $L \trianglelefteqslant\trianglelefteqslant G$ mit $K \not\leqslant L$ und $[K, L] > 1$.

Ist $K = G$, dann ist G quasieinfach und also $L \leqslant \mathrm{Z}(G)$ oder $L = G$; cf. Bemerkung 140. Ersterenfalls ist $[K, L] = 1$, zweiterenfalls ist $K \leqslant G$. Dies tritt also nicht auf, i.e. es ist $K < G$. Somit gibt es $K \trianglelefteqslant\trianglelefteqslant N \triangleleft G$.

Ist $L = G$, dann ist $K \leqslant L$. Dies tritt also nicht auf, i.e. es ist $L < G$. Somit gibt es $L \trianglelefteqslant\trianglelefteqslant N \triangleleft G$.

Daher ist $L' := [L, K] \leqslant N \cap M$. Ferner ist $K \leqslant \mathrm{N}_M([L, K]) = \mathrm{N}_M(L') =: G'$; cf. Aufgabe **??**.(5).

Es ist $K \in \mathrm{Komp}(G')$; cf. Bemerkung 143.(1). Es ist $L' \trianglelefteq G'$, also $L' \trianglelefteq\trianglelefteq G'$. Wegen der Minimalität von $|G|$ und wegen $|G'| \leqslant |M| < |G|$ folgt nun $K \leqslant L'$ oder $[K, L'] = 1$.

Ersterenfalls folgt $K \leqslant L' \leqslant N$ und also $K \in \mathrm{Komp}(N)$ ist; cf. Bemerkung 143.(1). Ferner ist $L \trianglelefteq\trianglelefteq N$. Wegen der Minimalität von $|G|$ und wegen $|N| < |G|$ liefert dies $K \leqslant L$ oder $[K, L] = 1$.

Zweiterenfalls ist $1 = [K, L'] = [K, [K, L]] = [[L, K], K]$, wegen K perfekt also $[L, K] = 1$; cf. Aufgabe **??**.(3). ▫

Korollar 146 *Seien* K, $\tilde{K} \in \mathrm{Komp}(G)$.

Dann ist $K = \tilde{K}$ *oder* $[K, \tilde{K}] = 1$.

Beweis. Sei $[K, \tilde{K}] > 1$. Zu zeigen ist $K \overset{!}{=} \tilde{K}$. Wegen Symmetrie genügt es, $K \overset{!}{\leqslant} \tilde{K}$ zu zeigen. Dies aber folgt wegen $[K, \tilde{K}] > 1$ aus Lemma 145. ▫

Definition 147 Sei $t := |\mathrm{Komp}(G)|$. Schreibe $\mathrm{Komp}(G) = \{ K_i : i \in [1, t] \}$.

Sei $\mathrm{E}(G) := K_1 K_2 \cdot \ldots \cdot K_t \cdot 1$ die *Schicht* von G.

Sei $\mathrm{FE}(G) := \mathrm{F}(G)\,\mathrm{E}(G)$ die *erweiterte Fittinguntergruppe* von G; cf. Definition 130.

> Oft wird $\mathrm{FE}(G)$ auch $\mathrm{F}^*(G)$ geschrieben und als *verallgemeinerte Fittinguntergruppe* bezeichnet.

Bemerkung 148

(1) *Es ist* $\mathrm{E}(G) \blacktriangleleft G$. *Es ist* $K \trianglelefteq \mathrm{E}(G)$ *für* $K \in \mathrm{Komp}(G)$.

(2) *Ist* G *auflösbar, dann ist* $\mathrm{Komp}(G) = \emptyset$, *sowie* $\mathrm{E}(G) = 1$ *und* $\mathrm{FE}(G) = \mathrm{F}(G)$.

(3) *Es ist* $[\mathrm{E}(G), \mathrm{F}(G)] = 1$.

(4) *Es ist* $\mathrm{FE}(G) \blacktriangleleft G$.

Beweis.

Ad (1). Wir haben den Gruppenmorphismus $\prod_{i \in [1,t]} K_i \longrightarrow G$, $(k_i)_i \longmapsto k_1 k_2 \cdot \ldots \cdot k_t$; cf. Aufgabe 2.(3), Korollar 146. Sein Bild ist die Untergruppe $\mathrm{E}(G) \leqslant G$; cf. auch Aufgabe 12.

Sei $\beta \in \mathrm{Aut}(G)$. Sei $i \in [1, t]$. Es genügt, $\beta(K_i) \overset{!}{\leqslant} \mathrm{E}(G)$ zu zeigen. Es genügt, $\beta(K_i) \overset{!}{\in} \mathrm{Komp}(G)$ zu zeigen. Aber aus $K_i \trianglelefteq\trianglelefteq G$ folgt $\beta(K_i) \trianglelefteq\trianglelefteq \beta(G) = G$, aus $K_i^{(1)} = K_i$ folgt $\beta(K_i)^{(1)} \overset{\text{A. 13.(1)}}{=} \beta(K_i^{(1)}) = \beta(K_i)$ und $\beta(K_i)/\mathrm{Z}(\beta(K_i)) = \beta(K_i)/\beta(\mathrm{Z}(K_i))$ ist isomorph zu $K_i/\mathrm{Z}(K_i)$ via des von β induzierten Isomorphismus, mithin einfach. Also ist $\beta(K_i)$ tatsächlich eine Komponente von G.

Sei nun $K \in \mathrm{Komp}(G)$. Wir haben $K \overset{!}{\trianglelefteqslant} \mathrm{E}(G)$ zu zeigen. Sei $\tilde{K} \in \mathrm{Komp}(G)$. Sei $\tilde{x} \in \tilde{K}$. Sei $y \in K$. Wir haben ${}^{\tilde{x}}y \overset{!}{\in} K$ zu zeigen. Ist $\tilde{K} = K$, so folgt dies aus $K \leqslant G$. Ist $\tilde{K} \neq K$, dann ist $[K, \tilde{K}] = 1$ dank Korollar 146 und also ${}^{\tilde{x}}y = y \in K$.

Ad (2). Sei G auflösbar. Wir haben $\mathrm{Komp}(G) = \emptyset$ zu zeigen. *Wäre* $K \in \mathrm{Komp}(G)$, dann wäre wegen $K \leqslant G$ auch K auflösbar dank Aufgabe 32.(2), was *nicht so ist.* Da $K \leqslant G$, ist K auflösbar.

Ad (3). Ist $\mathrm{E}(G) = 1$, so ist nichts zu zeigen.

Sei also $\mathrm{E}(G) > 1$. Dann können wir $K \in \mathrm{Komp}(G)$ wählen. *Annahme*, es ist $\mathrm{E}(G) \leqslant \mathrm{F}(G)$. Dann ist $K \leqslant \mathrm{F}(G)$ und somit $K \in \mathrm{Komp}(\mathrm{F}(G))$; cf. Bemerkung 143.(1). Aber $\mathrm{F}(G)$ ist nilpotent und also auflösbar; cf. Bemerkungen 131.(3) und 76. Also ist $\mathrm{Komp}(\mathrm{F}(G)) = \emptyset$. Wir haben einen *Widerspruch.* Also ist $\mathrm{E}(G) \not\leqslant \mathrm{F}(G)$.

Da $\mathrm{F}(G) \blacktriangleleft G$, ist insbesondere $\mathrm{F}(G) \trianglelefteqslant\trianglelefteqslant G$; cf. Bemerkung 131.(2). Mit Lemma 145 folgt $[\mathrm{E}(G), \mathrm{F}(G)] = 1$.

Ad (4). Da $\mathrm{F}(G) \blacktriangleleft G$ und $\mathrm{E}(G) \blacktriangleleft G$, ist $\mathrm{FE}(G) = \mathrm{F}(G)\mathrm{E}(G) \blacktriangleleft G$; cf. Beweis zu Bemerkung 131.(2). ▫

Lemma 149

(1) *Ist* N *minimal in* $\{ M \trianglelefteqslant G : M > 1 \}$*, dann ist* $N \leqslant \mathrm{FE}(G)$.

(2) *Ist* $K \in \mathrm{Komp}(G)$ *und ist* $\mathrm{Z}(K) = 1$*, dann ist das Normalteilererzeugnis* ${}^{G}\langle\!| K |\!\rangle$ *minimal in* $\{ M \trianglelefteqslant G : M > 1 \}$.

(3) *Ist* $G > 1$*, dann ist* $\mathrm{FE}(G) > 1$.

Cf. Aufgabe 37.

Beweis.

Ad (1). Ist N abelsch, so ist N nilpotent und also $N \trianglelefteqslant \mathrm{F}(G) \leqslant \mathrm{FE}(G)$; cf. Bemerkungen 76 und 131.(3).

