

# Gruppentheorie

Matthias Künzer

Universität Stuttgart

19. März 2025

## Inhalt

<b>1</b>	<b><i>G</i>-Mengentheorie</b>	<b>10</b>
1.1	Operationen von Gruppen . . . . .	10
1.2	Zentralisator . . . . .	15
1.3	Fixpunkte . . . . .	17
1.4	Primitivität . . . . .	18
1.5	Bahnenalgorithmus . . . . .	21
<b>2</b>	<b>Anwendungen der <i>G</i>-Mengentheorie</b>	<b>26</b>
2.1	Sylow . . . . .	26
2.2	Einfachheit . . . . .	28
2.2.1	Iwasawa . . . . .	28
2.2.2	Einfachheit von $A_n$ für $n \geq 5$ . . . . .	29
2.2.3	Einfachheit von $\text{PSL}_n(F)$ für $(n,  F ) \notin \{(2, 2), (2, 3)\}$ . . . . .	31
2.3	Präsentationen . . . . .	32
2.3.1	Freie Gruppen . . . . .	32
2.3.2	Endliche Präsentationen via Erzeuger und Relationen . . . . .	36
2.3.3	Bahnenalgorithmus für Relationen . . . . .	39
<b>3</b>	<b>Erweiterungen</b>	<b>43</b>
3.1	Jordan-Hölder . . . . .	43
3.2	Auflösbar, überauflösbar, nilpotent . . . . .	49
3.3	Semidirekte Produkte . . . . .	58
3.4	Schur-Zassenhaus . . . . .	64
3.4.1	Die ersten beiden Cohomologiegruppen . . . . .	64
3.4.2	Schur . . . . .	71
3.4.3	Zassenhaus . . . . .	78
<b>4</b>	<b>Kleine Untergruppen</b>	<b>82</b>
4.1	Die Frattiniuntergruppe . . . . .	82
4.2	Eine Bemerkung . . . . .	85
4.3	Die Fittinguntergruppe . . . . .	86
4.4	Die erweiterte Fittinguntergruppe . . . . .	89
<b>A</b>	<b>Aufgaben und Lösungen</b>	<b>97</b>
A.1	Aufgaben . . . . .	97

## Verzeichnis der Sätze und einiger sonstiger Aussagen

Lemma 19	§1.2	S. 16	Bahnenlemma
Lemma 31	§1.5	S. 21	Lemma von Schreier über Zentralisatorenerzeuger
Algorithmus 32	§1.5	S. 22	Bahnenalgorithmus
Satz 37	§2.1	S. 27	Satz von Sylow
Lemma 41	§2.2.1	S. 28	Iwasawa-Kriterium
Satz 46	§2.2.2	S. 30	Einfachheit der alternierenden Gruppe
Satz 47	§2.2.3	S. 31	Einfachheit der projektiven speziellen Gruppe
Satz 54	§2.3.2	S. 37	Universelle Eigenschaft einer endlich präsentierten Gruppe
Lemma 62	§3.1	S. 43	Schmetterlingslemma
Lemma 70	§3.1	S. 47	Lemma von Schreier über Subnormalreihen
Satz 71	§3.1	S. 49	Satz von Jordan und Hölder
Satz 83	§3.2	S. 54	Kommutatorreihe
Satz 85	§3.2	S. 55	Zentralreihen
Satz 88	§3.2	S. 57	Sylowzerlegung nilpotenter Gruppen
Lemma 115	§3.4.3	S. 78	Lemma von Frattini
Satz 119	§3.4.3	S. 79	Satz von Schur und Zassenhaus
Satz 132	§4.3	S. 88	Zentralisator der Fittinguntergruppe
Satz 148	§4.4	S. 94	Zentralisator der erweiterten Fittinguntergruppe

## Vorwort

### Automorphismengruppen

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

Es hat e.g. die Körpererweiterung  $\mathbf{C}|\mathbf{R}$  die Automorphismengruppe  $\{\text{id}_{\mathbf{C}}, \kappa\} \simeq \mathbf{C}_2$ , 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  $\mathbf{S}_5$ .

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

Es hat e.g. die Gruppe  $\mathbf{S}_5$  die Automorphismengruppe  $\text{Aut}(\mathbf{S}_5) \simeq \mathbf{S}_5$ .

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

$$\begin{array}{c} \mathbf{S}_5 \\ |_{\mathbf{C}_2} \\ \mathbf{A}_5 \\ |_{\mathbf{A}_5} \\ 1 \end{array}$$

Zwar ist  $S_5$  nicht als direktes Produkt  $A_5 \times C_2$  rekonstruierbar, wohl aber noch als semidirektes Produkt,

$$S_5 \simeq A_5 \rtimes C_2,$$

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

Betrachten wir ferner die Gruppe  $GL_n(K)$ . Sei hierbei  $K$  ein endlicher Körper und  $n \geq 2$ . Die Determinante gibt einen surjektiven Gruppenmorphisms von  $GL_n(K)$  nach  $K \setminus \{0\} = GL_1(K)$ . Der Kern der Determinante ist die Gruppe  $SL_n(K)$ . Die darin liegenden Diagonalmatrizen mit konstanter Diagonale bilden das Zentrum  $Z(SL_n(K))$  dieser Gruppe, was darin ein i.a. nichttrivialer Normalteiler ist. Die Gruppen  $GL_1(K)$  und  $Z(SL_n(K))$  sind abelsch, sogar zyklisch, ihre Kompositionsfaktoren mithin zyklisch von Primordnung. Schließlich ist die Faktorgruppe  $PSL_n(K) := SL_n(K)/Z(SL_n(K))$  eine einfache Gruppe, solange nur  $(K, n) \notin \{(\mathbf{F}_2, 2), (\mathbf{F}_3, 2)\}$  ist. Somit hat diesfalls die Gruppe  $GL_n(K)$  als Kompositionsfaktoren  $PSL_n(K)$  und weitere zyklische Gruppen von Primordnung.

$$\begin{array}{c} GL_n(K) \\ \quad \downarrow \text{abelsch} \\ SL_n(K) \\ \quad \downarrow PSL_n(K) \\ Z(SL_n(K)) \\ \quad \downarrow \text{abelsch} \\ 1 \end{array}$$

Es ist zwar

$$GL_n(K) \simeq SL_n(K) \rtimes GL_1(K),$$

jedoch ist i.a. dann

$$Z(SL_n(K)) \twoheadrightarrow SL_n(K) \twoheadrightarrow PSL_n(K)$$

eine nichtspaltende Erweiterung, i.e.  $SL_n(K)$  ist nicht als semidirektes Produkt seiner Untergruppe  $Z(SL_n(K))$  und seiner Faktorgruppe  $PSL_n(K)$  schreibbar. Die Tatsache, daß  $Z(SL_n(K))$  zentral in  $SL_n(K)$  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

$$S := \langle s_1, s_2, s_3, s_4 : s_1^2, s_2^2, s_3^2, s_4^2, (s_1 s_2)^3, (s_2 s_3)^3, (s_3 s_4)^3, (s_1 s_3)^2, (s_1 s_4)^2, (s_2 s_4)^2 \rangle$$

erzeugt von den Elementen  $s_1, s_2, s_3, s_4$ ; in ihr gelten die Gleichungen  $s_1^2 = 1, s_2^2 = 1, s_3^2 = 1, \dots, (s_2 s_4)^2 = 1$ ; 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  $s_i \mapsto \tilde{s}_i$  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  $s_1^2, s_2^2, s_3^2, \dots, (s_2s_4)^2$  erzeugten Normalteiler.

Insbesondere erhalten wir den Gruppenmorphismus  $S \rightarrow S_5$ , der  $s_i \mapsto (i, i+1)$  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 Bahnalgorithmus 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 NITSCHKE für Korrekturen und Hinweise. Für weitere Hinweise auf Fehler und Unklarheiten bin ich dankbar.

Stuttgart, im Wintersemester 2015/16

Matthias Künzer

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

- Sind  $a, b \in \mathbf{Z}$ , so schreiben wir  $[a, b] := \{z \in \mathbf{Z} : a \leq z \leq b\}$  für das ganzzahlige Intervall.
- Ist  $p > 0$  eine Primzahl und  $x \in \mathbf{Z} \setminus \{0\}$ , so schreiben wir  $v_p(x) := \max\{\alpha \in \mathbf{Z}_{\geq 0} : x \in p^\alpha \mathbf{Z}\}$  für die Bewertung (engl. valuation) von  $x$  bei  $p$ . Wir setzen noch  $v_p(0) = +\infty$ .
- Ist  $n \in \mathbf{Z}$  und  $p \in \mathbf{Z}_{>0}$  prim, so schreiben wir  $n[p] := p^{v_p(n)}$ .
- 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  $\text{Pot}(X)$  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  $k \geq 0$  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  $\text{id} = \text{id}_X$  die identische Abbildung von  $X$  nach  $X$ .
- Sei  $\text{Abb}(X, Y)$  die Menge der Abbildungen von  $X$  nach  $Y$ .
- Sei  $f : X \rightarrow Y$  eine Abbildung. Sei  $X' \subseteq X$ ,  $Y' \subseteq Y$  und  $f(X') \subseteq Y'$ . Wir schreiben  $f|_{X'}^{Y'} : X' \rightarrow Y'$ ,  $x' \mapsto f(x')$  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  $f : X \rightarrow Y$  bijektiv, so bezeichnet häufig  $f^- := f^{-1} : Y \rightarrow X$  ihre Umkehrabbildung, i.e.  $f^- \circ f = \text{id}_X$  und  $f \circ f^- = \text{id}_Y$ .
- Ist  $f : X \times Y \rightarrow Z$  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  $(X, \leq)$  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  $x \leq z$  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  $z \leq x$  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  $\exp(G) := \text{kgV}(|\langle g \rangle| : g \in G)$  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  $A^\times := A \setminus \{0\}$ .
- 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  $1_{S_n} = \text{id}_{[1, n]} = \text{id}$ . Für  $n \geq 0$  schreiben wir auch  $S_n := S_{[1, n]}$ . 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  $n \geq 1$ . Es bezeichnet  $C_n$  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  $U(A) := \{a \in A : \text{es gibt ein } b \in A \text{ mit } ab = 1 \text{ und } ba = 1\}$  die Einheitengruppe von  $A$ .
- Sei  $n \geq 2$ . Der Kern des Signummorphismus  $\text{sgn} : S_n \rightarrow U(\mathbf{Z}) = \{-1, +1\}$  ist die alternierende Gruppe  $A_n$ .
- Sei  $R$  ein kommutativer Ring. Seien  $n, m \geq 0$ . Sei  $R^{m \times n}$  die Menge der  $m \times n$ -Matrizen. Für  $i \in [1, m]$  und  $j \in [1, n]$  ist  $e_{i,j} \in R^{m \times n}$  das Element, das an Position  $(i, j)$  den Eintrag 1 hat, ansonsten überall den Eintrag 0.  
Sei  $E_n := \sum_{i \in [1, n]} e_{i,i} \in R^{n \times n}$  die Einheitsmatrix.  
Sei  $\text{diag}(\lambda_1, \dots, \lambda_n) = \sum_{i \in [1, n]} \lambda_i e_{i,i}$ , wobei  $\lambda_i \in R$  für  $i \in [1, n]$ .  
Sei  $R^m := R^{m \times 1}$ . Für  $i \in [1, m]$  ist  $e_i \in R^m$  das Element, das an Position  $i$  den Eintrag 1 hat, ansonsten überall den Eintrag 0, genannt der  $i$ -te Standardbasisvektor. I.e.  $e_i = e_{i,1}$ .

- Sei  $R$  ein kommutativer Ring. Es bezeichnet

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

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

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

den Kern des Gruppenmorphisms  $\det : \text{GL}_n(R) \rightarrow U(R)$ . Ferner bezeichnet

$$\text{PSL}_n(R) = \text{SL}_n(R)/\mathbf{Z}(\text{SL}_n(R)).$$

- Sei  $K$  ein Körper. Sei  $V$  ein  $K$ -Vektorraum. Es bezeichnet  $\text{GL}(V)$  die Gruppe der bijektiven  $K$ -linearen Abbildungen von  $V$  nach  $V$ , mit der Komposition als Multiplikation. Es ist also  $\text{GL}(K^n)$  isomorph zu  $\text{GL}_n(K)$  vermöge des Isomorphismus, der einem Element  $\varphi \in \text{GL}(K^n)$  die beschreibende Matrix bezüglich Standardbasis zuordnet.
- Es bezeichnet manchmal  $\rightarrow$  einen injektiven Gruppenmorphisms,  $\twoheadrightarrow$  einen surjektiven,  $\xrightarrow{\sim}$  einen bijektiven.
- Eine abelsche Gruppe  $A$  heißt endlich erzeugt, wenn es ein  $n \geq 0$  und einen surjektiven Gruppenmorphisms  $f : \mathbf{Z}^n \twoheadrightarrow A$  gibt.  
Man sagt diesenfalls auch,  $A$  sei von den Elementen  $f(e_1), \dots, f(e_n)$  erzeugt.
- Ein Gruppenmorphisms  $f : G \rightarrow H$  wird trivial genannt, wenn  $f(g) = 1$  ist für alle  $g \in G$ . Wir schreiben diesenfalls auch  $f = ! = !_G, H$ .
- Ein Gruppenmorphisms von  $G$  nach  $G$  heißt Endomorphisms. Ein bijektiver Endomorphisms heißt Automorphisms.
- Für  $g \in G$  bezeichne häufig  $g^- := g^{-1}$  das Inverse zu  $g$ , i.e.  $gg^- = 1 = g^-g$ .
- Für  $g \in G$ ,  $a \in \mathbf{Z}$  und  $b \in \mathbf{Z}_{\geq 0}$  sei  $g^{a^b} := g^{(a^b)}$ .
- Für  $g, x \in G$  ist  ${}^g x := gxg^-$ , gesprochen:  $g$  konjugiert  $x$ .
- Für  $g, h \in G$  ist  $[g, h] := g^-h^-gh$  der Kommutator von  $g$  und  $h$ .
- Ist  $S \subseteq G$ , dann ist  $\langle S \rangle \leq G$  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  $U, V \leq G$  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 80.
- Es bedeutet  $U \leq G$ , daß  $U$  eine Untergruppe von  $G$  ist. Es bedeutet  $U < G$ , daß  $U \leq G$  und  $U \neq G$  ist; es heißt dann  $U$  echte Untergruppe von  $G$ .
- Es bedeutet  $N \trianglelefteq G$ , daß  $N$  eine normale Untergruppe von  $G$  ist, auch Normalteiler genannt. Es bedeutet  $U \triangleleft G$ , daß  $U \trianglelefteq G$  und  $U \neq G$  ist.
- Eine Gruppe  $G$  mit  $|G| > 1$  heißt einfach, wenn 1 und  $G$  die einzigen Normalteiler von  $G$  sind.
- Für  $U \leq G$  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  $\text{Kern}(f) \trianglelefteq G$ , sein Bild  $\text{Im}(f) \leq H$  geschrieben.
- Eine Sequenz von Gruppen und Gruppenmorphisimen  $G' \xrightarrow{u} G \xrightarrow{v} G''$  heißt exakt bei  $G$ , wenn  $\text{Kern}(v) = \text{Im}(u)$  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  $(M, \alpha)$  bestehend aus einer Menge  $M$  und einem Gruppenmorphimus  $\alpha : G \rightarrow S_M$  heißt  $G$ -Menge. Hierbei heißt  $\alpha$  Operation von  $G$  auf  $M$ .

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

Ist  $\alpha$  injektiv, so heißt  $M$  eine *treue*  $G$ -Menge.

**Bemerkung.** Sei  $M$  eine Menge.

- (1) Sei gegeben ein Gruppenmorphimus  $\alpha : G \rightarrow S_M$ . Dieser liefert die Abbildung  $\mu : G \times M \rightarrow M$ ,  $(g, m) \mapsto \alpha(g)(m) =: g \cdot m = gm$ . Für diese gilt

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

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  $\mu : G \times M \rightarrow M$ ,  $(g, m) \mapsto g \cdot m = gm$ , 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  $M \rightarrow M$ ,  $m \mapsto g \cdot m$  beidseitig invertiert von der Abbildung  $M \rightarrow M$ ,  $m \mapsto g^{-1} \cdot m$ , da zum

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

$$\alpha : G \longrightarrow S_M, \quad g \longmapsto (m \mapsto g \cdot m)$$

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  $\alpha : G \longrightarrow S_M$  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  $n \geq 0$ . Es ist  $[1, n]$  eine  $S_n$ -Menge via  $\text{id}_{S_n} : S_n \longrightarrow S_n$ , i.e. via  $\sigma \cdot i = \sigma(i)$  für  $\sigma \in S_n$  und  $i \in [1, n]$ .

Sei  $U \leq S_n$ . Betrachte den Einbettungsmorphismus  $\iota : U \longrightarrow S_n$ . 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  $\varphi$  wird  $(M, \alpha \circ \varphi)$  eine  $H$ -Menge. Manchmal schreibt man diese  $M|_{\varphi}$  oder  $M|_H^G$ .

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

- (3) Ist  $U \leq G$ , 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  $\alpha : G \longrightarrow S_{G/U}, g \longmapsto (xU \mapsto gxU)$ .

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

Es ist  $x \in G$  genau dann in  $\text{Kern}(\alpha)$  enthalten, wenn für  $g \in G$  gilt, daß  $xgU = gU$ , i.e.  $g^{-1}xgU = U$ , i.e.  $g^{-1}xg \in U$ , i.e.  $x \in {}^gU$  ist. Also ist  $\text{Kern}(\alpha) = \bigcap_{g \in G} {}^gU$ . 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  $\alpha : \text{GL}(V) \longrightarrow S_V, \varphi \longmapsto \varphi$  ist  $V$  eine  $\text{GL}(V)$ -Menge, i.e. via  $\varphi \cdot v = \varphi(v)$  für  $\varphi \in \text{GL}(V)$  und  $v \in V$ . Ist  $H$  eine Gruppe und  $\gamma : H \longrightarrow \text{GL}(V)$  ein Gruppenmorphismus, so wird  $V|_{\gamma} = (V, \alpha \circ \gamma)$  auch zu einer  $H$ -Menge; cf. (2).