Sei nun N nichtabelsch. Gemäß Aufgabe 37.(1, 2) gibt es einen Isomorphismus $f : S^{\times k} \xrightarrow{\sim} N$ für ein $k \geqslant 1$ und eine einfache Gruppe S. Sei

$$S_j := \{ (s_i)_i \in S^{\times k} : s_i = 1 \text{ für } i \in [1,k] \smallsetminus \{j\} \}$$

für $j \in [1,k]$. Für $j \in [1,k]$ ist $S_j \trianglelefteqslant S^{\times k}$, also $f(S_j) \trianglelefteqslant N$ und somit $f(S_j) \trianglelefteqslant\trianglelefteqslant N$; da $f(S_j)$ einfach und nichtabelsch ist, ist $f(S_j)$ zudem perfekt; insgesamt $f(S_j) \in \mathrm{Komp}(G)$. Es folgt $N = f(S) = f(\langle S_j : j \in [1,k] \rangle) \leqslant \mathrm{E}(G) \leqslant \mathrm{FE}(G)$.

Ad (2). Nach Konstruktion ist $N := {}^{G}\langle\!| K |\!\rangle \trianglelefteqslant G$.

Sei $G = \sqcup_{i \in [1,\ell]} g_i \mathrm{N}_G(K)$, wobei $\ell := [G : \mathrm{N}_G(K)]$ und $g_i \in G$ für $i \in [1,\ell]$. Dann ist $\{ {}^{g}K : g \in G \} = \{ {}^{g_i}K : i \in [1,\ell] \}$, und es ist ${}^{g_i}K \neq {}^{g_j}K$ für $i, j \in [1,\ell]$ mit $i \neq j$. Da

mit K auch ${}^{g_i}K$ eine Komponente von G ist, folgt $[{}^{g_i}K, {}^{g_j}K] = 1$; cf. Korollar 146. Somit gibt es einen surjektiven Gruppenmorphismus $u : K^{\times \ell} \longrightarrow G$, $(x_i)_i \longmapsto {}^{g_1}x \cdot {}^{g_2}x \cdot \ldots \cdot {}^{g_\ell}x$; cf. Aufgabe 2.(3). Ferner ist ${}^{g_i}K \trianglelefteq N$ für $i \in [1, k]$.

Sei $i \in [1, k]$. *Annahme,* es ist ${}^{g_i}K \leqslant {}^{g_1}K \cdot \ldots \cdot {}^{g_{i-1}}K =: L$. Da $[{}^{g_i}K, L] = 1$ ist, folgt ${}^{g_i}K \leqslant \mathrm{Z}({}^{g_1}K \cdot \ldots \cdot {}^{g_{i-1}}K)$. Aber K ist nichtabelsch. Wir haben einen *Widerspruch.* Es folgt ${}^{g_i}K \not\leqslant L$, i.e. ${}^{g_i}K \cap L \lhd {}^{g_i}K$. Da ${}^{g_i}K$ einfach ist, folgt ${}^{g_i}K \cap L = 1$.

Also ist u ein Isomorphismus; cf. Lösung zu Aufgabe 2.(3).

Sei nun $M \trianglelefteq G$ mit $1 < M \leqslant N$ gegeben. Wir haben $M \overset{!}{=} N$ zu zeigen. Es genügt, ${}^{g}K \overset{!}{\leqslant} M$ zu zeigen für ein $g \in G$, da daraus wegen $M \trianglelefteq G$ dann ${}^{g}K \leqslant M$ für alle $g \in G$ und somit $N \leqslant M$ folgt.

Es ist $u^{-1}(M) \trianglelefteq K^{\times \ell}$. Da $u^{-1}(M) > 1$, gibt es ein $j \in [1, k]$ mit

$$K_j \;:=\; \{\, (x_i)_i \,:\, x_i = 1 \text{ für } i \in [1, \ell] \smallsetminus \{j\} \,\} \;\leqslant\; u^{-1}(M) \;;$$

cf. Aufgabe 37.(3). Folglich ist ${}^{g_j}K = u(K_j) \leqslant M$.

Ad (3). Ist $G > 1$, dann ist $G \in \{\, M \trianglelefteq G \,:\, M > 1 \,\}$, und folglich hat $\{\, M \trianglelefteq G \,:\, M > 1 \,\}$ ein minimales Element N. Gemäß (1) ist $\mathrm{FE}(G) \geqslant N > 1$. ▫

Lemma 150 *Sei* $H \trianglelefteqslant G$. *Dann ist* $\mathrm{E}(H) \leqslant \mathrm{E}(G)$ *und* $\mathrm{FE}(H) \leqslant \mathrm{FE}(G)$.

Beweis. Es ist $\mathrm{F}(H) \leqslant \mathrm{F}(G)$; cf. Bemerkung 141. Also genügt es, $\mathrm{E}(H) \overset{!}{\leqslant} \mathrm{E}(G)$ zu zeigen.

Sei $K \in \mathrm{Komp}(H)$. Wir haben $K \overset{!}{\leqslant} \mathrm{E}(G)$ zu zeigen. Aber in der Tat ist $K \in \mathrm{Komp}(G)$ und somit $K \leqslant \mathrm{E}(G)$; cf. Bemerkung 143.(3). ▫

Satz 151 (Zentralisator der erweiterten Fittinguntergruppe)

Wir erinnern an die endliche Gruppe G *und an ihre erweiterte Fittinguntergruppe* $\mathrm{FE}(G)$ *; cf. Definition* 147.

Es ist $\mathrm{C}_G(\mathrm{FE}(G)) \leqslant \mathrm{FE}(G)$.

> Damit sind wir in der Situation, die in Bemerkung 129 beschrieben wird.
>
> Cf. Satz 134 und Bemerkung 148.(4).

Beweis. Schreibe $C := \mathrm{C}_G(\mathrm{FE}(G))$. Da $\mathrm{FE}(G) \trianglelefteq G$, ist $C \trianglelefteq G$; cf. Bemerkungen 148.(4) und 18. Also ist $\mathrm{FE}(C) \leqslant \mathrm{FE}(G)$; cf. Lemma 150.

Es ist $Z := \mathrm{Z}(C) \trianglelefteq C$ abelsch, mithin nilpotent und somit $Z \leqslant \mathrm{F}(C) \leqslant \mathrm{FE}(C)$; cf. Bemerkung 131.(3).

Es genügt, $\mathrm{FE}(C/Z) \overset{!}{=} 1$ zu zeigen, da dann $C/Z = 1$, i.e. $C \leqslant Z$ folgt, was $C \leqslant \mathrm{FE}(G)$ nach sich zieht.

Für $x \in \mathrm{FE}(C)$ und $c \in C$ ist $x \in \mathrm{FE}(G)$ und also $[x,c] = 1$. Somit ist $\mathrm{FE}(C) \leqslant Z$. Insgesamt ist also $\mathrm{FE}(C) = Z$.

Schreibe $\mathrm{F}(C/Z) = N/Z$ mit $Z \trianglelefteqslant N \trianglelefteqslant C$; cf. Aufgabe 17.(3). Mit N/Z ist auch N nilpotent; cf. Bemerkung 131.(3), Aufgabe 32.(6). Also ist $Z \leqslant N \leqslant \mathrm{F}(C) = Z$ und somit $N = Z$, i.e. $\mathrm{F}(C/Z) = N/Z = 1$; cf. Bemerkung 131.(3).

Es bleibt $\mathrm{E}(C/Z) \stackrel{!}{=} 1$ zu zeigen, i.e. $\mathrm{Komp}(C/Z) \stackrel{!}{=} \emptyset$. *Annahme,* es gibt $K \in \mathrm{Komp}(C/Z)$. Schreibe $K = L/Z$ mit $Z \leqslant L \leqslant C$; cf. Aufgabe 17.(1). Es ist $L^{(1)} \in \mathrm{Komp}(C)$; cf. Lemma 144. Es ist $L^{(1)} > 1$ perfekt, also nichtabelsch. Andererseits ist $L^{(1)} \leqslant \mathrm{FE}(C) = Z$, was wegen Z abelsch auch $L^{(1)}$ abelsch nach sich zieht. Wir haben einen *Widerspruch.* ▫

Beispiel 152 Sei Q eine quasieinfache endliche Gruppe; cf. e.g. Beispiel 138.

Sei H eine endliche Gruppe. Sei $m \geqslant 1$. Sei $\beta : H \longrightarrow \mathrm{S}_m$ ein Gruppenmorphismus, mittels dessen $[1,m]$ zu einer H-Menge wird; cf. Beispiel 2.(2).

Sei $\mathrm{Kern}(\beta)$ als auflösbar vorausgesetzt.

Wir bilden das Kranzprodukt

$$G \;:=\; Q \wr_\beta H \;;$$

cf. Definition 97.