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

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

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

**Definition 3** Seien  $G$ -Mengen  $M$  und  $N$  gegeben.

Eine Abbildung  $a : M \rightarrow N$  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  $U \leq V \leq G$ . Dann ist  $f : G/U \rightarrow G/V$ ,  $gU \mapsto gV$  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  $G \rightarrow M$ ,  $g \mapsto gm$  eine  $G$ -Abbildung.

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

- (1) Es ist  $\text{id}_M$  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. Diesemfalls ist  $N$  via  $G \rightarrow S_N$ ,  $g \mapsto (n \mapsto gn)$  wieder eine  $G$ -Menge. Wir haben die  $G$ -Abbildung  $N \rightarrow M$ ,  $n \mapsto n$ .

**Beispiel 8**

- (1) Sei  $k \geq 0$ . Seien  $G$ -Mengen  $M_i$  für  $i \in [1, k]$  gegeben. Es wird  $M := \prod_{i \in [1, k]} M_i$  mittels  $\alpha : G \rightarrow S_M$ ,  $g \mapsto ((m_i)_i \mapsto (gm_i)_i)$  eine  $G$ -Menge.
- (2) Sei  $k \geq 0$ . 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  $g(h\bar{m}) = \overline{ghm} = \overline{ghm} = (gh)\bar{m}$  für  $m \in M$  und  $g, h \in G$ , was die Operation  $\bar{\alpha} : G \rightarrow S_{\bar{M}}, g \mapsto (\bar{m} \mapsto \overline{gm})$  liefert.

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

**Beispiel.** Sei eine  $G$ -Abbildung  $f : M \rightarrow N$  zwischen  $G$ -Mengen gegeben. Es ist  $f(M)$  eine  $G$ -Teilmenge von  $N$ . Sei die Äquivalenzrelation ( $\sim$ ) auf  $M$  definiert durch

$$m \sim m' \quad :\iff \quad f(m) = f(m')$$

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

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

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.

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ & \searrow r & \nearrow \\ & \bar{M} & \xrightarrow[\sim]{\bar{f}} f(M) \end{array}$$

**Definition 10** Sei  $M$  eine  $G$ -Menge.

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

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

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  $! : G \rightarrow S_{\bar{M}}$ . Denn sind  $m, m' \in M$  und  $g \in G$  mit  $gm = m'$  gegeben, dann ist für  $x \in G$  auch  $xgxm = xm'$ .

- (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 11** 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  ${}^Gx := \{ {}^gx : g \in G \}$  für die Konjugationsklasse von  $x$ .

**Bemerkung 12** Sei  $M$  eine transitive  $G$ -Menge.

- (1) Die einzigen  $G$ -Teilmengen von  $M$  sind  $\emptyset$  und  $M$ .
- (2) Ist  $M \rightarrow T$  eine surjektive  $G$ -Abbildung in eine  $G$ -Menge  $T$ , dann ist  $T$  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 13** Sei  $k \geq 0$ .

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 14** Sei  $M$  eine  $G$ -Menge. Sei  $0 \leq k \leq \ell$ . Ist  $M$  eine  $\ell$ -fach transitive  $G$ -Menge, so ist sie auch  $k$ -fach transitiv.

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

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

ist mithin surjektiv. Aus der Transitivität von  $M^{\times \ell, \neq}$  folgt also die Transitivität von  $M^{\times k, \neq}$ ; cf. Bemerkung 12.(2). □

**Beispiel 15**

- (1) Sei  $n \geq 0$ . 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  $(1, 2, \dots, n)$  auf dieses Tupel schickt.

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

(2) Betrachte

$$A_4 = \{\text{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), \\ (1, 2, 3), (1, 2, 4), (1, 3, 2), (1, 3, 4), (1, 4, 2), (1, 4, 3), (2, 3, 4), (2, 4, 3)\}.$$

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

$$\begin{aligned} & A_4(1, 2) \\ &= \{(\sigma(1), \sigma(2)) : \sigma \in A_4\} \\ &= \{(1, 2), (2, 1), (3, 4), (4, 3), \\ &\quad (2, 3), (2, 4), (3, 1), (3, 2), (4, 1), (4, 2), (1, 3), (1, 4)\} \\ &= [1, 4]^{\times 2, \neq}. \end{aligned}$$

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  $A_4 \xrightarrow{\sim} [1, 4]^{\times 2, \neq}$ ,  $\sigma \mapsto (\sigma(1), \sigma(2))$  zeigt; cf. Beispiel 5.

## 1.2 Zentralisator

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

**Definition 16** Sei  $N \subseteq M$  eine Teilmenge. Sei

$$C_G(N) := \{g \in G : gn = n \text{ für } n \in N\}$$

der *Zentralisator* (oder *Stabilisator*) von  $N$  <sup>(1)</sup>.

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

Insbesondere ist  $C_G(M) = \text{Kern}(\alpha) \trianglelefteq G$ .

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

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

**Bemerkung 17** Sei  $N \subseteq M$  eine Teilmenge. Sei  $x \in G$ . Schreibe  $xN := \{xn : n \in N\}$ . Es ist

$$C_G(xN) = {}^x C_G(N).$$

<sup>1</sup>Das  $C$  in  $C_G(N)$  steht für engl. centraliser.

*Beweis.* Es ist  $g \in C_G(xN)$  genau dann, wenn  $gxn = xn$  für  $n \in N$ , i.e.  $x^{-1}gxn = n$  für  $n \in N$ , i.e.  $x^{-1}gx \in C_G(N)$ , i.e.  $g \in {}^x C_G(N)$ .  $\square$

**Beispiel 18** Betrachte  $G$  als  $G$ -Menge via Konjugation.

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

**Lemma 19 (Bahnenlemma)** Sei  $m \in M$ .

Wir haben die  $G$ -Bijektion

$$\begin{array}{ccc} G/C_G(m) & \xrightarrow{\beta_m} & Gm \\ gC_G(m) & \mapsto & gm. \end{array}$$

*Beweis.* Schreibe  $C := C_G(m)$ .

Es ist  $\beta_m$  wohldefiniert und injektiv, da für  $g, \tilde{g} \in G$  genau dann  $gm = \tilde{g}m$  ist, wenn  $m = g^{-1}\tilde{g}m$  ist, i.e.  $g^{-1}\tilde{g} \in C$ , i.e.  $g^{-1}\tilde{g}C = C$ , i.e.  $\tilde{g}C = gC$ .

Es ist  $\beta_m$  surjektiv.

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

**Korollar 20** Ist  $G$  endlich und  $M$  transitiv, so ist  $|M|$  ein Teiler von  $|G|$ .

*Beweis.* Sei  $m \in M$ . Es ist  $|G| = |Gm| \cdot |C_G(m)| = |M| \cdot |C_G(m)|$ ; cf. Lemma 19.  $\square$

**Bemerkung 21** Sei  $M$  transitiv. Sei  $m \in M$ .

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

- (1) Es ist  $C_G(m) \leq C_G(f(m)) \leq G$ .
- (2) Es ist  $C_G(m) = C_G(f(m))$  genau dann, wenn  $f$  bijektiv ist.
- (3) Es ist  $C_G(f(m)) = G$  genau dann, wenn  $T$  trivial ist.

*Beweis.* Es ist  $T$  transitiv; cf. Bemerkung 12.(2). Also ist  $T$  isomorph zu  $G/C_G(f(m))$  gemäß Lemma 19.

*Ad (1).* Für  $g \in G$  folgt aus  $g \in C_G(m)$ , daß  $gf(m) = f(gm) = f(m)$  und also  $g \in C_G(f(m))$  ist.

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



Sei umgekehrt  $C_G(m) = C_G(f(m))$ . Sind  $g, h \in G$  gegeben mit  $f(gm) = f(hm)$ , dann ist  $gf(m) = hf(m)$ , also  $h^{-1}gf(m) = f(m)$ , also  $h^{-1}g \in C_G(f(m)) = C_G(m)$ , also  $h^{-1}gm = m$  und somit  $gm = hm$ . Also ist  $f$  injektiv.

Ad (3). Ist  $T$  trivial, dann ist  $|T| = 1$  und also  $C_G(f(m)) = G$ .

Ist umgekehrt  $C_G(f(m)) = G$ , dann ist  $T$  isomorph zu  $G/G$ , i.e. trivial.  $\square$

## 1.3 Fixpunkte

Sei  $M$  eine  $G$ -Menge.

**Definition 22** Sei  $A \subseteq G$  eine Teilmenge. Sei

$$\text{Fix}_A(M) := \{ m \in M : am = m \text{ f\"ur } a \in A \}$$

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

**Bemerkung 23** Sei  $x \in G$ . Sei  $A \subseteq G$ . Es ist  $\text{Fix}_{x^{-1}A}(M) = x \text{Fix}_A(M)$ .

*Beweis.* Es ist  $m \in \text{Fix}_{x^{-1}A}(M)$  genau dann, wenn  $x^{-1}a \cdot m = m$  f\"ur  $a \in A$ , i.e. wenn  $ax^{-1}m = m$  f\"ur  $a \in A$ , i.e. wenn  $x^{-1}m \in \text{Fix}_A(M)$ , i.e. wenn  $m \in x \text{Fix}_A(M)$ .  $\square$

**Lemma 24 (Cauchy)** Seien  $G$  und  $M$  endlich.

Sei  $t := |\{ Gg : g \in G \}|$ . W\"ahle  $g_i \in G$  f\"ur  $i \in [1, t]$  mit  $G = \bigsqcup_{i \in [1, t]} Gg_i$ .

Dann ist

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

*Beweis.*

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

$$\begin{aligned} \sum_{g \in G} |\text{Fix}_g(M)| &= |\{ (g, m) \in G \times M : m \in \text{Fix}_g(M) \}| \\ &= |\{ (g, m) \in G \times M : gm = m \}| \\ &= |\{ (g, m) \in G \times M : g \in C_G(m) \}| \\ &= \sum_{m \in M} |C_G(m)| \\ &\stackrel{\text{L. 19}}{=} |G| \sum_{m \in M} |Gm|^{-1} \\ &= |G| \sum_{i \in [1, \ell]} |Gm_i| |Gm_i|^{-1} \\ &= |G| \cdot \ell. \end{aligned}$$

Zeigen wir die zweite Gleichheit. Es genügt,  $\frac{1}{|G|} \sum_{g \in C_{g_i}} |\text{Fix}_g(M)| \stackrel{!}{=} \frac{|\text{Fix}_{g_i}(M)|}{|C_G(g_i)|}$  zu zeigen für  $i \in [1, t]$ . Gemäß Bemerkung 23 ist

$$\begin{aligned} \sum_{g \in C_{g_i}} |\text{Fix}_g(M)| &\stackrel{\text{B. 23}}{=} \sum_{g \in C_{g_i}} |\text{Fix}_{g_i}(M)| \\ &= |C_{g_i}| \cdot |\text{Fix}_{g_i}(M)| \\ &\stackrel{\text{L. 19}}{=} |G| \cdot |C_G(g_i)|^{-1} \cdot |\text{Fix}_{g_i}(M)|. \end{aligned}$$

□

Lemma 24 ist auch ein Spezialfall der Frobenius-Reziprozität aus der Charaktertheorie, sofern diese bekannt sein sollte. Sei dazu o.E.  $M$  transitiv. Es ist  $g \mapsto |\text{Fix}_g(M)|$  der Charakter des zu  $M$  gehörigen Permutationsmodul, welcher sich aus dem trivialen Charakter von  $C_G(m)$  durch Induktion nach  $G$  ergibt, wobei  $m \in M$  zu wählen ist. Da das Skalarprodukt des trivialen Charakters von  $C_G(m)$  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 transitive  $G$ -Menge; cf. Definition 1.

### Definition 25

- (1) Ist  $M$  nichttrivial, so heißt  $M$  *primitiv*, wenn für jede surjektive  $G$ -Abbildung  $M \rightarrow T$  in eine  $G$ -Menge  $T$  entweder diese  $G$ -Abbildung bijektiv 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 hat also eine transitive  $G$ -Menge nur die unvermeidbaren Teilobjekte, eine primitive  $G$ -Menge zudem nur die unvermeidbaren Faktorobjekte.

**Beispiel 26** Ist  $|M|$  endlich und prim, dann ist  $M$  primitiv. Denn ist  $f : M \rightarrow T$  eine surjektive  $G$ -Abbildung in eine nichttriviale  $G$ -Menge  $T$  und ist  $m \in M$ , so ist  $C_G(m) \leq C_G(f(m)) < G$  nach Bemerkung 21.(1, 3), folglich  $[G : C_G(f(m))]$  ungleich 1 und Teiler der Primzahl  $[G : C_G(m)] \stackrel{\text{L. 19}}{=} |M|$ , folglich  $[G : C_G(f(m))] = [G : C_G(m)]$ , i.e.  $C_G(m) = C_G(f(m))$ , i.e.  $f$  bijektiv; cf. Bemerkung 21.(2).

**Lemma 27** Sei an  $M$  transitiv erinnert. Sei  $M$  nichttrivial.

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  $C_G(m)$  maximal in der Menge der echten Untergruppen von  $G$ .*
- (5) *Für jedes  $m \in M$  ist  $C_G(m)$  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  $C_G(xm_0) = {}^x C_G(m_0)$ , sodaß aus  $C_G(m_0)$  maximal folgt, daß auch  $C_G(xm_0)$  maximal ist; cf. Bemerkung 17. Dank Transitivität von  $M$  folgt also aus  $C_G(m_0)$  maximal für ein  $m_0 \in M$ , daß  $C_G(m)$  maximal ist für alle  $m \in M$ .

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

Sei  $m \in M$ . Es ist  $C_G(m) \leq C_G(f(m)) \leq G$ ; cf. Bemerkung 21.(1). Da  $T$  nichttrivial ist, ist  $C_G(f(m)) < G$ ; cf. Bemerkung 21.(3). Da  $C_G(m)$  maximal ist, folgt  $C_G(m) = C_G(f(m))$ . Mithin ist  $f$  bijektiv; cf. Bemerkung 21.(2).

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

*Annahme,* es gibt  $C_G(m) < U < G$ . Dann ist  $G/U$  nichttrivial. Wir erhalten als Kompositum von  $M \xrightarrow{\sim} G/C_G(m) \rightarrow G/U$  eine surjektive, nichtinjektive  $G$ -Abbildung; cf. Beispiel 4, Lemma 19. Dies steht im *Widerspruch* zur Primitivität von  $M$ .

*Ad (¬1)  $\Rightarrow$  (¬2).* Sei  $M$  nicht primitiv. Dann gibt es eine surjektive, nichtinjektive  $G$ -Abbildung  $f : M \rightarrow T$  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, denn für  $m, m' \in M$  und  $g \in G$  folgt aus  $f(m) = f(m')$ , daß  $f(gm) = gf(m) = gf(m') = f(gm')$  ist. Da  $f$  nichtinjektiv ist, ist  $(\sim)$  nicht diskret. Da  $T$  nichttrivial ist, ist  $(\sim)$  nicht verklumpt.

*Ad (¬2)  $\Rightarrow$  (¬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  $M \rightarrow \bar{M}$ ,  $m \mapsto \bar{m}$ . Es ist  $\bar{M}$  nichttrivial, da  $(\sim)$  nicht verklumpt ist. Es ist diese Abbildung nicht bijektiv, da  $(\sim)$  nicht diskret ist.

*Ad (¬2)  $\Rightarrow$  (¬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 (¬3)  $\Rightarrow$  (¬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  $gm' \in B \cap gh^{-1}B$ , also  $B = gh^{-1}B$  und somit  $gm'' \in gh^{-1}B = B$  folgt. Es ist  $(\sim)$  eine  $G$ -Äquivalenzrelation, da für  $m, m' \in M$  und  $g, x \in G$  aus  $gm, gm' \in B$  auch  $gx^{-1}(xm), gx^{-1}(xm') \in B$  folgt. Es ist  $(\sim)$  nicht diskret, da  $|B| > 1$ . Es ist  $(\sim)$  nicht verklumpt, da  $B \subset M$  und infolgedessen für  $m \in M \setminus B, b \in B$  und  $g \in G$  nicht  $gm, gb \in B$  gelten kann, da ansonsten aus  $b \in B \cap g^{-1}B$  auch  $B = g^{-1}B \ni m$  folgte.  $\square$

**Lemma 28** *Sei  $M$  zweifach transitiv. Dann ist  $M$  primitiv.*

*Beweis.* Es ist  $M^{\times 2, \neq} \neq \emptyset$ , also  $|M| \geq 2$  und somit  $M$  nichttrivial. Es ist  $M$  transitiv; cf. Bemerkung 14.

*Annahme,*  $M$  ist nicht primitiv. Dann gibt es eine  $G$ -Äquivalenzrelation  $(\sim)$  auf  $M$ , die weder diskret noch verklumpt ist; cf. Lemma 27. 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*.  $\square$

**Beispiel 29** Sei  $n \geq 2$ . Sei  $G := S_n$ . Sei  $M := [1, n]$ ; cf. Beispiel 2.(1). Es ist  $C_{S_n}(n) = S_{[1, n-1]} = S_{n-1}$ .

Es ist  $[1, n]$  eine  $n$ -fach transitive  $S_n$ -Menge; cf. Beispiel 15.(1). Da  $n \geq 2$ , ist  $[1, n]$  auch eine 2-fach transitive  $S_n$ -Menge; cf. Bemerkung 14. Folglich ist  $[1, n]$  eine primitive  $S_n$ -Menge; cf. Lemma 28. Also ist  $S_{n-1} < S_n$  eine maximale echte Untergruppe; cf. Lemma 27. Ist  $n$  prim, dann ist dies auch von vornherein klar.

**Beispiel 30** Sei  $K$  ein Körper.

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

Es ist  $V$  eine  $GL(V)$ -Menge; cf. Beispiel 2.(4). Es ist  $V^\times \subseteq V$  eine  $GL(V)$ -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  $\lambda^{-1}$ , transitiv dank Produkt. Es ist  $(\sim)$  eine  $GL(V)$ -Äquivalenzrelation, da für  $\alpha \in GL(V)$ , 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  $P(V) := V^\times / (\sim)$  für die resultierende  $GL(V)$ -Menge. Für  $v \in V^\times$  ist die Äquivalenzklasse  $\bar{v}$  die von  $v$  aufgespannte Gerade in  $V$ , ausgenommen 0. Geometrisch gesehen ist  $P(V)$  der projektive Raum von  $V$ .

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

Wir wollen  $P(V)$  als zweifach transitive  $SL(V)$ -Menge erkennen.

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

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

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

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

Es gibt genau ein  $\beta \in GL(V)$  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.  $\beta \in SL(V)$ . 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  $P(V)$  eine zweifach transitive und damit auch primitive  $SL(V)$ -Menge; cf. Lemma 28.

Sei  $m \geq 2$ . Wir schreiben auch  $P^{m-1}(K) := P(K^m)$ . Es ist also auch  $P^{m-1}(K)$  eine zweifach transitive und somit primitive  $SL_m(K)$ -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  $C_G(m)$  liefern.

### Lemma 31 (Schreier)

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

Sei  $\tau : G \rightarrow T$  festgelegt durch  $\tau(g)m = gm$  für  $g \in G$ . Insbesondere ist  $\tau(1) = 1$ .

Dann ist

$$C_G(m) = \langle \tau(xt)^-xt : x \in S^\pm, t \in T \rangle$$

*Beweis.*

*Ad  $\geq$ .* Es ist  $xm = \tau(xt)m$ , i.e.  $\tau(xt)^-xm = m$ , i.e.  $\tau(xt)^-xt \in C_G(m)$  für  $x \in S^\pm$  und  $t \in T$ .

*Ad  $\leq$ .* Sei  $g \in C_G(m)$ . Schreibe  $g = x_k x_{k-1} \cdots x_1$  mit  $k \geq 0$  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

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

Da, wie schon gesehen,  $y \in C_G(m)$  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 32 (Bahnenalgorithmus)

Setze

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

und für  $i \geq 0$  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  $i \geq 0$

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

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  $T_{i+1} \rightarrow N_{i+1}$ ,  $\hat{t} \mapsto \hat{t}m$  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  $i \geq 0$  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  $i \geq 0$  folgt aus  $N_i = \emptyset$  auch  $N_{i+1} = \emptyset$ . Also gibt es genau ein

$$j \geq 0$$

mit  $N_i \neq \emptyset$  für  $i \leq j$  und  $N_i = \emptyset$  für  $i \geq j + 1$ .

Sei  $g \in G$ . Schreibe  $gm = x_\ell x_{\ell-1} \cdots x_1 m$  mit  $\ell \geq 0$  und  $x_i \in S^\pm$  für  $i \in [1, \ell]$ ; sei hierfür  $\ell$  minimal. Wir behaupten  $gm \in N_\ell$ . Wir wollen induktiv  $x_i x_{i-1} \cdots x_1 m \in N_i$  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  $x_{i+1} x_i x_{i-1} \cdots x_1 m \notin N_{[0, i]}$ , da sonst  $x_{i+1} x_i x_{i-1} \cdots x_1 m = y_k y_{k-1} \cdots y_1 m$  wäre

für ein  $k \in [0, i]$  und gewisse  $y_h \in S^\pm$  für  $h \in [1, k]$ , woraus  $gm = x_\ell x_{\ell-1} \cdots x_1 m = x_\ell x_{\ell-1} \cdots x_{i+2} y_k y_{k-1} \cdots y_1 m$  folgte, was wegen der Minimalität von  $\ell$  nicht so ist. Folglich ist  $x_{i+1} x_i x_{i-1} \cdots x_1 m \in N_{i+1}$ . 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  $\tau : G \rightarrow T_{[0,j]}$  mit  $gm = \tau(g)m$  für  $g \in G$ .

Sei  $\hat{R} := \{xt : x \in S^\pm, t \in T_{[0,j]}\}$ . Gemäß Lemma 31 ist

$$C_G(m) = \langle \tau(xt)^{-1}xt : x \in S^\pm, t \in T_{[0,j]} \rangle = \langle \tau(r)^{-1}r : r \in \hat{R} \rangle.$$

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

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

ist also immer noch

$$C_G(m) = \langle \tau(r)^{-1}r : r \in R \rangle.$$

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  $j \geq 0$  dann  $N_j \neq \emptyset$ , aber  $N_{j+1} = \emptyset$  ergibt.

Dann besteht  $Gm$  aus den unmarkierten Elementen des Baums.

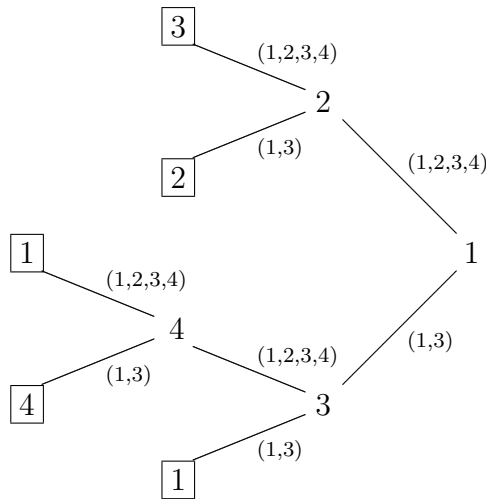
Für jedes markierte Element des Baums nehmen wir das Produkt  $r$  der auf dem Kantenzug von diesem Element nach  $m$  notierten Faktoren. Dieses markierte Element tritt rechts oder oberhalb von sich bereits unmarkiert im Baum auf. Das Produkt der auf dem Kantenzug von diesem unmarkierten Element nach  $m$  markierten Faktoren ist  $\tau(r)$ . Bilde  $\tau(r)^{-1}r$ . Sodann ist  $C_G(m)$  erzeugt von den so entstandenen Elementen  $\tau(r)^{-1}r$ .

Oft kann durch direkte Betrachtung das so gewonnene Erzeugendensystem von  $C_G(m)$  noch reduziert werden.

**Beispiel 33** Sei  $G := \langle (1, 2, 3, 4), (1, 3) \rangle \leq S_4$ . 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 Bahnalgorithmus, Algorithmus 32, liefert folgenden von rechts nach links erstellten Baum.



Somit ist  $M$  transitiv.

In der Notation von Algorithmus 32 ist  $j = 2$  und

$$T_{[0,2]} = \left\{ \underbrace{\text{id}}_{\in T_0}, \underbrace{(1, 2, 3, 4), (1, 3)}_{\in T_1}, \underbrace{(1, 2, 3, 4) \circ (1, 3)}_{\substack{\in T_2 \\ = (1,4)(2,3)}} \right\}$$



Ferner ist  $C_G(m)$  erzeugt von folgender Liste von Elementen.

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

Folglich ist  $C_G(m) = \langle (2, 4) \rangle$ .

Insbesondere ist  $|C_G(m)| = 2$  und  $|Gm| = 4$ , woraus wir  $|G| = |Gm| \cdot |C_G(m)| = 8$  entnehmen; cf. Lemma 19.

Ist die Ordnung von  $C_G(m)$  an dieser Stelle noch nicht ablesbar, so kann das Verfahren fortgesetzt werden, indem  $m' \in M \setminus \{m\}$  gewählt und die Operation von  $C_G(m)$  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 34

- (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  $U \leq G$  eine  $p$ -Untergruppe, falls  $U$  eine  $p$ -Gruppe ist.
- (3) Es heißt  $P \leq G$  eine  $p$ -Sylowuntergruppe, 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  $\text{Syl}_p(G)$  bezeichnet. Es ist  $\text{Syl}_p(G)$  eine  $G$ -Teilmenge von  $\text{Pot}(G)$  im Sinne von Aufgabe 4.(7).

**Lemma 35** Sei  $M$  eine nichtleere endliche  $G$ -Menge.

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

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

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

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

und

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

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  $\text{Fix}_{P(n')}(M) = \{n'\}$ . Folglich ist mit Aufgabe 7.(1)

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

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

**Lemma 36** Sei  $\Omega := \{U \leq G : U \text{ ist eine } p\text{-Untergruppe von } G\}$ . Es operiert  $G$  auf  $\Omega$  via Konjugation; cf. Aufgabe 4.(7).

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

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

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

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

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

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

*Ad*  $\subseteq$ . Sei  $P \in \text{Fix}_Q(\Omega_{\max})$  gegeben, i.e. sei  ${}^gP = P$  für  $g \in Q$ , i.e. sei  $Q \leq N_G(P)$ ; cf. Aufgabe 4.(6). Dann ist  $PQ \leq G$  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  $Q \not\leq P$ . Somit ist  $PQ > P$ , im *Widerspruch* zur Maximalität von  $P$ . □

**Satz 37 (Sylow)** Sei an die endliche Gruppe  $G$  und die Primzahl  $p > 0$  erinnert.

- (1) Es ist  $\text{Syl}_p(G) \neq \emptyset$ .
- (2) Es ist  $\text{Syl}_p(G)$  eine transitive  $G$ -Menge unter der Konjugationsoperation.
- (3) Es ist  $|\text{Syl}_p(G)| \equiv_p 1$ .

Für  $P \in \text{Syl}_p(G)$  ist dabei  $|\text{Syl}_p(G)| = |G|/|N_G(P)|$ , was  $|G|/|G|[p]$  teilt.

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

*Beweis.* Sei  $\Omega_{\max}$  die Menge der maximalen  $p$ -Untergruppen von  $G$ ; cf. Lemma 36. Dank Lemma 36 können wir Lemma 35 verwenden um zu schließen, daß  $\Omega_{\max}$  transitiv und  $|\Omega_{\max}| \equiv_p 1$  ist.

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

*Annahme*, es gibt ein  $Q \in \Omega_{\max}$  mit  $|Q| < |G|[p]$ . Sei  $N := N_G(Q)$ ; cf. Aufgabe 4.(6). Es ist  $[G : N] = |\Omega_{\max}| \equiv_p 1$ ; cf. Lemma 19. 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 (1) aus Lemma 36. Es folgt (2) aus  $\Omega_{\max}$  transitiv. Es folgt (3) aus  $|\Omega_{\max}| \equiv_p 1$  sowie aus Lemma 19 und  $P \leq N_G(P)$ ; cf. Aufgabe 4.(6). Es folgt (4) aus der Konstruktion von  $\Omega_{\max}$ .  $\square$

Cf. auch [7, Satz 13].

**Beispiel 38** Es ist  $\text{Syl}_3(S_4) = \{ \langle (1, 2, 3) \rangle, \langle (1, 2, 4) \rangle, \langle (1, 3, 4) \rangle, \langle (2, 3, 4) \rangle \}$ . Somit ist in der Tat  $|\text{Syl}_3(S_4)| = 4 \equiv_3 1$ ; cf. Satz 37.(3).

**Korollar 39** Sei  $P \in \text{Syl}_p(G)$  gewählt; cf. Satz 37.(1).

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

*Beweis.* Ist  $P \trianglelefteq G$ , dann ist  $\text{Syl}_p(G) = \{ {}^gP : g \in G \} = \{P\}$  gemäß Satz 37.(2) und also  $|\text{Syl}_p(G)| = 1$ .

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

## 2.2 Einfachheit

### 2.2.1 Iwasawa

Sei  $G$  eine Gruppe.

**Definition 40** Ist  $G = G^{(1)}$ , so heißt  $G$  *perfekt*; cf. Aufgabe 13.

**Lemma 41 (Iwasawa-Kriterium)**

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

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

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

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

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

*Beweis.*

*Ad (1).* Es ist  $\bigcap_{g \in G} {}^g C = \bigcap_{g \in G} C_G(gm) = K$  wegen der Transitivität von  $M$ ; cf. Bemerkung 17. Aus  $N \trianglelefteq G$  und  $N \not\leq K$  folgt also  $N \not\leq C$ . Da  $C$  eine maximale echte Untergruppe von  $G$  ist, folgt  $G = NC$ ; cf. Lemma 27, Aufgabe 12.(2).

Sei  $g \in G$ . Sei  $a \in A$ . Schreibe  $g = nc$  mit  $n \in N$  und  $c \in C$ . Es wird  ${}^g a = n(cac^{-1})n^{-1} = n \cdot {}^{cac^{-1}} n^{-1} \cdot (cac^{-1}) \in NA$ . Folglich ist  ${}^g A \leq NA$ .

Es folgt  $G = \langle {}^g A : g \in G \rangle \leq NA \leq G$ , also  $NA = G$ .

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

*Ad (2).* 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  $G = G^{(1)} \leq N \trianglelefteq G$ , also  $N = G$ .  $\square$

## 2.2.2 Einfachheit von $A_n$ für $n \geq 5$

**Lemma 42** *Sei  $n \geq 2$ . Es wird  $A_n$  von  $\{\sigma \in A_n : \sigma \text{ ist 3-Zykel}\}$  erzeugt.*

*Beweis.* Induktion über  $n$ . Es ist  $A_2 = 1$ .

Sei  $n \geq 2$ . Sei  $\rho \in A_{n+1}$  gegeben. Ist  $\rho(n+1) = n+1$ , dann ist  $\rho \in A_n$ , also Produkt von 3-Zykeln.

Sei  $\rho(n+1) \neq n+1$ . Sei  $\ell \in [1, n+1] \setminus \{n+1, \rho(n+1)\}$ , möglich, da  $n \geq 2$ . Dann ist mit  $\rho' := (\rho(n+1), n+1, \ell) \circ \rho$  wieder  $\rho'(n+1) = n+1$ . Also ist  $\rho' \in A_n$  und somit Produkt von 3-Zykeln. Folglich ist auch  $\rho$  Produkt von 3-Zykeln.  $\square$

**Lemma 43** *Sei  $n \geq 5$ . Sei  $N \trianglelefteq A_n$ . Enthält  $N$  einen 3-Zykel, dann ist  $N = A_n$ .*

*Beweis.* Sei  $(a, b, c) \in N$  mit  $a, b, c \in [1, n]$  mit  $|\{a, b, c\}| = 3$ . Für  $\sigma \in A_n$  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  $A_n^{(1)}$ ; cf. Aufgabe 5.  $\square$

**Lemma 44** *Sei  $n \geq 5$ . Es ist  $A_n$  perfekt.*

*Beweis.* Dank Lemma 43 bleibt also zu zeigen, daß  $A_n^{(1)}$  einen 3-Zykel enthält.

Es ist  $[(1, 2, 3), (3, 4, 5)] = (1, 3, 2) \circ (3, 5, 4) \circ (1, 2, 3) \circ (3, 4, 5) = (2, 5, 3) \in A_n^{(1)}$ .  $\square$

**Lemma 45** *Es ist  $A_5$  einfach.*

*Beweis.* Es operiert  $G := A_5$  dreifach transitiv und treu auf  $[1, 5]$ ; cf. Aufgabe 5. Also operiert  $G$  primitiv auf  $[1, 5]$ ; cf. Bemerkung 14, Lemma 28.

Es ist  $A_4 = C_G(5) =: C$ .

Es ist  $A := \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle = {}^C \text{id} \sqcup {}^C(1, 2)(3, 4) \trianglelefteq C$ . Es ist  $\langle {}^g A : g \in G \rangle = G$ ; cf. Aufgabe 14.

Somit folgt die Einfachheit von  $A_5$  aus Lemma 41.(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 45 nicht wirklich benötigt und sollen hiermit nur illustriert werden.

### Satz 46 (Einfachheit der alternierenden Gruppe)

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

*Beweis.* Induktion über  $n \geq 5$ . Für  $n = 5$  ist dies Lemma 45.

Sei  $n \geq 6$ .

*Behauptung 1.* Für  $N \triangleleft A_n$  ist  $|N|$  ein Teiler von  $n$ .

Es ist  $N \cap A_{n-1} \trianglelefteq A_{n-1}$ , dank Induktion also  $N \cap A_{n-1} = 1$  oder  $N \cap A_{n-1} = A_{n-1}$ .

Ist  $N \cap A_{n-1} = A_{n-1}$ , dann enthält  $N$  einen 3-Zykel, da  $n - 1 \geq 3$ . Also ist  $N = A_n$ ; cf. Lemma 43. Dies ist ausgeschlossen.

Ist  $N \cap A_{n-1} = 1$ , dann ist

$$A_{n-1} \simeq A_{n-1}/(N \cap A_{n-1}) \simeq NA_{n-1}/N \leq A_n/N;$$

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

Dies zeigt *Behauptung 1*.

*Behauptung 2.* Sei  $N \triangleleft A_n$ . Dann ist  $N \leq M := N \circ {}^{(1,2)}N \triangleleft A_n$  und auch  $M \triangleleft S_n$ .

Es ist  ${}^{(1,2)}N \trianglelefteq {}^{(1,2)}A_n = A_n$ , denn für  $\rho \in N$  und  $\xi \in A_n$  erhalten wir

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

Es ist  $M = N \circ {}^{(1,2)}N = {}^{(1,2)}N \circ N \trianglelefteq A_n$ ; cf. Aufgabe 12.(2, 3). Es ist

$$\begin{aligned} |M| &= |N| \cdot |{}^{(1,2)}N| / |N \cap {}^{(1,2)}N| \\ &\stackrel{\text{Beh. 1}}{\leq} n \cdot n \\ &< n \cdot ((n-1) \cdot 2) \\ &\leq n \cdot ((n-1) \cdot (n-2)) \cdot (n-3)/2 \\ &\leq n!/2 \\ &= |A_n|; \end{aligned}$$

cf. Aufgabe 12.(1).

Es bleibt  ${}^\sigma M \stackrel{!}{=} M$  zu zeigen für  $\sigma \in S_n$ . Falls  $\sigma \in A_n$ , ist  ${}^\sigma M = M$  wegen  $M \trianglelefteq A_n$ . Falls  $\sigma \in S_n \setminus A_n$ , dann sei  $\sigma' := \sigma \circ (1, 2)$ , 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  $M \trianglelefteq A_n$ . Dies zeigt *Behauptung 2*.

*Annahme*, es gibt  $1 < N \triangleleft A_n$ . Dank *Behauptung 2* ist o.E. auch  $N \triangleleft S_n$ .

Die folgende Fallunterscheidung ist nicht disjunkt.