Schreibe $Q_j := \{\, (\,(q_i)_i\,,\, h\,) \in G \,:\, q_i = 1 \text{ für } i \in [1,m] \smallsetminus \{j\}, \text{ sowie } h = 1 \,\}$ für $j \in [1,m]$.

Schreibe $N := \{\, (\,(q_i)_i\,,\, h\,) \in G \,:\, h = 1 \,\}$.

Schreibe $B := \{\, (\,(q_i)_i\,,\, h\,) \in G \,:\, q_i = 1 \text{ für } i \in [1,m], \text{ sowie } h \in \mathrm{Kern}(\beta) \,\}$.

Sei $j \in [1,m]$. Es ist $Q_j \trianglelefteqslant N \trianglelefteqslant G$. Folglich ist $Q_j \trianglelefteqslant\trianglelefteqslant G$. Desweiteren ist $Q_j \xrightarrow{\sim} Q$, $(\,(q_i)_i\,,\, h\,) \longmapsto q_j$. Also ist $Q_j \in \mathrm{Komp}(G)$.

Insgesamt folgt $\{\, Q_i \,:\, i \in [1,m] \,\} \leqslant \mathrm{Komp}(G)$.

Es ist $B \xrightarrow{\sim} \mathrm{Kern}(\beta)$, $(\,(q_i)_i\,,\, h\,) \longmapsto h$. Also ist B auflösbar.

Es ist $B \leqslant \mathrm{C}_G(N)$. Also ist $NB \leqslant G$; cf. Aufgabe 12.(2). Es ist auch $B \leqslant \mathrm{C}_G(\mathrm{Z}(N))$. Also ist auch $\mathrm{Z}(N)B \leqslant G$.

Wir *behaupten,* es ist $\mathrm{C}_G(N) = \mathrm{Z}(N)B$. Zu zeigen ist nur $\mathrm{C}_G(N) \stackrel{!}{\leqslant} \mathrm{Z}(N)B$. Sei $(\,(q_i)_i\,,\, h\,) \in \mathrm{C}_G(N)$. Wir haben $\beta(h) \stackrel{!}{=} \mathrm{id}$ und $q_i \stackrel{!}{\in} \mathrm{Z}(Q)$ für $i \in [1,m]$ zu zeigen.

Annahme, es gibt $k \in [1,m]$ mit $h \cdot k \neq k$. Wähle $x \in Q \smallsetminus \{1\}$. Betrachte $n := ((1,\ldots,1,x,1,\ldots,1),\, 1) \in N$, wobei der Eintrag x sich an Position k des Tupels befinde. Es ist

$$((1,\ldots,1,x,1,\ldots,1),\, 1) \cdot (\,(q_i)_i\,,\, h\,) \;=\; ((q_1,\ldots,q_{k-1},xq_k,q_{k+1},\ldots,q_m),\, h)$$

und

$$(\,(q_i)_i\,,\, h\,) \cdot ((1,\ldots,1,x,1,\ldots,1),\, 1) \;=\; ((q_1,\ldots,q_{h\cdot k-1},q_{h\cdot k}x,q_{h\cdot k+1},\ldots,q_m),\, h)\;.$$

Da $h \cdot k \neq k$, folgt $xq_k = q_k$ und also $x = 1$. Wir haben einen *Widerspruch.* Somit ist $\beta(h) = \mathrm{id}$.

Sei nun $(\,(x_i)_i\,,\,1) \in N$ gegeben. Dann ist

$$(\,(x_i)_i\,,\,1\,) \;=\; {}^{(\,(q_i)_i\,,\,h\,)}(\,(x_i)_i\,,\,1\,) \;=\; (\,({}^{q_i}x_i)_i\,,\,1\,)\,.$$

Somit ist $q_i \in \mathrm{Z}(Q)$ für $i \in [1,n]$. Dies zeigt die *Behauptung.*

Insbesondere ist $\mathrm{C}_G(N) = \mathrm{Z}(N)B$ auflösbar; cf. Aufgabe 32.(3).

Gäbe es ein $K \in \mathrm{Komp}(G)$ mit $K \notin \{\, Q_i \,:\, i \in [1,m]\,\}$, so wäre $[K, Q_i] = 1$ für $i \in [1,m]$ dank Korollar 146 und also $K \leqslant \mathrm{C}_G(N) = \mathrm{Z}(N)B$, was aber wegen K nichtauflösbar *nicht geht*; cf. Aufgabe 32.(2).

Also ist $\mathrm{Komp}(G) = \{\, Q_i \,:\, i \in [1,m]\,\}$ und somit

$$\mathrm{E}(G) \;=\; N.$$

Es ist $[\mathrm{Z}(N), B] = 1$ und $\mathrm{Z}(N) \cap B = 1$, also $\mathrm{Z}(N) \times B \xrightarrow{\sim} \mathrm{Z}(N)B$, $(z,b) \longmapsto zb$; cf. Aufgabe 2.(3). Es ist $\mathrm{F}(\mathrm{Z}(N) \times B) = \mathrm{F}(\mathrm{Z}(N)) \times \mathrm{F}(B) = \mathrm{Z}(N) \times \mathrm{F}(B)$; cf. Beispiel 132.(4), UeXXX. Also ist auch $\mathrm{F}(\mathrm{Z}(N)B) = \mathrm{Z}(N)\,\mathrm{F}(B)$.

Es ist $\mathrm{Z}(N) \trianglelefteqslant N \trianglelefteqslant G$, also $\mathrm{Z}(N) = \mathrm{F}(\mathrm{Z}(N)) \leqslant \mathrm{F}(G)$; cf. Bemerkung 76, Beispiel 132.(4), Bemerkung 141.

Es ist $B \trianglelefteqslant \mathrm{Z}(N)B = \mathrm{C}_G(N) \trianglelefteqslant G$; cf. Bemerkung 18. Also ist $\mathrm{F}(B) \leqslant \mathrm{F}(G)$; cf. Bemerkung 141.

Zusammen ist $\mathrm{Z}(N)\,\mathrm{F}(B) \leqslant \mathrm{F}(G)$.

Da $1 = [\mathrm{E}(G), \mathrm{F}(G)] = [N, \mathrm{F}(G)]$ nach Bemerkung 148.(3) und da $\mathrm{F}(G) \trianglelefteqslant G$ nach Bemerkung 131.(2), ist $\mathrm{F}(G) \trianglelefteqslant \mathrm{C}_G(N) = \mathrm{Z}(N)B$. Es folgt $\mathrm{F}(G) \leqslant \mathrm{F}(\mathrm{Z}(N)B) = \mathrm{Z}(N)\,\mathrm{F}(B)$; cf. Bemerkung 141.

Insgesamt ist also

$$\mathrm{F}(G) \;=\; \mathrm{Z}(N)\,\mathrm{F}(B)\,.$$

Also wird

$$\mathrm{FE}(G) \;=\; \mathrm{F}(G) \cdot \mathrm{E}(G) \;=\; \mathrm{Z}(N)\,\mathrm{F}(B) \cdot N \;=\; N\,\mathrm{F}(B)\,.$$

Anhang A

Aufgaben und Lösungen

A.1 Aufgaben

Aufgabe 1 (Definition) Sei G eine Menge. Sei $(\cdot) : G \times G \longrightarrow G$ eine assoziative Multiplikation auf G.

Gebe es $n \in G$ mit $gn = g$ für $g \in G$. Gebe es für alle $g \in G$ ein $h \in G$ mit $gh = n$.

Zeige, daß $G = (G, \cdot)$ eine Gruppe ist.

Aufgabe 2 (direkte Produkte) Zeige.

(1) Sei I eine Menge. Sei G_i eine Gruppe für $i \in I$. Zeige, daß das cartesische Produkt $G := \prod_{i \in I} G_i$ mit der Multiplikation $(g_i)_i \cdot (g'_i)_i := (g_i \cdot g'_i)_i$ für $(g_i)_i$, $(g'_i)_i \in G$ eine Gruppe wird, genannt das *(äußere) direkte Produkt* der Gruppen G_i für $i \in I$.

(2) Für $n \geqslant 0$ und eine Gruppe G schreiben wir $G^{\times n} := \prod_{i \in [1,n]} G$, mit $G^{\times 0} = 1$. Betrachte den Gruppenmorphismus $\delta : G \longrightarrow G \times G$, $g \longmapsto (g, g)$. Unter welcher Bedingung an G ist $\delta(G) \trianglelefteq G \times G$?

(3) Sei G eine Gruppe. Sei $n \geqslant 0$. Seien $U_i \leqslant G$ für $i \in [1, n]$. Sei $[u_i, u_j] = 1$ für $i, j \in [1, n]$ mit $i \neq j$ und $u_i \in U_i$, $u_j \in U_j$. Zeige, daß dann der Gruppenmorphismus $\prod_{i \in [1,n]} U_i \longrightarrow G$, $(u_i)_i \longmapsto u_1 \cdot \ldots \cdot u_n$ existiert. Wann ist dieser injektiv?