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

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

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

was mit Lemma 42 zu  $N = A_n$  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  $\rho$ , 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*. □

### 2.2.3 Einfachheit von $\text{PSL}_n(F)$ für $(n, |F|) \notin \{(2, 2), (2, 3)\}$

#### Satz 47 (Einfachheit der projektiven speziellen Gruppe)

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

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

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

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

Es ist  $M := \text{P}^{n-1}(F)$  eine primitive  $G$ -Menge; cf. Beispiel 30.

Sei  $m := \overline{e_1} = \overline{\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}} \in M$ . Sei  $C := C_G(m) = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \leq \mathrm{SL}_n(F)$ .

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

Sei  $A := \begin{pmatrix} 1 \\ 0 \end{pmatrix}_{\mathrm{E}_{n-1}} \leq C$  sein Kern. Es ist  $A$  abelsch.

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

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

Also zeigt 41.(2), daß  $G/K = \mathrm{PSL}_n(F)$  einfach ist. □

## 2.3 Präsentationen

### 2.3.1 Freie Gruppen

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

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

Sei  $F_0(X)$  die Menge der endlichen Wörter in  $X^\pm$ . Ein Element von  $F_0(X)$  ist also von der Form  $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$  mit  $n \in \mathbf{Z}_{\geq 0}$ ,  $x_i \in X$  und  $\varepsilon_i \in \{-1, +1\}$  für  $i \in [1, n]$ . Das leere Wort werde zur Kenntlichmachung mit  $\emptyset$  bezeichnet.

Sind  $u, v \in F_0(X)$ , so bezeichne  $uv$  deren Aneinandersetzung.

Es ist  $uvw := (uv)w = u(vw)$  für  $u, v, w \in F_0(X)$ .

Sei auf  $F_0(X)$  die Relation  $(\rightsquigarrow)$  dadurch erklärt, daß für  $u, v \in F_0(X)$ ,  $x \in X$  und  $\varepsilon \in \{-1, +1\}$  gelte, daß  $ux^\varepsilon x^{-\varepsilon} v \rightsquigarrow uv$  ist.

Sei  $(\approx)$  die Äquivalenzrelation auf  $F_0(X)$ , die von  $(\rightsquigarrow)$  erzeugt werde. Diese wollen wir nun auch konkret beschreiben.

Sei dazu auf  $F_0(X)$  die Relation  $(\overset{\sim}{\equiv})$  dadurch erklärt, daß für  $u, v \in F_0(X)$  genau dann  $u \overset{\sim}{\equiv} v$  gelte, wenn  $u \rightsquigarrow v$  oder  $u = v$  ist.

Für  $u, v \in F_0(X)$  ist also  $u \approx v$  genau dann, wenn es  $n \in \mathbf{Z}_{\geq 1}$  und  $w_i \in F_0(X)$  für



$i \in [1, n]$  und  $w'_i \in F_0(X)$  für  $i \in [1, n - 1]$  so gibt, daß, pars pro toto für  $n = 4$ ,

$$\begin{array}{rcc} u & = & w_1 \quad \overset{\sim}{\cong} \quad w'_1 \\ & & \parallel \\ & & w_2 \quad \overset{\sim}{\cong} \quad w'_1 \\ & & \parallel \\ & & w_2 \quad \overset{\sim}{\cong} \quad w'_2 \\ & & \parallel \\ & & w_3 \quad \overset{\sim}{\cong} \quad w'_2 \\ & & \parallel \\ & & w_3 \quad \overset{\sim}{\cong} \quad w'_3 \\ & & \parallel \\ v & = & w_4 \quad \overset{\sim}{\cong} \quad w'_3 \end{array}$$

ist. Bezeichne  $[u]$  die Äquivalenzklasse von  $u \in F_0(X)$ . Sei

$$F(X) := F_0(X)/(\approx) = \{ [u] : u \in F_0(X) \}$$

die Menge der Äquivalenzklassen auf  $F_0(X)$  bezüglich  $(\approx)$ . Wir haben die Abbildung

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

**Bemerkung 48** *Die Abbildung*

$$\begin{array}{ccc} F(X) \times F(X) & \xrightarrow{(\cdot)} & F(X) \\ ([u] \quad , \quad [v]) & \mapsto & [u] \cdot [v] = [u][v] := [uv] , \end{array}$$

*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  $u, \tilde{u}, v, \tilde{v} \in F_0(X)$ .

Zeigen wir ersteres; zweiteres ist dann analog zu behandeln.

Seien also  $u, \tilde{u}, v \in F_0(X)$  mit  $u \rightsquigarrow \tilde{u}$  gegeben. Dann gibt es  $u', u'' \in F_0(X)$ ,  $x \in X$  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 49 (und Definition)**

*Zusammen mit der Multiplikation von Bemerkung 48 ist  $F(X)$  eine Gruppe, genannt die freie Gruppe auf  $X$ .*

*Hierbei ist  $1 = 1_{F(X)} = [\emptyset]$ . 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  $u, v, w \in F_0(X)$ .

Zum Einselement. Es wird  $[u][\emptyset] = [u\emptyset] = [u]$  für  $u \in F_0(X)$ .

Zum inversen Element. Sei  $u \in F_0(X)$  gegeben. Schreibe  $u = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$  mit  $n \in \mathbf{Z}_{\geq 0}$ ,  $x_i \in X$  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 50 (Universelle Eigenschaft einer freien Gruppe)

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

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

$$\begin{array}{ccc} F(X) & \xrightarrow{\exists! \hat{f}} & G \\ \uparrow \iota & \nearrow f & \\ X & & \end{array}$$

Hierbei ist

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

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

*Beweis.*

*Zur Eindeutigkeit.* Sei  $h : F(X) \rightarrow G$  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 49. Also ist

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

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

*Zur Existenz.* Wir definieren zunächst  $\tilde{f} : F_0(X) \rightarrow G$  durch

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

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

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

Seien  $v, w \in F_0(X)$ ,  $x \in X$  und  $\varepsilon \in \{-1, +1\}$ . Wir haben

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

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

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

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

Bleibt zu verifizieren, daß  $\hat{f}$  ein Gruppomorphismus ist. Seien  $v, w \in F_0(X)$  in der Notation von eben gegeben. Dann wird

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

□

**Notation 51** Für  $x \in X$  schreiben wir unter Mißbrauch von Notation kurz

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

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

### 2.3.2 Endliche Präsentationen via Erzeuger und Relationen

#### Bemerkung 52 (und Definition)

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

$${}^H\langle T \rangle := \bigcap_{T \subseteq N \trianglelefteq H} N \trianglelefteq H.$$

das Normalteilererzeugnis von  $T$  in  $H$ .

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

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

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

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

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

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

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

Zu  $\stackrel{!}{\geq}$ . Es ist  $T \subseteq {}^H\langle T \rangle$ . Da  ${}^H\langle T \rangle \trianglelefteq H$  ist, ist auch  ${}^hT \subseteq {}^H\langle T \rangle$  für  $h \in H$ . Da  ${}^H\langle T \rangle \leq H$  ist, folgt schließlich  $\langle \bigcup_{h \in H} {}^hT \rangle \leq {}^H\langle T \rangle$ .  $\square$

**Notation 53** Seien  $n, m \geq 0$ .

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

Seien  $r_1, \dots, r_m \in F(X)$ .

Schreibe

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

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  $\langle x_1, \dots, x_n : r_1, \dots, r_m \rangle$  unter der Restklassenabbildung von  $F(X)$  nach  $\langle x_1, \dots, x_n : r_1, \dots, r_m \rangle$  gleich 1.

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

$$x_i := x_i {}^{F(X)}\langle \{r_1, \dots, r_m\} \rangle \stackrel{\text{N. 51}}{=} [x_i^{+1}] {}^{F(X)}\langle \{r_1, \dots, r_m\} \rangle.$$

Die beiden Surjektionen

$$\begin{array}{ccccc} F_0(X) & \longrightarrow & F(X) & \longrightarrow & \langle x_1, \dots, x_n : r_1, \dots, r_m \rangle \\ u & \longmapsto & [u] & \longmapsto & [u]^{F(X)} \langle \{r_1, \dots, r_m\} \rangle \end{array}$$

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

### Satz 54 (Universelle Eigenschaft einer endlich präsentierten Gruppe)

Wir befinden uns weiterhin in der Situation von Notation 53.

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

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

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

schickt; cf. Lemma 50.

Sei an  $f$  dazuhin

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

vorausgesetzt.

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

$$\begin{array}{ccc} x_i & & \langle x_1, \dots, x_n : r_1, \dots, r_m \rangle \xrightarrow{\exists! \check{f}} G \\ \uparrow & & \uparrow \\ \bar{x}_i & & X = \{x_1, \dots, x_n\} \xrightarrow{f} G \end{array}$$

*Beweis.*

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

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

wobei  $k \in \mathbf{Z}_{\geq 0}$  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  $\hat{f} : F(X) \rightarrow G$  mit  $\hat{f}(x_i) = f(x_i)$  für  $i \in [1, n]$ ; cf. Lemma 50. Nach Voraussetzung ist  $\hat{f}(r_j) = 1$  für  $j \in [1, m]$ , i.e.  $\{r_1, \dots, r_m\} \subseteq \text{Kern}(\hat{f}) \trianglelefteq F(X)$ . Also ist  ${}^{F(X)}\langle \{r_1, \dots, r_m\} \rangle \leq \text{Kern}(\hat{f})$ .

Somit ist der Gruppenmorphismus

$$\begin{array}{ccc} \langle x_1, \dots, x_n : r_1, \dots, r_m \rangle = F(X) / {}^{F(X)}\langle \{r_1, \dots, r_m\} \rangle & \xrightarrow{\check{f}} & G \\ u \in {}^{F(X)}\langle \{r_1, \dots, r_m\} \rangle & \longmapsto & \hat{f}(u) \end{array}$$

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

**Beispiel 55** Sei  $D_8 := \langle a, b : a^4, b^2, (ba)^2 \rangle$ .

In  $D_8$  ist jedes Element von der Form  $a^{i_1} b^{j_1} \cdots a^{i_\ell} b^{j_\ell}$ , wobei  $\ell \geq 0$  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  $a^i b^j$  mit  $i \in [0, 3]$  und  $j \in [0, 1]$ . Denn in einem Produkt von Elementen  $a$  und  $b$  können wir unter Verwendung von  $ba = a^3b$  die Faktoren  $b$  nach rechts tauschen; e.g. wird  $baabab = a^3babab = a^3a^3bbab = a^21ab = a^3b$ . Insbesondere ist  $|D_8| \leq 8$ . 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

$$\begin{array}{ccc} \{a, b\} & \xrightarrow{f} & S_4 \\ a & \mapsto & (1, 2, 3, 4) \\ b & \mapsto & (1, 3) . \end{array}$$

Betrachten wir  $\hat{f} : F(\{a, b\}) \rightarrow S_4$ , so wird

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

Also gibt Satz 54 den Gruppenmorphismus

$$\begin{array}{ccc} D_8 & \xrightarrow{\tilde{f}} & S_4 \\ a & \mapsto & (1, 2, 3, 4) \\ b & \mapsto & (1, 3) . \end{array}$$

Sein Bild ist die 2-Sylowgruppe  $H := \langle (1, 2, 3, 4), (1, 3) \rangle$  von  $S_4$ , hat also Ordnung 8; cf. Beispiel 33. Insbesondere ist  $|D_8| \geq 8$ .

Zusammengenommen ist also  $|D_8| = 8$ .

Es folgt, daß  $\tilde{f}|^H : D_8 \rightarrow H$  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 präsentierten Gruppe gleich 1 ist, ist allgemein lösbar.

**Beispiel 56** Sei

$$\begin{aligned} \{a, b\} &\xrightarrow{u} D_8 \\ a &\mapsto a \\ b &\mapsto ab. \end{aligned}$$

Betrachten wir  $\hat{u} : F(\{a, b\}) \rightarrow D_8$ , so wird

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

Also gibt Satz 54 den Gruppenmorphismus

$$\begin{aligned} D_8 &\xrightarrow{\tilde{u}} D_8 \\ a &\mapsto a \\ b &\mapsto ab. \end{aligned}$$

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

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

**Beispiel 57** Sei  $n \geq 1$ . Setze

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

Es ist

$$\begin{aligned} S_{P,n} &\xrightarrow{\sim} S_n \\ s_i &\mapsto (i, i+1) \quad \text{für } i \in [1, n-1]. \end{aligned}$$

Dies verifizieren wir in Aufgabe 22.

### 2.3.3 Bahnenalgorithmus für Relationen

**Bemerkung 58** Seien  $F$  und  $G$  Gruppen. Sei  $\varphi : F \rightarrow G$  ein Gruppenmorphismus.

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

$$C_F(1_G) = \text{Kern}(\varphi).$$

*Beweis.* Sei  $f \in F$  gegeben. Es ist  $f \in C_F(1_G)$  genau dann, wenn  $1_G = f \cdot 1_G = \varphi(f) \cdot 1_G = \varphi(f)$  ist, i.e. wenn  $f \in \text{Kern}(\varphi)$  ist.  $\square$

**Algorithmus 59** Sei  $G$  eine endliche Gruppe.

Sei  $n \geq 0$  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 50, über den surjektiven Gruppenmorphismus

$$\begin{aligned} F := F(\{\hat{g}_i : i \in [1, n]\}) &\xrightarrow{\varphi} G \\ \hat{g}_i &\mapsto g_i \quad \text{für } i \in [1, n]. \end{aligned}$$

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

Bestimme mittels Bahnenalgorithmus, Algorithmus 32, ein  $m \geq 0$  und eine endliche Teilmenge  $\{k_j : j \in [1, m]\} \subseteq C_F(1_G) \stackrel{\text{B.58}}{=} \text{Kern}(\varphi)$  mit

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

Dann ist insbesondere

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

Somit erhalten wir den Isomorphismus

$$\begin{aligned} \langle \hat{g}_1, \dots, \hat{g}_n : k_1, \dots, k_m \rangle &\xrightarrow{\tilde{\varphi}} G \\ \hat{g}_i \text{ Kern}(\varphi) &\mapsto g_i \quad \text{für } i \in [1, n]. \end{aligned}$$

Oft kann die in Algorithmus 59 gefundene Liste von Relationen noch mittels folgender Bemerkung 60 reduziert werden.

**Bemerkung 60** 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,  ${}^F\langle X \cup \{y\} \rangle \stackrel{!}{\subseteq} {}^F\langle X \cup \{z\} \rangle$  zu zeigen.

Schreibe  $N := {}^F\langle X \cup \{z\} \rangle \trianglelefteq F$ . Wir haben  $X \cup \{y\} \stackrel{!}{\subseteq} N$  zu zeigen.

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

Es ist  $y = f^{-1} z t f$  für ein  $t \in {}^F\langle X \rangle \trianglelefteq N$ . Da  $z \in N$  liegt, folgt  $z t \in N$  und also  $y \in N$ .  $\square$



**Beispiel 61** Betrachte  $G := \langle (1, 2, 3, 4), (1, 3) \rangle \leq S_4$ .

Wir kennen schon aus Beispiel 55 den Isomorphismus

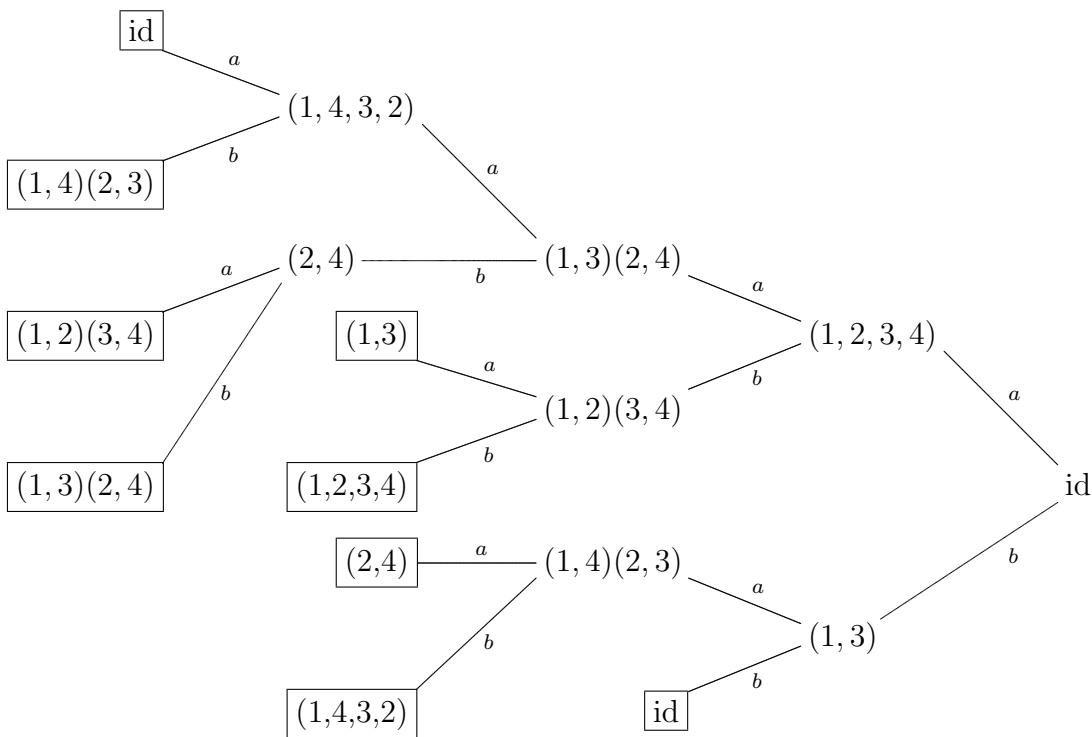
$$D_8 = \langle a, b : a^4, b^2, (ba)^2 \rangle \xrightarrow{\sim} G, \quad a \mapsto (1, 2, 3, 4), \quad b \mapsto (1, 3).$$

Wir wollen diesen abermals herleiten, diesesmal unter Verwendung von Algorithmus 59.

Wir haben den surjektiven Gruppenmorphimus

$$\begin{aligned} F := F(\{a, b\}) &\xrightarrow{\varphi} G \\ a &\mapsto (1, 2, 3, 4) \\ b &\mapsto (1, 3), \end{aligned}$$

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



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

$$b^2, \quad b^{-1}aba, \quad a^{-1}b^2a, \quad (ba^2)^{-1}a^2b, \quad a^{-3}(bab), \quad a^4, \quad (ab)^{-1}ba^3, \quad (ba)^{-1}aba^2, \quad a^{-2}b^2a^2$$

Nun wenden wir Bemerkung 60 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.

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

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.

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

Somit ist in der Tat

$$\begin{aligned} D_8 = \langle a, b : a^4, b^2, (ba)^2 \rangle &\xrightarrow[\sim]{\bar{\varphi}} G \\ a &\mapsto (1, 2, 3, 4) \\ b &\mapsto (1, 3) \end{aligned}$$

# Kapitel 3

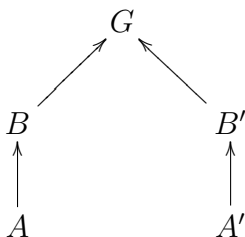
## Erweiterungen

### 3.1 Jordan-Hölder

Sei  $G$  eine Gruppe.

**Lemma 62 (Schmetterlingslemma)**

Sei  $A \trianglelefteq B \leq G$ . Sei  $A' \trianglelefteq B' \leq G$ .



Dann ist

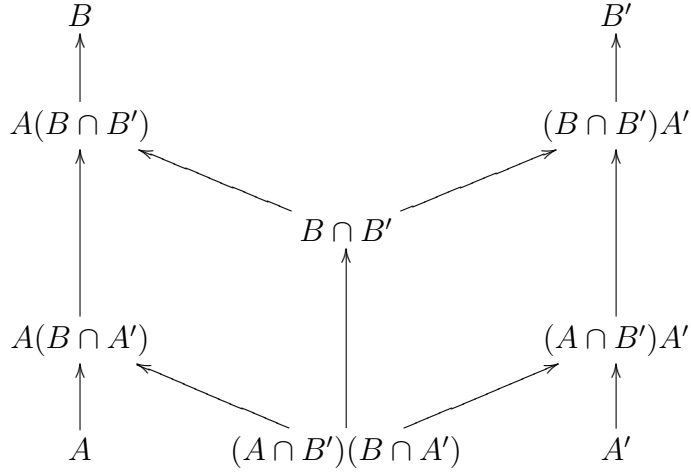
$$\begin{aligned}
 (A \cap B')(B \cap A') &\trianglelefteq B \cap B' \\
 A(B \cap A') &\trianglelefteq A(B \cap B') \\
 (A \cap B')A' &\trianglelefteq (B \cap B')A'.
 \end{aligned}$$

Wir haben die folgenden Isomorphismen.

$$\begin{aligned}
 (B \cap B') / ((A \cap B')(B \cap A')) &\xrightarrow{\varphi} (A(B \cap B')) / (A(B \cap A')) \\
 x((A \cap B')(B \cap A')) &\mapsto x(A(B \cap A')) \\
 (B \cap B') / ((A \cap B')(B \cap A')) &\xrightarrow{\varphi'} ((B \cap B')A') / ((A \cap B')A') \\
 x((A \cap B')(B \cap A')) &\mapsto x((A \cap B')A')
 \end{aligned}$$

Insbesondere ist

$$(A(B \cap B')) / (A(B \cap A')) \simeq ((B \cap B')A') / ((A \cap B')A').$$



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

Wegen  $A \trianglelefteq B$  und  $B \cap A' \trianglelefteq B \cap B' \leq B$  ist  $A(B \cap A') \leq A(B \cap B') \leq B$ ; 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  $A \trianglelefteq B$  und da  $z := {}^yx \in B \cap A'$  und mithin  ${}^{ay}x = aza^{-1} = a({}^za)^{-1}z \in A(B \cap A')$  wegen  $A \trianglelefteq B$ .

Es genügt, den Isomorphismus  $\varphi$  zu zeigen.

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

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

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  $y(A(B \cap A')) = xa(A(B \cap A')) = x(A(B \cap A'))$ .  $\square$

**Definition 63** Eine *Subnormalreihe* von  $G$  ist ein Tupel von Untergruppen  $(U_i)_{i \in [0, s]}$  von  $G$  für ein  $s \geq 0$ , für welches  $G = U_0$  und  $U_i \triangleright U_{i+1}$  für  $i \in [0, s-1]$  und  $U_s = 1$  gilt.

$$G = U_0 \triangleright U_1 \triangleright \dots \triangleright U_{s-1} \triangleright U_s = 1$$

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

**Definition 64** 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  $\rho : [0, s] \rightarrow [0, t]$  gibt mit  $\rho(0) = 0$ ,  $\rho(s) = t$  und  $U_i = V_{\rho(i)}$  für  $i \in [0, s]$ . Sei  $(\prec) := (\preccurlyeq) \setminus (=)$ .
- (4) Die Subnormalreihen  $(U_i)_{i \in [0,s]}$  und  $(V_j)_{j \in [0,t]}$  heißen *äquivalent*, wenn es eine bijektive Abbildung  $\sigma : [0, s - 1] \rightarrow [0, t - 1]$  gibt mit

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

für  $i \in [0, s - 1]$ .

- (5) Sei  $\alpha : [0, \check{s}] \rightarrow [0, s]$  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 65

- (1) Es ist  $(S_3, A_3, 1)$  eine Kompositionsreihe von  $S_3$ .
- (2) Betrachte  $D_8 = \langle a, b : a^4, b^2, (ba)^2 \rangle$ ; cf. Beispiel 55. Es sind  $(D_8, \langle a \rangle, \langle a^2 \rangle, 1)$  und  $(D_8, \langle a^2, b \rangle, \langle a^2 \rangle, 1)$  Kompositionsreihen von  $D_8$ . Beachte  $\langle a \rangle \not\preccurlyeq \langle a^2, b \rangle$ .
- (3) Es ist

$$(S_4, A_4, \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle, \langle (1, 2)(3, 4) \rangle, 1)$$

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

$$(S_4, \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle, 1)$$

- (4) Sei  $n \geq 5$ . Es ist  $(S_n, A_n, 1)$  eine Kompositionsreihe von  $S_n$ . Cf. Satz 46.
- (5) Es ist

$$(GL_3(\mathbf{F}_7), \langle SL_3(\mathbf{F}_7), \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rangle, SL_3(\mathbf{F}_7), \langle \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix} \rangle)$$

eine Kompositionsreihe von  $GL_3(\mathbf{F}_7)$ ; cf. Satz 47. Darin treten, bis auf Isomorphie, die Kompositionsfaktoren  $C_3, C_2, PSL_3(\mathbf{F}_7), C_3$  auf.

**Bemerkung 66** 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  $(\preceq)$  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  $1 < N/U_{i+1} \triangleleft U_i/U_{i+1}$ , wobei  $U_{i+1} \triangleleft N \triangleleft U_i$ ; 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  $\rho : [0, s] \rightarrow [0, s + 1]$ ,  $k \mapsto k + \partial_{k \geq i+1}$  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  $\rho : [0, s] \rightarrow [0, t]$ . Diese ist nicht surjektiv, da sie diesenfalls gleich  $\text{id}_{[0, s]}$  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  $\rho$ . 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  $1 \neq V_i/U_{i+1} \triangleleft U_i/U_{i+1}$ , somit  $U_i/U_{i+1}$  nicht einfach, und wir haben einen *Widerspruch*.  $\square$

**Beispiel 67** 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 68** 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  $\alpha : [0, \check{s} - 1] \rightarrow [0, s - 1]$  injektiv, monoton und mit Bild  $\{i \in [0, s - 1] : U_i > U_{i+1}\}$ .

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

Sei  $\sigma : [0, s - 1] \rightarrow [0, t - 1]$  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  $\sigma$  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  $\beta \circ \check{\sigma} = \sigma \circ \alpha$ .

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

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

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

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

**Bemerkung 69** 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  $\rho$  monoton und injektiv.  $\square$

**Lemma 70 (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

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

Ist  $k \equiv_t -1$ , dann ist

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

Dies zeigt die *Behauptung*.

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

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

cf. Lemma 62. 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

$$\begin{aligned}
U'_k/U'_{k+1} &\stackrel{\text{Beh.}}{=} (U_{\varphi_1(k)+1}(U_{\varphi_1(k)} \cap V_{\varphi_2(k)})) / (U_{\varphi_1(k)+1}(U_{\varphi_1(k)} \cap V_{\varphi_2(k)+1})) \\
&\stackrel{\text{L. 62}}{\simeq} ((U_{\varphi_1(k)} \cap V_{\varphi_2(k)})V_{\varphi_2(k)+1}) / ((U_{\varphi_1(k)+1} \cap V_{\varphi_2(k)})V_{\varphi_2(k)+1}) \\
&= ((V_{\varphi_2(k)} \cap U_{\varphi_1(k)})V_{\varphi_2(k)+1}) / ((V_{\varphi_2(k)} \cap U_{\varphi_1(k)+1})V_{\varphi_2(k)+1}) \\
&\stackrel{\text{Beh.}}{=} ((V_{\psi_1(\sigma(k))} \cap U_{\psi_2(\sigma(k))})V_{\psi_1(\sigma(k))+1}) / ((V_{\psi_1(\sigma(k))} \cap U_{\psi_2(\sigma(k))+1})V_{\psi_1(\sigma(k))+1})) \\
&= V'_{\sigma(k)} / V'_{\sigma(k)+1}.
\end{aligned}$$

*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 68.

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 69.

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

**Satz 71 (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 64.*

*Sei daran erinnert, daß, falls  $G$  endlich ist, eine Kompositionsreihe von  $G$  existiert; cf. Beispiel 67.*

*Beweis.* Gemäß Lemma 70 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 66. 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 72

- (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  $U_i \triangleleft G$  für  $i \in [0, s]$  und  $U_i/U_{i+1} \leq Z(G/U_{i+1})$  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 73

- (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 66, Beispiel 67. 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 66, Beispiel 67. 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  $p$ . 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 74

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

(2) Ist  $G > 1$  und  $G$  nilpotent, so ist  $Z(G) > 1$ .

*Beweis.*

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

Sei  $|G| > 1$ . Dann ist  $Z(G) \neq 1$ ; cf. Aufgabe 31.(1). Nach Induktion ist  $G/Z(G)$  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  $s \geq 1$ . Es ist  $U_{s-1} > U_s = 1$  und  $U_{s-1}/U_s \leq Z(G/U_s)$ , also  $U_{s-1} \leq Z(G)$ .  $\square$

**Bemerkung 75** Wir haben die Implikationen

$G$  abelsch  $\Rightarrow G$  nilpotent  $\Rightarrow G$  überauflösbar  $\Rightarrow G$  auflösbar  $\Rightarrow G$   $p$ -auflösbar für  $p > 0$  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  $U_{i-1}/U_i \leq Z(G/U_i)$  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 73.(1) jeder Kompositionsfaktor von  $G$  zyklisch von Primordnung, dank Bemerkung 73.(2) also  $G$  auch  $p$ -auflösbar für  $p > 0$  prim.  $\square$

**Beispiel 76**

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

Es ist  $S_3$  überauflösbar, da  $S_3/A_3 \simeq C_2$  und  $A_3 \simeq C_3$ .

Es ist  $S_3$  nicht nilpotent, da  $Z(S_3) = \{\text{id}\}$  ist; cf. Aufgabe 20.(2), Bemerkung 74.(2). Beachte, daß nichtsdestoweniger  $S_3/A_3$  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  $A_4(a, b, c) \sqcup A_4(b, c, d)$  enthält.

Insbesondere ist  $(A_4, V, 1)$  eine Subnormalreihe von  $A_4$ .

Es ist  $A_4$  auflösbar, da  $A_4/V \simeq C_3$  und  $V \simeq C_2 \times C_2$ ; 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  $n \geq 5$ . Es hat  $S_n$  die Kompositionsreihe  $(S_n, A_n, 1)$ ; cf. Satz 46. Somit hat  $S_n$  die Kompositionsfaktoren  $C_2$  und  $A_n$ , die nicht beide zyklisch von Primzahlordnung sind, da  $|A_n| \equiv_{60} 0$ . Folglich ist  $S_n$  nicht auflösbar; cf. Bemerkung 73.(1).

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

Sei  $n \geq 2$ . Sei  $(n, p^\alpha) \notin \{(2, 2), (2, 3)\}$ . Es hat  $\text{GL}_n(K)$  die Subnormalreihe  $(\text{GL}_n(K), \text{SL}_n(K), \text{Z}(\text{SL}_n(K)), 1)$ . Da diese zu einer Kompositionsreihe verfeinerbar ist, hat  $\text{GL}_n(K)$  den Kompositionsfaktor  $\text{PSL}_n(K)$ ; cf. Satz 47. Es ist

$$|\text{PSL}_n(K)| = (q^n - q^0)(q^n - q^1) \cdots (q^n - q^{n-1}) \cdot (q - 1)^{-1} \cdot |\text{Z}(\text{SL}_n(K))|^{-1}.$$

Da  $\text{Z}(\text{SL}_n(K)) \simeq \{x \in \text{U}(K) : x^n = 1\} \leq \text{U}(K)$  ist, ist  $|\text{Z}(\text{SL}_n(K))|$  ein Teiler von  $q - 1$ . Folglich ist  $|\text{PSL}_n(K)|$  teilbar durch  $(q + 1)q$  und also nicht prim. Somit ist  $\text{GL}_n(K)$  nicht auflösbar; cf. Bemerkung 73.(1).

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

Sei  $n \geq 1$ . Sei

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

die Untergruppe der oberen Dreiecksmatrizen. Sei

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

darin die Untergruppe der unipotenten oberen Dreiecksmatrizen.

Es ist  $U$  der Kern des surjektiven Gruppenmorphismus

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

Da  $|U| = p^{\alpha n(n-1)/2}$ , ist  $U$  nilpotent, folglich auflösbar; cf. Bemerkungen 74.(1) und 75. Es ist  $\text{U}(K)^{\times n}$  abelsch, folglich auflösbar. Also ist  $B$  auflösbar; cf. Aufgabe 32.(1).

**Definition 77** Sei  $U \leq G$ .

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

Wir schreiben  $U \triangleleft G$  für  $(U \triangleleft G \text{ und } U < G)$ .

Hierfür genügt es, wenn  $\alpha(U) \leq U$  ist für  $\alpha \in \text{Aut}(G)$ . Denn daraus folgt  $U \leq \alpha^{-1}(U)$  für  $\alpha \in \text{Aut}(G)$ . Oder aber man verwendet die vorausgesetzte Endlichkeit von  $G$ .

**Beispiel 78** Sei  $V := \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle \trianglelefteq S_4$ ; cf. Beispiel 65. Es ist  $V \simeq C_2 \times C_2$ ; 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  $\alpha \in \text{Aut}(V)$ . Sei  $U := \langle (1, 3)(2, 4) \rangle \leq V$ . Es ist

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

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

### Bemerkung 79

- (1) Sei  $U \leq G$ . Da genau dann  $U \trianglelefteq G$  ist, wenn  $\alpha(U) = U$  ist für alle  $\alpha \in \text{Inn}(G)$ , haben wir die Implikation  $U \trianglelefteq G \Rightarrow U \trianglelefteq G$ ; cf. Aufgabe 23.
- (2) Ist  $U \trianglelefteq V \trianglelefteq G$ , dann ist  $U \trianglelefteq G$ . Denn für  $g \in G$  ist  $\alpha : V \rightarrow V, x \mapsto {}^g x$  in  $\text{Aut}(V)$ , sodaß  ${}^g U = \alpha(U) = U$  folgt.
- (3) Ist  $U \trianglelefteq V \trianglelefteq G$ , dann ist  $U \trianglelefteq G$ . Denn für  $\beta \in \text{Aut}(G)$  ist  $\alpha := \beta|_V^V \in \text{Aut}(V)$ , sodaß  $\beta(U) = \alpha(U) = U$  folgt.
- (4) Es ist  $Z(G) \trianglelefteq G$ . Denn für  $\alpha \in \text{Aut}(G)$  ist  $\alpha(Z(G)) \leq Z(G)$ ; cf. Aufgabe 34.(3).
- (5) Sind  $U, V \trianglelefteq G$ , dann ist  $[U, V] \trianglelefteq G$ . Denn für  $\alpha \in \text{Aut}(G)$  ist  $\alpha([U, V]) = [\alpha(U), \alpha(V)] = [U, V]$ ; cf. Aufgabe 34.(1).
- (6) Ist  $U \trianglelefteq G$  und  $U \leq V \leq G$  mit  $V/U \trianglelefteq G/U$  gegeben, dann ist  $V \trianglelefteq G$ . Denn für  $\alpha \in \text{Aut}(G)$  ist  $\bar{\alpha} : G/U \rightarrow G/U, gU \mapsto \bar{\alpha}(gU) := \alpha(g)U$  wegen  $\alpha(U) = U$  wohldefiniert und also in  $\text{Aut}(G/U)$  enthalten. Wegen  $V/U \trianglelefteq G/U$  ist  $\alpha(V)/U = \bar{\alpha}(V/U) = V/U$  und also  $\alpha(V) = V$ .
- (7) Ist  $p > 0$  prim und ist  $\text{Syl}_p(G) = \{P\}$ , dann ist  $P \trianglelefteq G$ , denn für  $\alpha \in \text{Aut}(G)$  ist  $|\alpha(P)| = |P| = |G|/p$ , also  $\alpha(P) \in \text{Syl}_p(G) = \{P\}$ , also  $\alpha(P) = P$ .

### Definition 80

- (1) Setze rekursiv  $G^{(0)} := G$  und  $G^{(i+1)} := (G^{(i)})^{(1)} = [G^{(i)}, G^{(i)}]$  für  $i \geq 0$ . Cf. auch Aufgabe 13.
- (2) Setze rekursiv  $G^{[0]} := G$  und  $G^{[i+1]} := [G^{[i]}, G]$  für  $i \geq 0$ .
- (3) Setze  $G^{[0]1} := 1$ . Definiere rekursiv  $G^{[i+1]1} \leq G$  durch  $G^{[i+1]1}/G^{[i]1} := Z(G/G^{[i]1})$  für  $i \geq 0$ ; cf. Aufgabe 17.(3).