(4) Sei G eine Gruppe. Seien $N \trianglelefteq G$ und $M \trianglelefteq G$. Sei $N \cap M = 1$ und $NM = G$. Zeige die Existenz des Gruppenisomorphismus $N \times M \xrightarrow{\sim} G$, $(n, m) \longmapsto nm$. Ist die Aussage noch richtig, wenn die Normalität der Untergruppe M nicht verlangt wird?

Aufgabe 3 (abelsche Gruppen)

(1) Sei $n \geqslant 1$. Sei $x = (x_i)_i \in \mathbf{Z}^{n \times 1}$. Sei $g := \mathrm{ggT}(x_1, \ldots, x_n)$.

Zeige, daß es ein $S \in \mathrm{SL}_n(\mathbf{Z})$ gibt mit $Sx = \begin{pmatrix} g \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.

(2) Seien $m, n \geqslant 1$. Sei $A \in \mathbf{Z}^{m\times n}$. Zeige, daß es $S \in \mathrm{SL}_m(\mathbf{Z})$ und $T \in \mathrm{SL}_n(\mathbf{Z})$ derart gibt, daß $SAT =: D = (d_{i,j})_{i,j}$ eine Diagonalmatrix ist, i.e. $d_{i,j} = 0$ für $i \in [1, m]$ und $j \in [1, n]$, bei der ferner die Diagonaleinträge sich konsekutiv teilen, i.e. $d_{i+1,i+1} \in d_{i,i}\mathbf{Z}$ für $i \in [1, \min\{m, n\} - 1]$.

(3) Sei $n \geqslant 0$. Sei $B \leqslant \mathbf{Z}^n$. Zeige, daß B endlich erzeugt ist.

(4) Sei C eine additiv geschriebene abelsche Gruppe. Sei C endlich erzeugt.

Zeige, daß $C \simeq \prod_{i\in[1,k]} \mathbf{Z}/c_j\mathbf{Z}$ ist als abelsche Gruppen für geeignete $k \in \mathbf{Z}_{\geqslant 0}$ und $c_j \in \mathbf{Z}$ für $j \in [1, k]$ mit $c_{j+1} \in c_j\mathbf{Z}$ für $j \in [1, k-1]$.

(5) Sei folgender Morphismus kurz exakter Sequenzen abelscher Gruppen und Gruppenmorphismen gegeben.

$$\begin{array}{ccccc} A' & \xrightarrow{a'} & A & \xrightarrow{a''} & A'' \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\ B' & \xrightarrow{b'} & B & \xrightarrow{b''} & B'' \end{array}$$

Zeige, daß es eine abelsche Gruppe P, eine linksexakte Sequenz $P \longrightarrow A \times B' \longrightarrow B$ und kurz exakte Sequenzen $P \longrightarrow A \longrightarrow \mathrm{Im}(f'')$ und $A' \longrightarrow P \longrightarrow \mathrm{Kern}(f'')$ gibt.

(6) Berechne im Sinne von (4) unter Verwendung von (5) Kern und Bild des Gruppenmorphismus

$$\begin{array}{ccccccccccc} \mathbf{Z}/4\mathbf{Z} & \times & \mathbf{Z}/8\mathbf{Z} & \times & \mathbf{Z}/8\mathbf{Z} & \longrightarrow & \mathbf{Z}/2\mathbf{Z} & \times & \mathbf{Z}/2\mathbf{Z} & \times & \mathbf{Z}/16\mathbf{Z} \\ (x + 4\mathbf{Z} & , & y + 8\mathbf{Z} & , & z + 8\mathbf{Z}) & \longmapsto & (0 & , & z + 2\mathbf{Z} & , & 4x + 4y + 8z + 16\mathbf{Z}) \,. \end{array}$$

Aufgabe 4 (§1.1, §1.2) Seien G und H Gruppen.

Sei $M = (M, \alpha)$ eine G-Menge. Sei $N = (N, \beta)$ eine H-Menge. Als G-Menge sei G mit der Konjugation ausgestattet; cf. Beispiel 2.(5).

Zeige.

(1) Es ist $M \times N$ eine $(G \times H)$-Menge via $(g, h) \cdot (m, n) := (gm, hn)$ für $g \in G$, $h \in H$, $m \in M$, $n \in N$.

(2) Es ist $M \times M$ auf wenigstens drei verschiedene Weisen eine G-Menge, unter Verwendung von (1), vorausgesetzt, es ist $\alpha \neq !$.

(3) Es ist ${}_{\mathrm{Abb}}(M, N)$ eine $(G \times H)$-Menge via $((g, h)f)(m) := h\, f(g^- m)$ für $g \in G$, $h \in H$, $f \in {}_{\mathrm{Abb}}(M, N)$.

(4) Es ist $\mathrm{Pot}(M)$ eine G-Menge, unter Verwendung von (3).

(5) Die Menge der Untergruppen von G ist eine G-Menge, unter Verwendung von (4).

(6) Sei $U \leqslant G$. Sei $\mathrm{N}_G(U) := \mathrm{C}_G(\{U\})$ der *Normalisator* von U in G; cf. (5).
Dann ist $\mathrm{C}_G(U) \trianglelefteqslant \mathrm{N}_G(U)$ und $U \trianglelefteqslant \mathrm{N}_G(U)$. Ist stets $U\mathrm{C}_G(U) = \mathrm{N}_G(U)$?

(7) Sei $k \geqslant 1$. Die Menge der Untergruppen von Ordnung k von G bildet eine G-Menge, unter Verwendung von (4).

(8) Ist Ω eine G-Teilmenge von $\mathrm{Pot}(M)$, dann auch die Menge $\Omega_{\max}$ der maximalen Elemente von Ω.

Aufgabe 5 (§1.1) Sei $n \geqslant 3$. Betrachte die A_n-Menge $[1, n]$; cf. Beispiel 2.(1).

Weise $[1, n]$ als $(n-2)$-fach transitive, aber nicht $(n-1)$-fach transitive A_n-Menge nach.

Aufgabe 6 (§1.2, §1.3) Sei G eine Gruppe. Zeige.

(1) Sei M eine transitive G-Menge. Sei $m \in M$. Sei $H \leqslant G$.
Genau dann ist $H\mathrm{C}_G(m) = G$, wenn $M\downarrow_H^G$ eine transitive H-Menge ist.

(2) Sei G endlich. Sei $U \leqslant G$. Sei p der kleinste Primteiler von $|U|$. Sei $p \geqslant [G : U]$.
Es ist $U \trianglelefteqslant G$. (Hinweis: $\mathrm{Fix}_U(G/U)$.)

Aufgabe 7 (§1.1, §1.3) Zeige.

(1) Sei p prim. Sei P eine *p-Gruppe,* i.e. sei P eine endliche Gruppe und p der einzige Primteiler von $|P|$.
Sei M eine endliche P-Menge. Es ist $|\mathrm{Fix}_P(M)| \equiv_p |M|$.

(2) Sei G eine endliche Gruppe. Sei p ein Primteiler von $|G|$.
Es gibt in G ein Element von Ordnung p.
(Hinweis: Es ist $M := \{\, (g_i)_i \in G^{\times p} \,:\, g_1 g_2 \cdot \ldots \cdot g_p = 1 \,\}$ eine C_p-Menge. Wieso ist $|\mathrm{Fix}_{\mathrm{C}_p}(M)| \geqslant p$?)

Aufgabe 8 (§1.1) Zeige.

(1) Sei $n \geqslant 1$ ungerade. Sei G eine endliche Gruppe von Ordnung $2n$. Es gibt in G einen Normalteiler von Index 2.
(Hinweis: G als G-Menge via Multiplikation gibt injektive Operation $G \longrightarrow \mathrm{S}_G$. Zykeltyp von Element von Ordnung 2 ? Ist das Kompositum $G \longrightarrow \mathrm{S}_G \longrightarrow \{\pm 1\}$ surjektiv? Kern?)

(2) Sei G eine endliche Gruppe. Sei $U \leqslant G$. Es gibt $N \trianglelefteqslant G$ so, daß $[G : U]$ ein Teiler von $[G : N]$ und dies ein Teiler von $[G : U]!$ ist.
(Hinweis: Kern von Operation auf G/U.)

(3) Wenn x und y Elemente einer einfachen Gruppe von Ordnung 60 sind mit $|\langle x \rangle| = 3$ und $|\langle y \rangle| = 5$, dann ist $[x, y] \neq 1$.