### Bemerkung 81

- (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  $G^{[1]1} = Z(G)$ .

- (2) Es ist  $G^{(i)} \triangleleft G$  und  $G^{[i]} \triangleleft G$  und  $G^{[i]} \triangleleft G$  für  $i \geq 0$ .
- (3) Es ist  $G^{(i)} \leq G^{[i]}$  für  $i \geq 0$ .
- (4) Sei  $i \geq 0$ . Sei  $x \in G$ . Es ist  $x \in G^{[i+1]}$  genau dann, wenn  $xG^{[i]} \in Z(G/G^{[i]})$ , i.e. wenn  $[x, G] \subseteq G^{[i]}$  ist.
- (5) Es ist  $(G/Z(G))^{[i]} = G^{[i+1]}/Z(G)$  für  $i \geq 0$ .
- (6) Seien  $i, j \geq 0$ . Genau dann ist  $G^{[i]} \leq G^{[j+1]}$ , wenn  $G^{[i+1]} \leq G^{[j]}$  ist.

*Beweis.*

*Ad (2).* Es folgen  $G^{(i)} \triangleleft G$  und  $G^{[i]} \triangleleft G$  für  $i \geq 0$  aus iterierter Anwendung von Bemerkung 79.(5).

Es folgt  $G^{[i]} \triangleleft G$  für  $i \geq 0$  aus iterierter Anwendung von Bemerkung 79.(4) unter Verwendung von Bemerkung 79.(6).

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

*Ad (5).* Schreibe  $Z := Z(G)$ . Induktion über  $i \geq 0$ . Für  $i = 0$  ist  $(G/Z)^{[0]} = Z/Z = G^{[1]}/Z$ . Sei die Gleichung für ein  $i \geq 0$  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  $G^{[i]} \leq G^{[j+1]}$  genau dann, wenn  $G^{[i+1]} = [G^{[i]}, G] \leq G^{[j]}$  ist.  $\square$

**Beispiel 82** Sei  $B = \left\{ \begin{pmatrix} a & b \\ u & c \end{pmatrix} \in \text{GL}_2(\mathbf{F}_3) : u = 0 \right\} \leq \text{GL}_2(\mathbf{F}_3)$ ; cf. Beispiel 76.(5). Kurz,  $B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ .

Damit  $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in Z(B)$  liegt, muß  $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$  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  $B^{[1]} = Z(B) = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$ .

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

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

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

**Satz 83 (Kommutatorreihe)** Weiterhin ist  $G$  eine endliche Gruppe.

Die Aussagen (1,2) sind äquivalent.

- (1) *Es ist  $G$  auflösbar.*  
 (2) *Es gibt ein  $i \geq 0$  mit  $G^{(i)} = 1$ .*

Diesenfalls sei  $m := \min\{i \geq 0 : G^{(i)} = 1\}$ ; 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  $G^{(i)} \stackrel{!}{\leq} U_i$  für  $i \in [0, s]$ . Induktion über  $i \in [0, s]$ . Es ist  $G^{(0)} = G = U_0$ . Sei nun  $G^{(i)} \leq U_i$  für ein  $i \in [0, s-1]$ . Es ist  $U_i/U_{i+1}$  abelsch. Also ist  $[x, y]U_{i+1} = [xU_{i+1}, yU_{i+1}] = 1U_{i+1}$  für  $x, y \in U_i$ . Es folgt  $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [U_i, U_i] \leq U_{i+1}$ . Dies zeigt die Behauptung. Für  $i = s$  liefert diese  $G^{(s)} \leq U_s = 1$ , i.e.  $G^{(s)} = 1$ .

*Ad (2)  $\Rightarrow$  (1).* Es ist  $G^{(i+1)} \triangleleft G$ , also  $G^{(i+1)} \trianglelefteq G^{(i)}$  für  $i \geq 0$ ; cf. Bemerkung 81.(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  $G$ .  $\square$

**Bemerkung 84** Sei  $G$  auflösbar.

Es ist in der Kommutatorreihe  $(G^{(i)})_{i \in [0, m]}$  zwar  $G^{(i)} \trianglelefteq G$  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 76.(2).

**Satz 85 (Zentralreihen)** *Weiterhin ist  $G$  eine endliche Gruppe.*

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

- (1) *Es ist  $G$  nilpotent.*  
 (2) *Es gibt ein  $i \geq 0$  mit  $G^{[i]} = 1$ .*  
 (3) *Es gibt ein  $j \geq 0$  mit  $G^{[j]} = G$ .*

*Sei  $G$  nilpotent. Dann ist*

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

*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  $G^{[i]} \leq G^{[u-i]}$  für  $i \in [0, u]$ .*

*Beweis.* Schreibe  $Z := Z(G)$ .

*Ad (1)  $\Rightarrow$  (3).* Induktion über  $|G|$ . Sei  $|G| > 1$ . Es ist  $Z > 1$ , also  $|G/Z| < |G|$ ; cf. Bemerkung 74.(2). Es ist auch  $G/Z$  nilpotent; cf. Aufgabe 32.(7). Mit Induktion gibt es ein  $j' \geq 0$  mit  $(G/Z)^{j'l} = G/Z$ . Dank Bemerkung 81.(5) ist  $(G/Z)^{j'l} = G^{j'+1l}/Z$ . Insgesamt folgt  $G = G^{j'+1l}$ .

*Ad (3)  $\Rightarrow$  (1).* Induktion über  $|G|$ . Sei  $|G| > 1$ . Sei  $t \geq 0$  minimal mit  $G^{tl} = G$  gegeben. Es ist  $t \geq 1$ . Es ist  $G^{1l} = Z > 1$ . Es ist  $(G/Z)^{t-1l} = G^{t-1l}/Z = G/Z$  dank Bemerkung 81.(5). Mit Induktion ist  $G/Z$  nilpotent. Also ist  $G$  nilpotent; cf. Aufgabe 32.(6).

*Ad (2)  $\Rightarrow$  (3).* Sei  $s$  minimal mit  $G^{sl} = 1$ . Wir behaupten  $G^{[s-j]l} \stackrel{!}{\leq} G^{jl}$  für  $j \in [0, s]$ . Induktion über  $j \in [0, s]$ . Aus  $G^{[s-j]l} \leq G^{jl}$  folgt  $G^{[s-j-1]l} \leq G^{j+1l}$ , sofern  $j \in [0, s-1]$ ; cf. Bemerkung 81.(6). Dies zeigt die *Behauptung*. Für  $j = s$  folgt  $G = G^{[0]l} \leq G^{sl} \leq G$ , also  $G^{sl} = G$ . Insbesondere ist dann  $\min\{i \geq 0 : G^{il} = 1\} = s \geq \min\{j \geq 0 : G^{jl} = G\}$ .

*Ad (3)  $\Rightarrow$  (2).* Sei  $t$  minimal mit  $G^{tl} = G$ . Wir behaupten  $G^{[t-i]l} \stackrel{!}{\geq} G^{il}$  für  $i \in [0, t]$ . Induktion über  $i \in [0, t]$ . Aus  $G^{[t-i]l} \geq G^{il}$  folgt  $G^{[t-i-1]l} \geq G^{i+1l}$ , sofern  $i \in [0, t-1]$ ; cf. Bemerkung 81.(6). Dies zeigt die *Behauptung*. Für  $i = t$  folgt  $1 = G^{[0]l} \geq G^{tl} \geq 1$ , also  $G^{tl} = 1$ . Insbesondere ist dann  $\min\{j \geq 0 : G^{jl} = G\} = t \geq \min\{i \geq 0 : G^{il} = 1\}$ .

Falls  $G$  nilpotent ist, so zeigt dies auch

$$\underbrace{\min\{i \geq 0 : G^{il} = 1\}}_{=s} = \underbrace{\min\{j \geq 0 : G^{jl} = G\}}_{=t} =: u$$

und  $G^{il} \leq G^{[u-i]l}$  für  $i \in [0, u]$ . □

**Beispiel 86 (Fortsetzung)** Im Lichte von Satz 85 wurde in Beispiel 82 gezeigt, daß die dortige Gruppe  $B$  nicht nilpotent ist, da  $B^{jl} < B$  für alle  $j \geq 0$ .

**Lemma 87** Sei  $p$  eine Primzahl. Sei  $N \trianglelefteq G$ .

(1) Wir haben die surjektive Abbildung

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

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

*Beweis.*

*Ad (1).* Sei  $P \in \text{Syl}_p(N)$ ; cf. Satz 37.(1). Sei  $\tilde{Q} \in \text{Syl}_p(G)$  mit  $P \leq \tilde{Q}$ ; cf. Satz 37.(4).

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



Sei  $x \in G$  mit  ${}^xQ = \tilde{Q}$ ; cf. Satz 37.(2). Es ist  ${}^{xN}((QN)/N) = (xN)((QN)/N)(xN)^{-1} = (x(QN)x^{-1})/N = {}^x(QN)/N = ({}^xQ {}^xN)/N = (\tilde{Q}N)/N$ . Somit können wir uns darauf beschränken,  $(\tilde{Q}N)/N \stackrel{!}{\in} \text{Syl}_p(G/N)$  zu zeigen.

Wegen  $\tilde{Q} \cap N \leq \tilde{Q}$  ist  $\tilde{Q} \cap N$  eine  $p$ -Gruppe. Wegen  $P \leq \tilde{Q} \cap N \leq N$  und wegen  $P \in \text{Syl}_p(N)$  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  $(\tilde{Q}N)/N \in \text{Syl}_p(G/N)$ .

Zeigen wir die Surjektivität von  $\rho_{G,N}$ . Sei  $K/N \in \text{Syl}_p(G/N)$ , wobei  $N \leq K \leq G$ ; cf. Aufgabe 17.(1). Da auch  $(\tilde{Q}N)/N \in \text{Syl}_p(G/N)$  ist, gibt es ein  $y \in G$  mit  $K/N = {}^{yN}((\tilde{Q}N)/N) = ({}^y\tilde{Q}N)/N$ ; cf. Satz 37.(2). Da auch  ${}^y\tilde{Q} \in \text{Syl}_p(G)$  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  $Q, Q' \in \text{Syl}_p(G)$  mit  $QN/N = Q'N/N$  gegeben. Zu zeigen ist  $Q \stackrel{!}{=} Q'$ . Es ist  $QN = Q'N$ . Wegen  $Q, Q' \leq QN \leq G$  sind auch  $Q, Q' \in \text{Syl}_p(QN)$ . Folglich gibt es  $q \in Q$  und  $n \in N$  mit  ${}^{qn}Q = Q'$ ; cf. Satz 37.(2). Wegen  $N \leq Z(G)$  ist aber  ${}^{qn}Q = {}^qQ = Q$ . Also ist  $Q' = Q$ .  $\square$

### Satz 88 (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  $Q_i \in \text{Syl}_{p_i}(G)$ ; cf. Satz 37.(1).*

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

- (1) *Es ist  $G$  nilpotent.*
- (2) *Es ist  $|\text{Syl}_p(G)| = 1$  für  $p \in \pi(G)$ .*
- (3) *Wir haben den Gruppenisomorphismus  $\prod_{i \in [1, \ell]} Q_i \xrightarrow{\sim} G$ ,  $(q_i)_i \mapsto q_1 \cdot q_2 \cdots q_\ell$ .*
- (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 74.(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  $U_j \triangleleft G$  für  $j \in [0, s]$  und sei  $U_j/U_{j+1} \leq Z(G/U_{j+1})$  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  $U_j/U_{j+1} \leq Z(G/U_{j+1})$  ist und da  $(G/U_{j+1})/(U_j/U_{j+1}) \simeq G/U_j$  ist, folgt dies mit Lemma 87.(2).

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

*Ad (2)  $\Rightarrow$  (3).* Nun ist  $\text{Syl}_{p_i}(G) = \{Q_i\}$  und also  $Q_i \trianglelefteq G$  für  $i \in [1, \ell]$ ; cf. Satz 37.(2).

Wir *behaupten*, es ist  $|Q_1 Q_2 \cdots Q_i| = |Q_1| |Q_2| \cdots |Q_i|$  und  $(Q_1 \cdots Q_{i-1}) \cap Q_i = 1$  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  $|Q_1 \cdots Q_i| = |Q_1| \cdots |Q_i|$  bekannt. Zunächst sind  $|Q_1 \cdots Q_i| = |Q_1| \cdots |Q_i|$  und  $|Q_{i+1}|$  teilerfremd, woraus wir  $(Q_1 \cdots Q_i) \cap Q_{i+1} = 1$  ersehen. Weiter folgt

$$|Q_1 \cdots Q_i Q_{i+1}| \stackrel{\text{A. 12.(1)}}{=} \frac{|Q_1 \cdots Q_i| |Q_{i+1}|}{|(Q_1 \cdots Q_i) \cap Q_{i+1}|} = |Q_1 \cdots Q_i| |Q_{i+1}| = |Q_1| \cdots |Q_i| |Q_{i+1}|.$$

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

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

Schließlich ist

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

Also ist  $f$  ein Gruppenisomorphismus.

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

### 3.3 Semidirekte Produkte

**Definition 89** Sei  $H$  eine Gruppe. Sei  $N$  eine Gruppe. Sei  $\alpha : H \rightarrow \text{Aut}(N)$  ein Gruppenmorphismus. Schreibe auch  $(\alpha(h))(n) =: {}^h n$  für  $h \in H$  und  $n \in N$ . Beachte  ${}^h(nn') = {}^h n {}^h n'$  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

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

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

Da dann

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

und

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

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  $(\cdot, \alpha)$  dank Aufgabe 1 zu einer Gruppe, genannt (*äußeres*) *semidirektes Produkt* von  $N$  mit  $H$  mittels  $\alpha$  und geschrieben

$$N \rtimes_{\alpha} H .$$

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

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

$$\begin{array}{ccccc} N & \xrightarrow{\iota} & N \rtimes_{\alpha} H & \xrightarrow{\rho} & H \\ n & \mapsto & (n, 1) & & \\ & & (n, h) & \mapsto & h . \end{array}$$

Wir haben den Gruppenmorphismus  $\sigma : H \rightarrow N \rtimes_{\alpha} H$ ,  $h \mapsto (1, h)$ . Es ist  $\rho \circ \sigma = \text{id}_H$ .

**Bemerkung 90** Seien  $H$  und  $N$  Gruppen. Es ist  $N \rtimes_{\downarrow} H = N \times H$ . In diesem Sinne verallgemeinert das semidirekte Produkt das direkte Produkt; cf. Aufgabe 2.(1).

### Lemma 91 (Universelle Eigenschaft des semidirekten Produktes)

Sei  $H$  eine Gruppe. Sei  $N$  eine Gruppe. Sei  $\alpha : H \rightarrow \text{Aut}(N)$  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 89 angemerkt.

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

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

$$\begin{array}{ccccc} N & \xrightarrow{\iota} & N \rtimes_{\alpha} H & \xleftarrow{\sigma} & H \\ & \searrow u & \downarrow f & \swarrow v & \\ & & T & & \end{array}$$

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

*Beweis.*

*Eindeutigkeit.* Sei  $\tilde{f} : N \rtimes_{\alpha} H \rightarrow T$  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  $(n, h), (\tilde{n}, \tilde{h}) \in N \rtimes_{\alpha} H$ . Dann ist

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

□

**Lemma 92** Sei  $G$  eine Gruppe. Sei  $N \trianglelefteq G$ . Sei  $H \leq G$ .

Setze  $\alpha : H \rightarrow \text{Aut}(N)$ ,  $h \mapsto (n \mapsto {}^hn = hnh^{-1})$ . Es ist  $\alpha$  ein Gruppenmorphismus.

Wir haben den Gruppenmorphismus

$$\begin{array}{ccc} N \rtimes_{\alpha} H & \xrightarrow{\varphi} & G \\ (n, h) & \mapsto & nh \end{array}$$

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

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

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

*Beweis.* Es ist  $\alpha$  wohldefiniert, denn für  $h \in H$  ist die Abbildung  $N \rightarrow N$ ,  $n \mapsto hnh^{-1}$  in der Tat ein Automorphismus von  $N$ . Es ist  $\alpha$  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  $\varphi$  folgt mit Lemma 91, angewandt auf die beiden Inklusionsabbildungen  $N \hookrightarrow G$  und  $H \hookrightarrow G$ .

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

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

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

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

Cf. Aufgabe 2.(4).

**Bemerkung 93** Sei  $G$  eine Gruppe.

Sei  $N \triangleleft G$ . 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  $\psi : H \xrightarrow{\sim} G/N$ ,  $h \mapsto hN$ .

*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  $\psi$  ein Gruppenmorphismus. Es ist  $\psi$  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  $\psi$  injektiv, da  $\text{Kern}(\psi) = H \cap N = 1$  ist.  $\square$

**Beispiel 94**

- (1) Es hat  $\langle (1, 2, 3) \rangle \triangleleft S_3$  das Komplement  $\langle (1, 2) \rangle$ . So ist  $S_3$  isomorph zum semidirekten Produkt  $\langle (1, 2, 3) \rangle \rtimes_{\alpha} \langle (1, 2) \rangle$ , wobei  $\alpha : \langle (1, 2) \rangle \rightarrow \text{Aut}(\langle (1, 2, 3) \rangle)$ ,  $(1, 2) \mapsto ((1, 2, 3)^i \mapsto {}^{(1,2)}(1, 2, 3)^i = (1, 2, 3)^{-i})$ , wobei  $i \in [0, 2]$ .

Schreiben wir  $C_3 = \langle a : a^3 \rangle$  und  $C_2 = \langle b : b^2 \rangle$ , so wird mit  $\beta : C_2 \rightarrow \text{Aut}(C_3)$ ,  $a \mapsto (b \mapsto b^{-1})$  auch

$$\begin{aligned} C_3 \rtimes_{\beta} C_2 &\xrightarrow{\sim} S_3 \\ (a^i, b^j) &\mapsto (1, 2, 3)^i \circ (1, 2)^j, \quad \text{wobei } i \in [0, 2] \text{ und } j \in [0, 1]. \end{aligned}$$

Kurz,  $S_3 \simeq C_3 \rtimes C_2$ .

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  $V := \overbrace{\langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle}^{=: a} \triangleleft A_4$  das Komplement  $\overbrace{\langle (1, 2, 3) \rangle}^{=: c}$ . So ist  $A_4$  isomorph zu  $V \rtimes_{\alpha} \langle c \rangle$ , wobei  $\alpha : \langle c \rangle \rightarrow \text{Aut}(V)$ ,  $c \mapsto (a \mapsto {}^c a = ab, b \mapsto {}^c b = a)$ .

Kurz,  $A_4 \simeq (C_2 \times C_2) \rtimes C_3$ .

- (3) Es hat  $V := \langle \overbrace{(1, 2)(3, 4)}{=: a}, \overbrace{(1, 3)(2, 4)}{=: b} \rangle \trianglelefteq S_4$  das Komplement  $S_3 = \langle \overbrace{(1, 2, 3)}{=: c}, \overbrace{(1, 2)}{=: d} \rangle$ , denn  $V \cap S_3 = 1$  und  $|V||S_3| = |S_4|$ , woraus  $|VS_3| = |V||S_3|/|V \cap S_3| = |S_4|$  und also  $VS_3 = S_4$  folgt. So ist  $S_4$  isomorph zu  $V \rtimes_{\alpha} S_3$ , wobei  $\alpha : S_3 \rightarrow \text{Aut}(V)$ ,  $c \mapsto (a \mapsto {}^c a = ab, b \mapsto {}^c b = a)$ ,  $d \mapsto (a \mapsto {}^d a = a, b \mapsto {}^d b = ab)$ .

Kurz,  $S_4 \simeq V \rtimes S_3 \stackrel{(1)}{\simeq} (C_2 \times C_2) \rtimes (C_3 \rtimes C_2)$ .

- (4) Betrachte  $D_8 = \langle a, b : a^4, b^2, (ab)^2 \rangle$ ; cf. Beispiel 55. Es hat  $\langle a \rangle \trianglelefteq D_8$  das Komplement  $\langle b \rangle$ . So ist  $D_8$  isomorph zu  $\langle a \rangle \rtimes_{\alpha} \langle b \rangle$ , wobei  $\alpha : \langle b \rangle \rightarrow \text{Aut}(\langle a \rangle)$ ,  $b \mapsto (a \mapsto {}^b a = a^{-1})$ .

Kurz,  $D_8 \simeq C_4 \rtimes C_2$ .

- (5) Schreibe  $C_7 = \langle c : c^7 \rangle$  und  $C_3 = \langle x : x^3 \rangle$ . Es ist

$$\begin{aligned} \text{Aut}(C_7) = \{ \alpha_i : c \mapsto c^i : i \in [1, 6] \} &\simeq \text{U}(\mathbf{Z}/7\mathbf{Z}) = \langle 3 + 7\mathbf{Z} \rangle \simeq C_6 \\ \alpha_i &\mapsto i + 7\mathbf{Z}. \end{aligned}$$

Also ist  $\text{Aut}(C_7) = \langle \alpha_3 \rangle$  zyklisch von Ordnung 6.

Es ist  $\beta : C_3 \rightarrow \text{Aut}(C_7)$ ,  $x \mapsto \alpha_3^2 = \alpha_2$  ein Gruppenmorphismus. Wir können das semidirekte Produkt  $G := C_7 \rtimes_{\beta} C_3$  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  $i, k, j, \ell \in \mathbf{Z}_{\geq 0}$ .

- (6) Schreibe  $C_4 = \langle a : a^4 \rangle$ . Die Untergruppen von  $C_4$  sind 1,  $\langle a^2 \rangle$  und  $C_4$ .

Es hat  $\langle a^2 \rangle \trianglelefteq C_4$  kein Komplement.

**Lemma 95** Sei  $N \xrightarrow{i} G \xrightarrow{r} H$  eine kurz exakte Sequenz von Gruppen.

Sei  $H \xrightarrow{s} G$  ein Gruppenmorphismus mit  $r \circ s = \text{id}_H$ .

Wir haben den Gruppenmorphismus  $\beta : H \rightarrow \text{Aut}(i(N))$ ,  $h \mapsto (i(n) \mapsto {}^{s(h)}(i(n)))$ , 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  $\gamma : \text{Aut}(i(N)) \xrightarrow{\sim} \text{Aut}(N)$ ,  $w \mapsto i'^{-1} \circ w \circ i'$ .

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

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

- (2) Wir haben den Gruppenisomorphismus

$$\begin{aligned} N \rtimes_{\alpha} H &\xrightarrow{\sim} G \\ (n, h) &\mapsto i(n) \cdot s(h) \end{aligned}$$

(3) Folgendes Diagramm kommutiert.

$$\begin{array}{ccccc}
 N & \xrightarrow{\iota} & N \rtimes_{\alpha} H & \xrightarrow{\rho} & H \\
 \downarrow \text{id}_N & & \downarrow f & & \downarrow \text{id}_H \\
 N & \xrightarrow{i} & G & \xrightarrow{r} & H
 \end{array}$$

*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  $r(g \cdot sr(g)^{-}) = r(g) \cdot r(sr(g)^{-}) = 1$ , 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 91, 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  $\text{Im}(f) = i(N) \cdot s(H) = G$  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  $(n, i) \in N \rtimes_{\alpha} H$ .  $\square$

**Definition 96** Sei  $H$  eine Gruppe. Sei  $m \geq 1$ . Sei  $\beta : H \rightarrow S_m$  ein Gruppenmorphismus. Schreibe  $(\beta(h))(i) =: h \cdot i = hi$  für  $h \in H$  und  $i \in [1, m]$ .

Sei  $K$  eine Gruppe. Setze

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

Sei

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

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

Es ist  $\alpha$  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 97**

Sei  $N := \langle (1, 2, 3), (4, 5, 6), (7, 8, 9) \rangle \leq S_9$ . Sei  $H := \langle (1, 4, 7)(2, 5, 8)(3, 6, 9) \rangle \leq S_9$ .

Schreibe  $C_3 = \langle c : c^3 \rangle$ . Dank Aufgabe 2.(3) haben wir den injektiven Gruppenmorphismus

$$\begin{aligned} C_3^{\times 3} &\xrightarrow{u} S_9 \\ (c^{i_1}, c^{i_2}, c^{i_3}) &\longmapsto (1, 2, 3)^{i_1} (4, 5, 6)^{i_2} (7, 8, 9)^{i_3}, \quad \text{wobei } (i_1, i_2, i_3) \in \mathbf{Z}^{\times 3}. \end{aligned}$$

Wir haben den injektiven Gruppenmorphismus

$$\begin{aligned} C_3 &\xrightarrow{v} S_9 \\ c^k &\longmapsto ((1, 4, 7)(2, 5, 8)(3, 6, 9))^k, \quad \text{wobei } k \in \mathbf{Z}. \end{aligned}$$

Wir haben den Gruppenmorphismus  $\beta : C_3 \rightarrow S_3$ ,  $c^k \mapsto (1, 2, 3)^k$ , wobei  $k \in \mathbf{Z}$ ; so wird  $[1, 3]$  zu einer  $C_3$ -Menge.

Es ist

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

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 96. Die universelle Eigenschaft des semidirekten Produkts aus Lemma 91 gibt also den Gruppenmorphismus

$$C_3 \wr_{\beta} C_3 = C_3^{\times 3} \rtimes_{\alpha} C_3 \xrightarrow{f} S_9.$$

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

$$C_3 \wr_{\beta} C_3 \xrightarrow{f|_{NH}} NH = \langle (1, 2, 3), (4, 5, 6), (7, 8, 9), (1, 4, 7)(2, 5, 8)(3, 6, 9) \rangle \in \text{Syl}_3(S_9),$$

denn  $3^3 \cdot 3 = |C_3 \wr_{\beta} C_3| = |NH| = |S_9|[3]$ .

Kurz, die 3-Sylowgruppen von  $S_9$  sind von der Form  $C_3 \wr C_3$ .

## 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  $\alpha : H \rightarrow \text{Aut}(A)$  ein Gruppenmorphismus.

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

**Definition 98** Sei

$$Z^1(H, A) := \{ d : H \rightarrow A : \text{es ist } {}^h d(h') \cdot d(hh')^{-1} \cdot d(h) = 1 \text{ für } h, h' \in H \}$$

die Menge der *Derivationen* oder *1-Cozykel*,

$$B^1(H, A) := \{ d_b : H \rightarrow A, h \mapsto {}^h b \cdot b^{-1} : b \in A \}$$

die Menge der *inneren Derivationen* oder *1-Coränder*,

$$Z^2(H, A) := \{ z : H \times H \rightarrow A : \text{es ist } {}^h z(h', h'') \cdot z(hh', h'')^{-1} \cdot z(h, h'h'') \cdot z(h, h')^{-1} = 1 \text{ für } h, h', h'' \in H \}$$

die Menge der *2-Cozykel*,

$$B^2(H, A) := \{ z_c : H \times H \rightarrow A, (h, h') \mapsto {}^h c(h') \cdot c(hh')^{-1} \cdot c(h) : c : H \rightarrow A \}$$

die Menge der *2-Coränder*

von  $H$  mit Koeffizienten in  $A$  bezüglich  $\alpha$ .

**Bemerkung 99** Ist  $M$  eine Menge und  $B$  eine Gruppe, dann ist die Menge  $\text{Abb}(M, B)$  der Abbildungen von  $M$  nach  $B$  eine abelsche Gruppe unter punktwiser Multiplikation, i.e. für  $u, v \in \text{Abb}(M, B)$  setzen wir

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

Das Einselement ist gegeben durch  $1 : M \rightarrow B, m \mapsto 1$ . Das zu  $u \in \text{Abb}(M, B)$  inverse Element ist gegeben durch  $u^- : M \rightarrow B, m \mapsto u^-(m) := u(m)^-$ .

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

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

**Bemerkung 100**

$$(1) \text{ Es ist } B^1(H, A) \leq Z^1(H, A) \leq \text{Abb}(H, A).$$

$$(2) \text{ Es ist } B^2(H, A) \leq Z^2(H, A) \leq \text{Abb}(H \times H, A).$$

*Beweis.*

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

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

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

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  $B^1(H, A) \leq_{\text{Abb}}(H, A)$ .

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  $d_b \in Z^1(H, A)$ . Somit ist  $B^1(H, A) \leq Z^1(H, A)$ .

*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  $Z^2(H, A) \leq_{\text{Abb}}(H \times H, A)$ .

Es ist  $z_1 = 1$ . Sind  $c, \tilde{c} : H \rightarrow A$  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  $B^2(H, A) \leq_{\text{Abb}}(H \times H, A)$ .

Sei  $c : H \rightarrow A$  gegeben. Es ist

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

Also ist  $z_c \in Z^2(H, A)$ . Somit ist  $B^2(H, A) \leq Z^2(H, A)$ .  $\square$

**Definition 101** Sei

$$\begin{aligned} H^1(H, A) &:= Z^1(H, A)/B^1(H, A) \quad \text{die erste Cohomologiegruppe,} \\ H^2(H, A) &:= Z^2(H, A)/B^2(H, A) \quad \text{die zweite Cohomologiegruppe} \end{aligned}$$

von  $H$  mit Koeffizienten in  $A$  bezüglich  $\alpha$ .

**Bemerkung 102** Sei  $\alpha = ! : H \rightarrow \text{Aut}(A)$ , 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  $B^1(H, A) = 1$ .

Insgesamt ist  $H^1(H, A) = \{d : H \rightarrow A : d \text{ ist Gruppenmorphismus}\}$ .

- (2) Eine Abbildung  $z : H \times H \rightarrow A$  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 103** Sei  $p$  prim. Sei  $H = C_p = \langle h : h^p \rangle$ . Sei  $A = C_p = \langle a : a^p \rangle$ .

Sei  $\alpha = ! : H \rightarrow \text{Aut}(A)$ , 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  $B^1(H, A) = 1$ .

Da eine Derivation  $d : H \rightarrow A$  gerade ein Gruppenmorphismus ist, erhalten wir  $Z^1(H, A) = \{d_i : H \rightarrow A : d_i(h) := a^i\} = \langle d_1 \rangle \simeq C_p$ .

Folglich ist  $H^1(H, A) \simeq C_p$ .

- (2) Sei  $z \in Z^2(H, A)$ . 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

$$\begin{aligned} \varphi : Z^2(H, A) &\longrightarrow C_2 \times C_2 \\ z &\longmapsto (a^{\zeta(0,0)}, a^{\zeta(1,1) - \zeta(0,0)}) \end{aligned}$$

ist bijektiv, da zum einen jede konstante Abbildung von  $H \times H$  nach  $A$  in  $Z^2(H, A)$  liegt und zum anderen die Bedingung  $\zeta(j, k) - \zeta(i+j, k) + \zeta(i, j+k) - \zeta(i, j) \equiv_2 0$

an  $\zeta$  unter Berücksichtigung obiger Bemerkung redundant ist für  $i = 0$  oder  $j = 0$  oder  $k = 0$  oder  $(i, j, k) = (1, 1, 1)$ .

Sei  $c : H \rightarrow A$ ,  $h^i \rightarrow c(h^i) =: a^{\gamma(i)}$  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

$$\varphi(B^2(H, A)) = C_2 \times 1.$$

Es folgt  $H^2(H, A) \simeq (C_2 \times C_2)/(C_2 \times 1) \simeq C_2$ .

(3) Sei e.g.  $H = 1$ . Es ist  $H^1(1, A) = 1$ ; cf. Bemerkung 102.(1).

Es ist  $H^2(1, A) = 1$ . Für eine Abbildung  $c : 1 \rightarrow A$  wird  $z_c(1, 1) = c(1)$ , sodaß  $B^2(1, A)$  ist die Menge aller Abbildungen von  $1 \times 1$  nach  $A$  ist, woraus  $B^2(1, A) = Z^2(1, A) = \text{Abb}(1 \times 1, A)$  folgt.

**Lemma 104** Sei  $K \leq H$  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  $\alpha : H \rightarrow \text{Aut}(A)$ , für  $K$  bezüglich  $\alpha|_K : K \rightarrow \text{Aut}(A)$ , wobei  $i \in \{1, 2\}$ .

(1) Wir haben die Gruppenmorphisimen

$$\begin{array}{ccc} Z^1(K, A) & \longleftrightarrow & Z^1(H, A) \\ d & \longmapsto & (d|_K^H : H \rightarrow A, h \mapsto \prod_{t \in T} {}^{t^-}d(\kappa(th))) \\ \tilde{d}|_K & \longleftarrow & \tilde{d} \end{array}$$

(2) Wir haben die Gruppenmorphisimen

$$\begin{array}{ccc} H^1(K, A) & \longleftrightarrow & H^1(H, A) \\ dB^1(K, A) & \xrightarrow{\text{Cores}|_K^H} & d|_K^H B^1(H, A) \\ \tilde{d}|_K B^1(K, A) & \xleftarrow{\text{Res}|_K^H} & \tilde{d} B^1(H, A). \end{array}$$

Es ist

$$(\text{Cores}|_K^H \circ \text{Res}|_K^H)(\tilde{d} B^1(H, A)) = (\tilde{d} B^1(H, A))^{[H:K]}$$

für  $\tilde{d} \in Z^1(H, A)$ .

(3) Wir haben die Gruppenmorphisimen

$$\begin{array}{ccc} Z^2(K, A) & \longleftrightarrow & Z^2(H, A) \\ z & \longmapsto & (z|_K^H : H \times H \rightarrow A, (h, h') \mapsto \prod_{t \in T} {}^{t^-}z(\kappa(th), \kappa(th)^{-1} \kappa(thh'))) \\ \tilde{z}|_{K \times K} & \longleftarrow & \tilde{z} \end{array}$$

(4) Wir haben die Gruppenmorphisimen

$$\begin{array}{ccc} H^2(K, A) & \longleftrightarrow & H^2(H, A) \\ zB^2(K, A) & \xrightarrow{\text{Cores}|_K^H} & z|_K^H B^2(H, A) \\ \tilde{z}|_{K \times K} B^2(K, A) & \xleftarrow{\text{Res}|_K^H} & \tilde{z}B^2(H, A) . \end{array}$$

Es ist

$$(\text{Cores}|_K^H \circ \text{Res}|_K^H)(\tilde{z}B^2(H, A)) = (\tilde{z}B^2(H, A))^{[H:K]}$$

für  $\tilde{z} \in Z^2(H, A)$ .

Die Formeln für  $\text{Cores}|_K^H$  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  $\tilde{d} \in Z^1(H, A)$ , so liegt a fortiori  $\tilde{d}|_K \in Z^1(K, A)$ . Da die Abbildung  $\tilde{d} \mapsto \tilde{d}|_K$  punktweise Multiplikation respektiert, ist sie ein Gruppenmorphismus.

Sei umgekehrt  $d \in Z^1(K, A)$  gegeben. Wir haben  $d|_K^H \in Z^1(H, A)$  zu zeigen.

Beachte, daß für  $k, k' \in K$  sich  ${}^k d(k^{-1}k') \cdot d(k')^{-1} \cdot d(k) = 1$  ergibt durch Anwendung der 1-Cozykel-Bedingung auf  $(k, k^{-1}k')$ .