Aufgabe 9 (§1.4) Sei $G := \langle\, (1,2,3,4,5,6,7,8,9),\ (1,9)(2,8)(3,7)(4,6) \,\rangle \leqslant \mathrm{S}_9$.

Enthält die G-Menge $[1, 9]$ einen Block B mit $|B| \in [2, 8]$? Ist $[1, 9]$ primitiv?

Aufgabe 10 (§1.1, §1.4) Zeige oder widerlege.

Sei G eine endliche Gruppe. Sei M eine G-Menge.

(1) Sei $k \geqslant 1$. Sei M eine k-fach transitive G-Menge. Dann ist $k!$ ein Teiler von $|G|$. (Hinweis: S_k operiert auf $M^{\times k, \neq}$.)

(2) Sei M primitiv. Dann ist M zweifach transitiv.

(3) Ist M regulär, dann ist M treu.

(4) Ist M transitiv und treu, dann ist M regulär.

(5) Ist G abelsch und ist M transitiv und treu, dann ist M regulär.

Aufgabe 11 (§1.4) Sei K ein Körper. Zeige.

(1) Die $\mathrm{GL}_2(K)$-Menge $\mathrm{P}^1(K)$ ist dreifach transitiv.

(2) Genau dann ist die $\mathrm{GL}_2(K)$-Menge $\mathrm{P}^1(K)$ vierfach transitiv, wenn $|K| = 3$ ist.

(3) Sei K endlich. Genau dann ist die $\mathrm{SL}_2(K)$-Menge $\mathrm{P}^1(K)$ dreifach transitiv, wenn $\operatorname{char} K = 2$ ist.

(4) Sei $n \geqslant 3$. Die $\mathrm{GL}_n(K)$-Menge $\mathrm{P}^{n-1}(K)$ ist nicht dreifach transitiv.

(5) Sei $n \geqslant 2$. Der Kern der Operation von $\mathrm{GL}_n(K)$ auf $\mathrm{P}^{n-1}(K)$ ist $\mathrm{Z}(\mathrm{GL}_n(K)) = K^{\times}\mathrm{E}_n$.

Aufgabe 12 (Aufgabe 4.(6)) Sei G eine Gruppe. Seien $U, V \leqslant G$. Zeige.

(1) Seien U und V endlich. Es ist $|UV| = |U| \cdot |V|/|U \cap V|$.

(2) Ist $U \leqslant \mathrm{N}_G(V)$, dann ist $V \trianglelefteq UV = VU \leqslant G$ und $U \cap V \trianglelefteq U$ und $U/(U \cap V) \xrightarrow{\sim} (UV)/V$, $u(U \cap V) \longmapsto uV$ ein Gruppenisomorphismus.

(3) Sind $U, V \trianglelefteq G$, dann ist $UV \trianglelefteq G$.

(4) Sei $N \trianglelefteq G$. Sei $N \trianglelefteq H \trianglelefteq G$. Dann haben wir den Isomorphismus $G/H \xrightarrow{\sim} (G/N)/(H/N)$, $gH \longmapsto (gN)(H/N)$.

Aufgabe 13 (§2.3.1) Seien G und H Gruppen. Sei $G \xrightarrow{f} H$ ein Gruppenmorphismus.

Sei $G^{(1)} := \langle\, [g, \tilde{g}] \,:\, g, \tilde{g} \in G \,\rangle$ die Kommutatoruntergruppe von G.

Zeige.

(1) Sei f surjektiv. Es ist $f(G^{(1)}) = H^{(1)}$.

(2) Es ist $G^{(1)} \trianglelefteq G$ und $G/G^{(1)}$ abelsch.

(3) Schreibe $G \xrightarrow{r} G/G^{(1)}$, $g \longmapsto gG^{(1)}$. Sei H abelsch.
Es gibt genau einen Gruppenmorphismus $\bar{f} : G/G^{(1)} \longrightarrow H$ mit $\bar{f} \circ r = f$.

(4) Sei $N \trianglelefteq G$. Genau dann ist G/N abelsch, wenn $G^{(1)} \leqslant N$ liegt.

(5) Es ist $\mathrm{A}_4/\mathrm{A}_4^{(1)} \simeq \mathrm{C}_3$.

Aufgabe 14 (§1.5, §2.3.2) Sei $G_0 := \langle\, (1,2)(3,4)\,,\ (1,2)(3,5)\,,\ (1,3)(4,5)\,\rangle \leqslant \mathrm{A}_5$.

Betrachte die G_0-Menge $M = [1,5]$; cf. Beispiel 2.(1).

(1) Bestimme Erzeuger für $G_1 := \mathrm{C}_{G_0}(1)$.

(2) Bestimme Erzeuger für $G_2 := \mathrm{C}_{G_1}(2)$.

(3) Zeige $G_0 = \mathrm{A}_5$ unter Verwendung von (1) und (2).

Aufgabe 15 (§1.5) Zeige.

(1) Sei G endlich erzeugt. Sei $H \leqslant G$ mit $[G : H]$ endlich.
Dann ist auch H endlich erzeugt.

(2) Sei $n \geqslant 1$. Sei $k \geqslant 1$. Sei p prim. Sei $U \leqslant \mathrm{S}_n$ mit $U \simeq \mathrm{C}_p^{\times k}$. Dann ist $[\mathrm{S}_n : U] \geqslant k/2$.

Aufgabe 16 (§2.3.1) Sei G eine Gruppe. Sei M eine endliche transitive G-Menge mit $|M| > 1$. Betrachte die G-Menge $M^{\times 2, \neq}$; cf. Beispiel 8.(2).

(1) Sei X eine Bahn von $M^{\times 2, \neq}$. Sei Γ_X der gerichtete Graph mit Eckenmenge M und Kantenmenge X. Definiere den Begriff eines Morphismus von gerichteten Graphen (ohne Kantenmultiplizitäten). Konstruiere einen Gruppenmorphismus $G \longrightarrow \mathrm{Aut}_{\mathrm{Graph}}(\Gamma_X)$.

(2) Zeige, daß der Graph Γ_X genau dann zusammenhängend ist für alle Bahnen X von $M^{\times 2, \neq}$, wenn M primitiv ist.

(3) Erstelle einen Graphen Γ_X im Sinne von (1) für die Situation aus Aufgabe 9, welcher nicht zusammenhängend ist.

Aufgabe 17 (§2.3.1) Sei G eine Gruppe. Sei $K \trianglelefteq G$.

Schreibe den Restklassenmorphismus $r : G \longrightarrow G/K$, $g \longmapsto gK$. Zeige.

(1) Wir haben die inklusionserhaltende Bijektion

$$\begin{array}{rcl} \{\, U \subseteq G \,:\, K \leqslant U \leqslant G \,\} & \longrightarrow & \{\, V \subseteq G/K \,:\, V \leqslant G/K \,\} \\ U & \longmapsto & r(U) \\ r^{-1}(V) & \longmapsfrom & V \,. \end{array}$$

(2) Seien U und U' aus der linken Seite von (1) mit $U \trianglelefteq U'$ gegeben.
Dann ist auch $r(U) \trianglelefteq r(U')$ und $U'/U \xrightarrow{\sim} r(U')/r(U)$, $u'U \longmapsto r(u')\,r(U)$.

(3) Die Bijektion aus (1) schränkt ein zu einer Bijektion von $\{\, U \subseteq G \,:\, K \leqslant U \trianglelefteq G \,\}$ nach $\{\, V \subseteq G/K \,:\, V \trianglelefteq G/K \,\}$.

Aufgabe 18 (§2.3.3) Sei F ein Körper. Zeige.

(1) Sei $n \geqslant 3$. Es ist $\mathrm{SL}_n(F)^{(1)} = \mathrm{SL}_n(F)$.

(2) Sei $|F| \geqslant 4$. Es ist $\mathrm{SL}_2(F)^{(1)} = \mathrm{SL}_2(F)$.

(3) Sei $n \geqslant 2$. Sei

$$A \;:=\; \left(\begin{smallmatrix} 1 & * \\ 0 & \mathrm{E}_{n-1} \end{smallmatrix}\right) \;:=\; \left\{ \left(\begin{smallmatrix} 1 & y \\ 0 & \mathrm{E}_{n-1} \end{smallmatrix}\right) \,:\, y \in F^{1\times n} \right\} \;\trianglelefteq\; \mathrm{C}_{\mathrm{SL}_n(F)}(\overline{\mathrm{e}_1})\;.$$

Es ist $\left\langle \bigcup_{g\in \mathrm{SL}_n(F)} {}^gA \right\rangle = \mathrm{SL}_n(F)$.

(4) Sei $n \geqslant 2$. Es ist $\mathrm{Z}(\mathrm{SL}_n(F)) = F^\times \mathrm{E}_n \cap \mathrm{SL}_n(F)$. Cf. Aufgabe 11.(5).

Aufgabe 19 (§2.3.3)

(1) Bestimme den Kern der Operation $\mathrm{GL}_2(\mathbf{F}_3) \longrightarrow \mathrm{S}_{\mathrm{P}^1(\mathbf{F}_3)}$; cf. Beispiel 31.
Ist sie surjektiv?

(2) Zeige, daß $\mathrm{PSL}_2(\mathbf{F}_3)$ isomorph zu A_4 ist. Ist $\mathrm{PSL}_2(\mathbf{F}_3)$ einfach?

(3) Zeige, daß $\mathrm{PSL}_2(\mathbf{F}_2) = \mathrm{SL}_2(\mathbf{F}_2) = \mathrm{GL}_2(\mathbf{F}_2)$ isomorph zu S_3 ist. Ist $\mathrm{PSL}_2(\mathbf{F}_2)$ einfach?

Aufgabe 20 (§2.3.2, §2.1) Zeige.

(1) Sei $n \geqslant 5$. Es hat A_n keine echte Untergruppe von Index $< n$.

(2) Sei $n \geqslant 3$. Es ist $\mathrm{Z}(\mathrm{S}_n) = 1$.

(3) Sei $n \geqslant 5$. Es hat S_n nur die Normalteiler 1, A_n und S_n.

(4) Sei G eine einfache Gruppe von Ordnung 60. Es ist G isomorph zu A_5.
(Hinweis: $\mathrm{Syl}_p(G)$ als G-Menge. Fall, $|\mathrm{Syl}_2(G)| = 15$. Wieso gibt es dann ein Element $x \in G \smallsetminus \{1\}$, das im Schnitt zweier 2-Sylowgruppen liegt? Warum ist dann 4 ein echter Teiler von $|\mathrm{C}_G(x)|$? Betrachte dann $G \longrightarrow \mathrm{S}_{(G:\langle x\rangle)}$.)

Aufgabe 21 (§1.4) Sei G eine endliche Gruppe.
Sei M eine primitive G-Menge mit $|M| \equiv_2 0$ und $|M| \geqslant 3$. Zeige $|G| \equiv_4 0$.
(Hinweis: Annahme, nicht. Wende Aufgabe 8.(1) an, dann Block als Bahn unter Normalteiler.)

Aufgabe 22 (§2.4.2) 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 58.

Zeige die Existenz des Gruppenisomorphismus

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

Aufgabe 23 (§2.4.2) Sei G eine Gruppe.

Ein Automorphismus α von G heißt *inner,* falls es ein $g \in G$ gibt mit $\alpha(x) = {}^g x$ für $x \in G$.

Die Menge der inneren Automorphismen wird mit $\mathrm{Inn}(G)$ bezeichnet.

Die Menge der Automorphismen von G wird mit $\mathrm{Aut}(G)$ bezeichnet.

(1) Zeige $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G) \leqslant \mathrm{S}_G$.

(2) Ist $\mathrm{Inn}(\mathrm{S}_4) = \mathrm{Aut}(\mathrm{S}_4)$?

(3) Konstruiere einen Gruppenendomorphismus von S_4 mit Bild von Ordnung 6.

(4) Ist $\mathrm{Inn}(\mathrm{S}_6) = \mathrm{Aut}(\mathrm{S}_6)$?
(Hinweis: $(1,2) \mapsto (1,2)(3,4)(5,6)$, $(1,2,3,4,5,6) \mapsto (1,2,3)(4,5)$.)

Aufgabe 24 (§2.3.3, §2.1)

(1) Konstruiere einen Isomorphismus $\mathrm{PSL}_2(\mathbf{F}_4) \xrightarrow{\sim} \mathrm{A}_5$.

(2) Konstruiere einen Isomorphismus $\mathrm{PSL}_2(\mathbf{F}_5) \xrightarrow{\sim} \mathrm{A}_5$. (Hinweis: $\mathrm{Syl}_2(\mathrm{PSL}_2(\mathbf{F}_5))$.)

Aufgabe 25 (§2.1)

(1) Sei G eine Gruppe von Ordnung 77. Zeige $G \simeq \mathrm{C}_{77}$.

(2) Sei G eine Gruppe von Ordnung 105. Zeige, daß G einen Normalteiler von Index 3 enthält.

(3) Finde eine 2-Sylowgruppe von S_6.

(4) Finde zu jedem Primteiler der Gruppenordnung eine Sylowgruppe von $\mathrm{GL}_2(\mathbf{F}_{11})$.

(5) Finde zu jedem Primteiler der Gruppenordnung eine Sylowgruppe von $\mathrm{GL}_3(\mathbf{F}_5)$.

Aufgabe 26 (§2.4.3)

(1) Finde eine endlich präsentierte Gruppe mit 2 Erzeugern isomorph zu A_4.

(2) Finde eine endlich präsentierte Gruppe isomorph zu
$\mathrm{Q}_8 := \langle \left(\begin{smallmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \rangle \leqslant \mathrm{GL}_2(\mathbf{C})$. Welche Ordnung hat Q_8?

Aufgabe 27 (§3.2) Sei G eine Gruppe. Sei $(U_i)_{i\in[0,s]}$ eine Subnormalreihe von G.

(1) Sei $H \leqslant G$. Zeige, daß $(H \cap U_i)_{i\in[0,s]}$ eine Subnormalreihe von H ist. Gib einen injektiven Gruppenmorphismus $(H\cap U_i)/(H\cap U_{i+1}) \longrightarrow U_i/U_{i+1}$ an für $i \in [0, s-1]$.

(2) Sei $N \trianglelefteq G$. Schreibe $\bar{U}_i := (U_iN)/N$ für $i \in [0, s]$. Zeige, daß $(\bar{U}_i)_{i\in[0,s]}$ eine Subnormalreihe von G/N ist. Gib einen surjektiven Gruppenmorphismus $U_i/U_{i+1} \longrightarrow \bar{U}_i/\bar{U}_{i+1}$ an für $i \in [0, s-1]$.

Aufgabe 28 (§2.4.2)

(1) Zeige, daß es genau einen Gruppenmorphismus $f : \mathrm{S}_4 \longrightarrow \mathrm{GL}_3(\mathbf{Z})$ mit $(1,2) \longmapsto \left(\begin{smallmatrix} 1 & 0 & 0 \\ 1 & -1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ und $(1,2,3,4) \longmapsto \left(\begin{smallmatrix} -2 & 1 & 0 \\ -3 & 0 & 1 \\ -4 & 0 & 1 \end{smallmatrix}\right)$ gibt.

(2) Bestimme $|\mathrm{GL}_2(\mathbf{Z}/4\mathbf{Z})|$ und $|\mathrm{GL}_3(\mathbf{Z}/4\mathbf{Z})|$. (Hinweis: Reduktion modulo 2.).

(3) Finde eine Untergruppe von Index 28 in $\mathrm{GL}_3(\mathbf{Z})$, die das Bild von f enthält. (Hinweis: Kongruenzen modulo 4 in dritter Zeile. Verwende (2).)

Aufgabe 29 (§2.4.2)

(1) Sei G eine endliche Gruppe. Zeige, daß G isomorph zu einer endlich präsentierten Gruppe ist. (Hinweis: Multiplikationstafel für Relationen verwenden.)

(2) Sei G eine endlich präsentierte Gruppe, $G = \langle\, x_1\,, \ldots\,, x_n \,:\, r_1\,, \ldots\,, r_m \,\rangle$.

Schreibe $X := \{\, x_1\,, \ldots\,, x_n \,\}$. Sei $A := \prod_{x\in X} \mathbf{Z}$ die additiv geschriebene freie abelsche Gruppe auf der Menge X. Für $y \in X$ schreiben wir auch $y := (\partial_{x,y})_{x\in X}$. Wir haben einen surjektiven Gruppenmorphismus $\varphi : \mathrm{F}(X) \longrightarrow A$, welcher jedes $x \in X$ nach x abbildet. Sei $U := \langle\, \varphi(r_j) \,:\, j \in [1,m] \,\rangle \leqslant A$. Zeige die Existenz des Gruppenisomorphismus

$$\begin{array}{rcll} G/G^{(1)} & \xrightarrow{\bar{\varphi}} & A/U & \\ xG^{(1)} & \longmapsto & x+U & \text{für } x \in X\,. \end{array}$$

(3) Berechne $\mathrm{S}_5/\mathrm{S}_5^{(1)}$ einmal direkt und einmal mittels (2).

Aufgabe 30 (§3.1) Bestimme alle Kompositionsreihen der Gruppe G.

(1) $G = \mathrm{C}_{20}$

(2) $G = \mathrm{S}_4$

Aufgabe 31 (§3.2) Sei p eine Primzahl. Sei P eine p-Gruppe. Zeige.

(1) Ist $P > 1$, dann ist $\mathrm{Z}(P) > 1$. (Hinweis: Aufgabe 7.(1).)

(2) Ist P einfach, dann ist $P \simeq \mathrm{C}_p$.

Aufgabe 32 (§3.2)

Sei G eine endliche Gruppe. Sei $H \leqslant G$. Sei $N \trianglelefteq G$. Zeige.

(1) Sind N und G/N auflösbar, dann auch G.

(2) Ist G auflösbar, dann auch H und G/N.

(3) Sind H und N auflösbar, dann auch HN.

(4) Ist $N \leqslant \mathrm{Z}(G)$ und ist G/N überauflösbar, dann auch G.

(5) Ist G überauflösbar, dann auch H und G/N.

(6) Ist $N \leqslant \mathrm{Z}(G)$ und ist G/N nilpotent, dann auch G.

(7) Ist G nilpotent, dann auch H und G/N.

Aufgabe 33 (§3.2)

Sei G eine Gruppe. Seien p, q und r drei verschiedene Primzahlen. Zeige.

(1) Ist $|G| = pq$, dann ist G überauflösbar.

(2) Ist $|G| = p^2q$, dann ist G auflösbar.

(3) Ist $|G| = p^2q^2$, dann ist G auflösbar.

(4) Ist $|G| = pqr$, dann ist G auflösbar.

(5) Ist $|G| = pq^k$, wobei $p < q$ und $k \geqslant 0$, dann ist G auflösbar.

(6) Ist $|G| < 60$, dann ist G auflösbar.

Aufgabe 34 (§3.2) Seien G und H Gruppen. Sei $f : G \longrightarrow H$ ein Gruppenmorphismus. Zeige oder widerlege.

(1) Seien U, $V \leqslant G$. Es ist $[f(U), f(V)] = f([U, V])$.

(2) Es ist $f(\mathrm{Z}(G)) \leqslant \mathrm{Z}(H)$.

(3) Es ist $f(\mathrm{Z}(G)) \leqslant \mathrm{Z}(f(G))$.

(4) Es ist $f(\mathrm{Z}(G)) = \mathrm{Z}(f(G))$.

Aufgabe 35 (§3.2) Seien G und H Gruppen.

Sei $(U_i)_{i\in[0,s]}$ eine Subnormalreihe von G. Sei $(V_i)_{i\in[0,t]}$ eine Subnormalreihe von H.

Sei o.E. $s \leqslant t$. Setze noch $U_i := 1$ für $i \in [s+1, t]$. Zeige.

(1) Sind $(U_i)_{i\in[0,s]}$ und $(V_i)_{i\in[0,t]}$ auflösend, dann auch $(U_i \times V_i)_{i\in[0,t]}$.

(2) Sind $(U_i)_{i\in[0,s]}$ und $(V_i)_{i\in[0,t]}$ nilpotent auflösend, dann auch $(U_i \times V_i)_{i\in[0,t]}$.

(3) Es ist $(G \times H)^{[i]} = G^{[i]} \times H^{[i]}$ für $i \geqslant 0$.

(4) Es ist $(G \times H)^{]i[} = G^{]i[} \times H^{]i[}$ für $i \geqslant 0$.

(5) Sind G und H nilpotent, so auch $G \times H$.
Folgere dies separat aus (2), aus (3) resp. aus (4).

Aufgabe 36 (§2.4.2, §3.2) Sei $\mathrm{D}_{16} := \langle\, a, b \,:\, a^8,\, b^2,\, (ab)^2 \,\rangle$. Sei $G := \mathrm{D}_{16} \times \mathrm{C}_2$.

(1) Zeige $|\mathrm{D}_{16}| = 16$.

(2) Zeige, daß die Kommutatorreihe, die absteigende Zentralreihe und die aufsteigende Zentralreihe von G paarweise verschieden sind.

Aufgabe 37 (§3.2) Eine Gruppe H heiße *charakteristisch-einfach*, wenn $H > 1$ ist und wenn H außer 1 und H keine weiteren charakteristischen Untergruppen hat.

In einer Gruppe H heißt ein Normalteiler $K \trianglelefteq H$ *minimal*, wenn er ein minimales Element von $\{\, L \trianglelefteq H \,:\, L > 1 \,\}$ ist.

(1) Sei G eine Gruppe. Sei $N \trianglelefteq G$ minimal.
Zeige, daß N charakteristisch-einfach ist.

(2) Sei N eine charakteristisch einfache endliche Gruppe. Sei S ein minimaler Normalteiler von N. Zeige, daß S einfach ist und es ein $k \geqslant 1$ mit $N \simeq S^{\times k}$ gibt.
(Hinweis: $S \trianglelefteq N$ minimal; $k \geqslant 1$ maximal mit Automorphismen $(\alpha_i)_{i\in[1,k]}$ so, daß $S^{\times k} \longrightarrow N$, $(s_i)_i \longmapsto \alpha_1(s_1)\cdot\ldots\cdot\alpha_k(s_k)$ injektiver Gruppenmorphismus; Bild charakteristisch in N, also Isomorphismus; S einfach, da aus normal in S auch normal in $S^{\times k}$ und also normal in N folgt.)

(3) Sei S eine nichtabelsche einfache Gruppe. Sei $k \geqslant 1$. Sei $X \trianglelefteq S^{\times k}$. Zeige die Existenz einer Teilmenge $I \subseteq [1,k]$ mit $X = \{\, (s_i)_i \in S^{\times k} \,:\, s_i = 1 \text{ für } i \in [1,k] \smallsetminus I \,\}$. Wieviele Normalteiler enthält $S^{\times k}$ demnach?

(4) Sei G eine endliche Gruppe. Sei $N \trianglelefteq G$ minimal. Zeige, daß es $S \trianglelefteq N$ mit S einfach so gibt, daß ${}^G\langle\!\langle\, S \,\rangle\!\rangle = N$ ist. Ist für jedes solche S auch $|\{\, {}^gS \,:\, g \in G \,\}| = \log_{|S|} |N|$? Trifft dies zu, wenn S nichtabelsch ist?

Aufgabe 38 (§3.2) Sei $G := \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$, additiv geschrieben.

(1) Bestimme die Anzahl der Endomorphismen von G.

(2) Bestimme $|\operatorname{Aut}(G)|$.

(3) Bestimme die charakteristischen Untergruppen von G.

Aufgabe 39 (§3.2) Sei G eine endliche Gruppe. Zeige.

(1) Sei $N \trianglelefteq G$. Sei $\operatorname{Aut}(N)$ abelsch. Es ist $[G^{(1)}, N] = 1$.

(2) Ist G überauflösbar, dann ist $G^{(1)}$ nilpotent. Gilt auch die Umkehrung?

Aufgabe 40 (§3.2) Sei p prim. Sei P eine p-Gruppe. Zeige.

(1) Sei $U < P$. Es ist $U < \mathrm{N}_P(U)$. (Hinweis: aus $P^{]i[} \leqslant U$ folgt $P^{]i+1[} \leqslant \mathrm{N}_P(U)$.)

(2) Sei $U < P$ maximale echte Untergruppe. Es ist $U \trianglelefteq P$.

(3) Sei P nichtabelsch. Es ist $[P : \mathrm{Z}(P)] \equiv_{p^2} 0$.

Aufgabe 41 (§3.3) Zeige oder widerlege.

Sei G eine Gruppe. Sei $N \trianglelefteq G$. Seien K und L Komplemente zu N in G.

(1) Es ist $K \simeq L$.

(2) Es gibt ein $x \in G$ mit ${}^xK = L$.

Aufgabe 42 (§3.3) Betrachte die Gruppe Q_8 aus Aufgabe 26.(2).

(1) Bestimme alle Untergruppen und alle Normalteiler von Q_8 .

(2) Welche Normalteiler haben ein Komplement in Q_8 ?

Aufgabe 43 (§3.3)

(1) Bestimme die Isoklassen der nichtabelschen Gruppen der Ordnung 12.

(2) Bestimme die Isoklassen der Gruppen der Ordnung 52, die ein Element der Ordnung 4 enthalten.

Aufgabe 44 (§3.3) Sei $p \geqslant 3$ prim.

Sei G eine nichtabelsche Gruppe von Ordnung p^3.

(1) Zeige $\mathrm{Z}(G) \simeq \mathrm{C}_p$. Bestimme die Kommutatorreihe, die absteigende und die aufsteigende Zentralreihe von G.

(2) Betrachte den Fall, daß alle Elemente von $G \setminus \{1\}$ Ordnung p haben.
Zeige, daß G einen Normalteiler isomorph zu $\mathrm{C}_p \times \mathrm{C}_p$ hat. Zeige

$$G \;\simeq\; \langle\, x, y, z \,:\, z^p,\, x^p,\, y^p,\, [z,x],\, [z,y],\, [x,y]z \,\rangle\ .$$

(3) Betrachte den Fall, daß ein Element b von G von Ordnung p^2 existiert.
Zeige, daß $\langle b \rangle$ ein Komplement in C_p hat. Zeige

$$G \;\simeq\; \langle\, x, y \,:\, x^p,\, y^{p^2},\, [x,y]y^p \,\rangle\ .$$

(Hinweis: Annahme, es hat $\langle b \rangle$ kein Komplement. Sei $c \in G \setminus \langle b \rangle$. Es ist $|\langle c \rangle| = p^2$. O.E. $b^p = c^p$. Es ist $\mathrm{Z}(G)$ kein Komplement, also $\mathrm{Z}(G) = \langle b^p \rangle$ dank (1). Es ist ${}^c b = b^k$ für ein $k \in \mathbf{Z}$. Da $b^p = {}^c(b^p)$, folgt $k \equiv_p 1$. Zeige $|\langle b^- c \rangle| = p$. Das Komplement $\langle bc^- \rangle$ gibt den Widerspruch.)

Aufgabe 45 (§3.3) Sei H eine Gruppe.

(1) Sei M eine H-Menge, mit Operation $\beta : H \longrightarrow \mathrm{S}_M$. Sei K eine Gruppe, aufgefaßt als H-Menge via $! : H \longrightarrow \mathrm{S}_K$. Wir haben die H-Menge ${}_{\mathrm{Abb}}(M, K)$, mit der Operationsabbildung $\alpha_0 : H \longrightarrow \mathrm{S}_{\mathrm{Abb}(M,K)}$; cf. Aufgabe 4.(3). Zeige, daß der Gruppenmorphismus $\alpha := \alpha_0|^{\mathrm{Aut}({}_{\mathrm{Abb}}(M,K))}$ definiert ist. Inwiefern verallgemeinert dies Definition 97? Schreibe auch hier $H \wr K = K \wr_\beta H := {}_{\mathrm{Abb}}(M, K) \underset{\alpha}{\rtimes} H$.

(2) Sei $L \leqslant H$ eine Untergruppe von endlichem Index. Sei β die Operation von H auf H/L; cf. Beispiel 2.(3). Seien R, $N \trianglelefteqslant L$ mit $N \trianglelefteqslant H$.

Wähle $T \subseteq H$ mit $1 \in T$ und $H = \bigsqcup_{t \in T} tL$. Schreibe $h =: \tau(h) \cdot \lambda(h)$ mit $\tau(h) \in T$ und $\lambda(h) \in L$ für $h \in H$.

Für $h \in H$ sei $u_h : H/L \longrightarrow L/R$, $xL \longmapsto \lambda(x) \cdot \lambda(h^- x)^- R$. Zeige die Wohldefiniertheit dieses Elements der Gruppe ${}_{\mathrm{Abb}}(H/L, L/R)$. Zeige die Existenz des Gruppenmorphismus

$$\begin{array}{ccc} H & \xrightarrow{f} & (L/R) \wr_\beta (H/N) \\ h & \longmapsto & (\, u_h \,,\, hN \,) \end{array}$$

Wann ist f injektiv?

(3) Sei X eine endliche, transitive und treue H-Menge. Sei Y eine H-Menge. Sei $X \xrightarrow{u} Y$ eine surjektive H-Abbildung. Sei $x \in X$. Sei $L := \mathrm{C}_H(u(x))$. Weise $Z := u^{-1}(u(x))$ als transitive L-Teilmenge von X nach. Sei R der Kern der Operation von L auf Z. Sei N der Kern der Operation von H auf Y.

Ist in dieser Situation der Gruppenmorphismus f aus (2) injektiv?

Aufgabe 46 (§3.3) Sei K eine Gruppe. Sei X eine K-Menge. Sei H eine Gruppe. Sei $\beta : H \longrightarrow \mathrm{S}_m$ ein Gruppenmorphismus; schreibe $(\beta(h))(i) = hi$ für $h \in H$ und $i \in [1, m]$.

(1) Zeige, daß $X^{\times m}$ via $((k_i)_i\,,\, h) \cdot (x_i)_i := (k_i\, x_{h^{-}i})_i$ eine $K \wr_\beta H$-Menge ist.

(2) Sei X eine transitive K-Menge. Zeige, daß $X^{\times m}$ eine transitive $K \wr_\beta H$-Menge ist. Bestimme den Zentralisator eines Elements von $X^{\times m}$ unter Verwendung eines Zentralisators in K.

Aufgabe 47 (§3.4.1)

(1) Zeige Lemma 106.(3).

(2) Zeige Lemma 106.(4).

Aufgabe 48 (§3.4.1)

(1) Sei H eine endliche Gruppe. Sei A eine endliche abelsche Gruppe.

Sei $\alpha : H \longrightarrow \mathrm{Aut}(A)$ ein Gruppenmorphismus.

Sei $1 < K \trianglelefteqslant H$ ein abelscher Normalteiler mit $|K|$ teilerfremd zu $|A|$.

So wird $A \smallsetminus \{1\}$ zu einer K-Menge. Sei $\mathrm{C}_K(a) = 1$ für $a \in A \smallsetminus \{1\}$.

Zeige $\mathrm{H}^2(H, A) = 1$ und $\mathrm{H}^1(H, A) = 1$, genommen bezüglich α.

(Hinweis: Sei E eine Erweiterung von A mit H. Sei $F \leqslant E$ das Urbild von $K \leqslant H$. Es hat A in F ein Komplement. Sei Q eine Sylowgruppe von F, konstruiert als Bild einer Sylowgruppe von K. Verwende Frattini, um $A \cdot \mathrm{N}_E(Q) = E$ zu zeigen.)

(2) Sei $n \geqslant 1$. Sei $q \geqslant 3$ eine Primpotenz. Sei $H = \mathrm{GL}_n(\mathbf{F}_q)$. Sei $A := \mathbf{F}_q^{n\times 1}$, additiv geschrieben. Sei $\alpha : H \longrightarrow \mathrm{Aut}(A)$, $h \longmapsto (a \longmapsto ha)$ gegeben via Matrixmultiplikation von $h \in \mathrm{GL}_n(\mathbf{F}_q) \subseteq \mathbf{F}_q^{n\times n}$ mit $a \in \mathbf{F}_q^{n\times 1}$.

Zeige $\mathrm{H}^2(H, A) = 0$ und $\mathrm{H}^1(H, A) = 0$, genommen bezüglich α, ebenfalls additiv geschrieben.

Aufgabe 49 (Aufgabe ??) Sei A eine abelsche Gruppe. Sei $B \leqslant A$. Zeige.

(1) Sei Q eine abelsche Gruppe. Sei Q *divisibel*, i.e. sei für alle $q \in Q$ und alle $z \in \mathbf{Z}^\times$ ein $\tilde{q} \in Q$ mit $\tilde{q}^z = q$ existent. Für alle Gruppenmorphismen $B \xrightarrow{g} Q$ gibt es einen Gruppenmorphismus $A \xrightarrow{f} Q$ mit $f|_B = g$.
(Hinweis: Zorn über $\{\, (C,h) \,:\, B \leqslant C \leqslant A,\ h \text{ Gruppenmorphismus mit } h|_B = g \,\}$.)

(2) Ist B divisibel, so hat B ein Komplement in A.

(3) Es ist $(\mathbf{Q},+)$ divisibel. Es ist $(\mathbf{Q}/\mathbf{Z},+)$ divisibel. Es ist $\mathrm{U}(\mathbf{C})$ divisibel.
Es ist $\mathrm{U}_1(\mathbf{C}) := \{\, u \in \mathrm{U}(\mathbf{C}) \,:\, |u| = 1 \,\}$ eine divisible Untergruppe von $\mathrm{U}(\mathbf{C})$.

Literatur

[1] Aschbacher, M., *Finite Group Theory,* 2nd ed., Cambridge University Press, 2000.

[2] Hiss, G., *Group Theory,* Vorlesung in Aachen, 2008.

[3] Kimmerle, W., *Gruppen, Geometrie und Darstellungstheorie,* Stuttgart, 2008.

[4] Kurzweil, H.; Stellmacher, B., *Theorie der endlichen Gruppen,* Springer, 1998.

[5] Künzer, M., *Cohomologie von Gruppen,* Skript, Aachen, 2006.

[6] dito, *Galoistheorie,* Skript, Koblenz, 2009.

[7] dito, *Gewöhnliche Darstellung endlicher Gruppen,* Skript, Stuttgart, 2013.

[8] dito, *Computeralgebra,* Skript, Stuttgart, 2011.

[9] dito, *Lineare Algebra für Informatiker,* Skript, Ulm, 2004.