Seien nun  $h, h' \in H$  gegeben. Zunächst ist  $th^{-1} = \kappa(th^{-1}) \cdot \tau(th^{-1})$ , also  $t = \kappa(th^{-1}) \cdot \tau(th^{-1})h$  und auch  $1 = \kappa(t) = \kappa(th^{-1}) \cdot \kappa(\tau(th^{-1})h)$  für  $t \in T$ , wegen  $\bigsqcup_{t \in T} Kth^{-1} = H$  somit

$$\begin{aligned} {}^h d|_K^H(h') &= {}^h \left( \prod_{t \in T} t^{-1} d(\kappa(th')) \right) \\ &= \prod_{t \in T} (th^{-1})^{-1} d(\kappa(th')) \\ &= \prod_{t \in T} (\kappa(th^{-1}) \cdot \tau(th^{-1}))^{-1} d(\kappa(\kappa(th^{-1}) \cdot \tau(th^{-1})hh')) \\ &= \prod_{t \in T} \tau(th^{-1})^{-1} \cdot \kappa(th^{-1})^{-1} d(\kappa(th^{-1}) \cdot \kappa(\tau(th^{-1})hh')) \\ &= \prod_{t \in T} \tau(th^{-1})^{-1} \cdot \kappa(\tau(th^{-1})h) d(\kappa(\tau(th^{-1})h)^{-1} \kappa(\tau(th^{-1})hh')) \\ &= \prod_{t \in T} t^{-1} \cdot \kappa(th) d(\kappa(th)^{-1} \kappa(thh')) . \end{aligned}$$

Also wird

$$\begin{aligned} &{}^h d|_K^H(h') \cdot d|_K^H(hh')^{-1} \cdot d|_K^H(h) \\ &= \left( \prod_{t \in T} t^{-1} \cdot \kappa(th) d(\kappa(th)^{-1} \kappa(thh')) \right) \cdot \left( \prod_{t \in T} t^{-1} d(\kappa(thh')) \right)^{-1} \cdot \left( \prod_{t \in T} t^{-1} d(\kappa(th)) \right) \\ &= \prod_{t \in T} t^{-1} \left( \kappa(th) d(\kappa(th)^{-1} \kappa(thh')) \right) \cdot d(\kappa(thh'))^{-1} \cdot d(\kappa(th)) \\ &= 1 . \end{aligned}$$

Da auch die Abbildung  $d \mapsto d|_K^H$  punktweise Multiplikation respektiert, ist sie ein Gruppenmorphismus.

Ad (2). Es ist zu zeigen, daß für  $\tilde{d} \in B^1(H, A)$  auch  $\tilde{d}|_K \in B^1(K, A)$  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  $\tilde{d}|_K \in B^1(K, A)$ .

Es ist zu zeigen, daß für  $d \in B^1(K, A)$  auch  $d|_K^H \in B^1(H, A)$  liegt. Wähle ein  $b \in A$  mit  $d(k) = {}^k b \cdot b^-$  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

$$\begin{aligned} d|_K^H(h) &= \prod_{t \in T} {}^{t^-} d(\kappa(th)) \\ &= \prod_{t \in T} {}^{t^-} ({}^{\kappa(th)} b \cdot b^-) \\ &= \left( \prod_{t \in T} {}^{t^- \kappa(th)} b \right) \cdot \left( \prod_{t \in T} {}^{t^-} b \right)^- \\ &= {}^h \left( \prod_{t \in T} {}^{\tau(th)^-} b \right) \cdot \left( \prod_{t \in T} {}^{t^-} b \right)^- \\ &= {}^h \left( \prod_{t \in T} {}^{t^-} b \right) \cdot \left( \prod_{t \in T} {}^{t^-} b \right)^- \\ &= {}^h \tilde{b} \cdot \tilde{b}^-, \end{aligned}$$

wobei  $\tilde{b} := \prod_{t \in T} {}^{t^-} b \in A$ .

Sei  $\tilde{d} \in Z^1(H, A)$ . Es bleibt  $(\text{Cores}|_K^H \circ \text{Res}|_K^H)(\tilde{d}B^1(H, A)) \stackrel{!}{=} (\tilde{d}B^1(H, A))^{[H:K]}$  zu zeigen.

Sei  $h \in H$  gegeben. Dann wird  $th = \kappa(th) \cdot \tau(th)$ , also

$$\tilde{d}(h) \cdot \tilde{d}(t) = \tilde{d}(th) = \tilde{d}(\kappa(th) \cdot \tau(th)) = {}^{\kappa(th)} \tilde{d}(\tau(th)) \cdot \tilde{d}(\kappa(th)).$$

Dank  $\bigsqcup_{t \in T} Kth = H$  wird also

$$\begin{aligned} \tilde{d}|_K|_K^H(h) &= \prod_{t \in T} {}^{t^-} \tilde{d}(\kappa(th)) \\ &= \prod_{t \in T} \left( \tilde{d}(h) \cdot ({}^{t^- \kappa(th)} \tilde{d}(\tau(th)))^- \cdot {}^{t^-} \tilde{d}(t) \right) \\ &= \tilde{d}(h)^{|T|} \cdot \left( \prod_{t \in T} {}^{h\tau(th)^-} \tilde{d}(\tau(th)) \right)^- \cdot \left( \prod_{t \in T} {}^{t^-} \tilde{d}(t) \right) \\ &= \tilde{d}(h)^{|T|} \cdot {}^h \left( \prod_{t \in T} {}^{\tau(th)^-} \tilde{d}(\tau(th)) \right)^- \cdot \left( \prod_{t \in T} {}^{t^-} \tilde{d}(t) \right) \\ &= \tilde{d}(h)^{|T|} \cdot {}^h \left( \prod_{t \in T} {}^{t^-} (\tilde{d}(t)^-) \right) \cdot \left( \prod_{t \in T} {}^{t^-} (\tilde{d}(t)^-) \right)^- \\ &= \tilde{d}(h)^{[H:K]} \cdot {}^h \tilde{b} \cdot \tilde{b}^- \end{aligned}$$

wobei  $\tilde{b} := \prod_{t \in T} {}^{t^-} (\tilde{d}(t)^-) \in A$ .

Die Abbildung  $\text{Cores}|_K^H$  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  $d \in Z^1(K, A)$ . Es wird für  $h \in H$  auch  $\bigsqcup_{t \in T} Kth = H$  und also

$$\begin{aligned}
\prod_{t' \in T'} {}^{t'} d(\kappa'(t'h)) &= \prod_{t \in T} {}^{t-k_t^-} d(\kappa'(k_t th)) \\
&= \prod_{t \in T} {}^{t-k_t^-} d(k_t \kappa'(th)) \\
&= \prod_{t \in T} {}^{t-k_t^-} d(k_t \kappa(th) k_{\tau(th)}^-) \\
&= \prod_{t \in T} {}^{t-k_t^-} ({}^{k_t \kappa(th)} d(k_{\tau(th)}^-) \cdot {}^{k_t} d(\kappa(th)) \cdot d(k_t)) \\
&= \prod_{t \in T} {}^{t-} ({}^{\kappa(th)} d(k_{\tau(th)}^-) \cdot d(\kappa(th)) \cdot {}^{k_t^-} d(k_t)) \\
&= (\prod_{t \in T} {}^{t-\kappa(th)} d(k_{\tau(th)}^-)) \cdot (\prod_{t \in T} {}^{t-} d(\kappa(th))) \cdot (\prod_{t \in T} {}^{t-k_t^-} d(k_t)) \\
&= (\prod_{t \in T} {}^{h\tau(th)-} d(k_{\tau(th)}^-)) \cdot (\prod_{t \in T} {}^{t-k_t^-} d(k_t)) \cdot (\prod_{t \in T} {}^{t-} d(\kappa(th))) \\
&= {}^h (\prod_{t \in T} {}^{\tau(th)-} k_{\tau(th)}^- d(k_{\tau(th)}^-)) \cdot (\prod_{t \in T} {}^{t-k_t^-} d(k_t)) \cdot (\prod_{t \in T} {}^{t-} d(\kappa(th))) \\
&= {}^h (\prod_{t \in T} {}^{t-k_t^-} d(k_t)) \cdot (\prod_{t \in T} {}^{t-k_t^-} d(k_t)) \cdot (\prod_{t \in T} {}^{t-} d(\kappa(th))) \\
&= {}^{h\tilde{b}} \cdot \tilde{b}^- \cdot (\prod_{t \in T} {}^{t-} d(\kappa(th))),
\end{aligned}$$

wobei  $\tilde{b} := (\prod_{t \in T} {}^{t-k_t^-} d(k_t))^- \in A$ .

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 105 (und Definition)

Sei  $A \xrightarrow{i} G \xrightarrow{r} H$  eine kurz exakte Sequenz von Gruppen.

Sei  $\beta : H \rightarrow \text{Aut}(i(A))$ ,  $h \mapsto (\beta(h) : i(a) \mapsto {}^g i(a))$ , wobei  $g \in G$  mit  $r(g) = h$  gewählt werde. Es ist  $\beta$  ein Gruppenmorphismus.

Sei  $i' := i|^{i(A)} : A \xrightarrow{\sim} i(A)$ . Sei  $\gamma : \text{Aut}(i(A)) \rightarrow \text{Aut}(A)$ ,  $\varphi \mapsto i'^- \circ \varphi \circ i'$ .

Es ist auch  $\alpha := \gamma \circ \beta : H \rightarrow \text{Aut}(A)$  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  $\alpha$  von der kurz exakten Sequenz  $A \xrightarrow{i} G \xrightarrow{r} H$  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  ${}^g i(a) \stackrel{!}{=} \tilde{g} i(a)$  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  $\beta$  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  $\gamma$  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

$$\begin{aligned} i({}^h a) &= i'((\alpha(h))(a)) = i'((\gamma \circ \beta)(h)(a)) \\ &= i'((i'^{-1} \circ \beta(h) \circ i')(a)) = i'(i'^{-1}({}^g i(a))) = {}^g i(a). \end{aligned}$$

□

Im Unterschied zur Situation von Lemma 95 ist nun kein Gruppenmorphismus  $G \xleftarrow{s} H$  mit  $r \circ s = \text{id}_H$  gegeben, dafür ist nun aber die linksstehende Gruppe abelsch – was ebenfalls die Wohldefiniertheit von  $\alpha$  sichert.

**Beispiel 106** Sei  $A \trianglelefteq G$ . Sei  $A \xrightarrow{i} G$  die Inklusion  $\text{id}_G|_A$ . Sei  $G \xrightarrow{r} G/A$ ,  $g \mapsto gA$ . Dies gibt die kurz exakte Sequenz  $A \xrightarrow{i} G \xrightarrow{r} G/A$ . Diese induziert einen Gruppenmorphismus  $\alpha : G/A \rightarrow \text{Aut}(A)$ ; cf. Lemma 105.

**Lemma 107** Sei  $A \xrightarrow{i} G \xrightarrow{r} H$  eine kurz exakte Sequenz von Gruppen, mit  $A$  abelsch.

Diese induziert einen Gruppenmorphismus  $\alpha : H \rightarrow \text{Aut}(A)$ ; cf. Lemma 105.

Sei  $H^1(H, A)$  genommen bezüglich  $\alpha$ .

Sei ein Gruppenmorphismus  $G \xleftarrow{s} H$  mit  $r \circ s = \text{id}_H$  gegeben.

Die folgenden Aussagen (1, 2) sind äquivalent.

(1) Es ist  $H^1(H, A) = 1$ .

(2) Für alle Gruppenmorphisme  $G \xleftarrow{\tilde{s}} H$  mit  $r \circ \tilde{s} = \text{id}_H$  gibt es ein  $b \in A$  mit  ${}^{i(b)}\tilde{s}(h) = \tilde{s}(h)$  für  $h \in H$ .

*Beweis.*

Ad (1)  $\Rightarrow$  (2). Sei ein Gruppenmorphismus  $G \xleftarrow{\tilde{s}} H$  mit  $r \circ \tilde{s} = \text{id}_H$  gegeben. Es ist  $r(s(h)\tilde{s}(h)^{-1}) = hh^{-1} = 1$  für  $h \in H$ , sodaß es eine Abbildung  $d : H \rightarrow A$  gibt mit



$i(d(h)) := s(h)\tilde{s}(h)^{-}$  für  $h \in H$ . Es ist  $d \in Z^1(H, A)$ , 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  $H^1(H, A) = 1$  ist  $d \in B^1(H, A)$ . 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  $H^1(H, A) \stackrel{!}{=} 1$  zu zeigen, i.e.  $Z^1(H, A) \stackrel{!}{=} B^1(H, A)$ .

Sei  $d \in Z^1(H, A)$  gegeben. Wir haben  $d \stackrel{!}{\in} B^1(H, A)$  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  $r \circ \tilde{s} = \text{id}_H$ , 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 108** Sei  $G$  eine Gruppe. Sei  $A \triangleleft G$  ein abelscher Normalteiler. Sei  $K$  ein Komplement zu  $A$  in  $G$ .

Sei  $H^1(G/A, A)$  genommen bezüglich  $\alpha : G/A \rightarrow \text{Aut}(A)$  wie in Beispiel 106.

Die folgenden Aussagen (1, 2) sind äquivalent.

- (1) Es ist  $H^1(G/A, A) = 1$ .
- (2) Für alle Komplemente  $\tilde{K}$  zu  $A$  in  $G$  gibt es ein  $g \in G$  mit  ${}^gK = \tilde{K}$ .

*Beweis.* Sei  $A \xrightarrow{i} G$  die Inklusion  $\text{id}_G|_A$ . Sei  $G \xrightarrow{r} G/A$ ,  $g \mapsto gA$ . Dies gibt die kurz exakte Sequenz  $A \xrightarrow{i} G \xrightarrow{r} G/A$ .

Wir haben den Gruppenisomorphismus  $\psi := r|_K : K \rightarrow G/A$ ,  $k \mapsto kA$ ; cf. Bemerkung 93.(2). Sei  $s := \text{id}_G|_K \circ \psi^{-1} : G/A \rightarrow G$ ,  $gA \mapsto \psi^{-1}(gA)$ . Es ist  $s$  ein Gruppenmorphismus mit Bild  $K$  und mit  $r \circ s = \text{id}_{G/A}$ , denn  $(r \circ s)(xA) = r(\psi^{-1}(xA)) = \psi(\psi^{-1}(xA)) = xA$  für  $x \in G$ .

*Ad (1)  $\Rightarrow$  (2).* Sei  $\tilde{K}$  ein Komplement zu  $A$  in  $G$ .

Sei  $\tilde{s} : G/A \rightarrow G$  ein Gruppenmorphismus mit Bild  $\tilde{K}$  und mit  $r \circ \tilde{s} = \text{id}_{G/A}$ .

Lemma 107 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 107 genügt es, für jeden Gruppenmorphismus  $\tilde{s} : G/A \rightarrow G$  mit  $r \circ \tilde{s} = \text{id}_{G/A}$  ein  $b \in A$  zu finden mit  ${}^{i(b)}s(xA) = \tilde{s}(xA)$  für  $x \in G$ .

Es ist  $\tilde{K} := \text{Im}(\tilde{s})$  ein Komplement zu  $A$  in  $G$ ; cf. Lemma 95. 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  $xA \stackrel{!}{=} x'A$  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 109** Sei  $p > 0$  prim. Sei  $G = \langle a, b : a^p, b^p, [a, b] \rangle \simeq C_p \times C_p$ . 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 105 induzierte Gruppenmorphismus  $G/\langle a \rangle \rightarrow \text{Aut}(\langle b \rangle)$  ist wegen  $G$  abelsch gleich  $!$ . Cf. Aufgabe 41.(2).

Folglich ist  $H^1(C_p, C_p) > 1$ , genommen bezüglich  $! : C_p \rightarrow \text{Aut}(C_p)$ .

In der Tat ist  $H^1(C_p, C_p) \simeq C_p$ ; cf. Beispiel 103.(1).

**Lemma 110** Sei  $\alpha : H \rightarrow \text{Aut}(A)$  ein Gruppenmorphismus. Sei  $H^2(H, A)$  genommen bezüglich  $\alpha$ .

Die folgenden Aussagen (1, 2) sind äquivalent.

- (1) Es ist  $H^2(H, A) = 1$ .
- (2) Für jede kurz exakte Sequenz von Gruppen  $A \xrightarrow{i} G \xrightarrow{r} H$ , die  $\alpha$  induziert im Sinne von Lemma 105, gibt es einen Gruppenmorphismus  $s : H \rightarrow G$  mit  $r \circ s = \text{id}_H$ .

Diesemfalls sind wir also in der Situation von Lemma 95. Insbesondere ist  $G$  dann ein semidirektes Produkt aus  $A$  und  $H$ .

*Beweis.*

*Ad (1)  $\Rightarrow$  (2).* Sei  $A \xrightarrow{i} G \xrightarrow{r} H$  eine kurz exakte Sequenz von Gruppen. Sei  $\mathfrak{s} : H \rightarrow G$  eine Abbildung mit  $r \circ \mathfrak{s} = \text{id}_H$ , wählbar, da  $r$  surjektiv ist <sup>(2)</sup>. 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  $z : H \times H \rightarrow A$ .

Wir behaupten  $z \in Z^2(H, A)$ . Für  $h, h', h'' \in H$  wird

$$\begin{aligned} & i(z(h, h')^{-} \cdot {}^h z(h', h'') \cdot z(h, h'h'') \cdot z(hh', h'')^{-}) \\ \stackrel{\text{L.105}}{=} & i(z(h, h')^{-} \cdot {}^{\mathfrak{s}(h)} i(z(h', h'')) \cdot i(z(h, h'h'')) \cdot i(z(hh', h''))^{-}) \\ = & (\mathfrak{s}(hh') \cdot \mathfrak{s}(h')^{-} \cdot \mathfrak{s}(h)^{-}) \cdot (\mathfrak{s}(h) \cdot \mathfrak{s}(h') \cdot \mathfrak{s}(h'') \cdot \mathfrak{s}(h'h'')^{-} \cdot \mathfrak{s}(h)^{-}) \\ & \cdot (\mathfrak{s}(h) \cdot \mathfrak{s}(h'h'') \cdot \mathfrak{s}(hh'h'')^{-}) \cdot (\mathfrak{s}(hh'h'') \cdot \mathfrak{s}(h'')^{-} \cdot \mathfrak{s}(hh')^{-}) \\ = & 1. \end{aligned}$$

Die Behauptung folgt hieraus dank  $i$  injektiv.

Wegen  $H^2(H, A) = 1$  ist nun  $Z^2(H, A) = B^2(H, A)$ . Also ist  $z \in B^2(H, A)$ . Wähle eine Abbildung  $c : H \rightarrow A$  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  $s : H \rightarrow G$ ,  $h \mapsto s(h) := c'(h)^{-} \cdot \mathfrak{s}(h)$ .

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  $r \circ s = \text{id}_H$ .

Wir haben zu zeigen, daß  $s$  ein Gruppenmorphismus ist. Seien  $h, h', \in H$  gegeben. Es wird

$$\begin{aligned} s(hh') &= c'(hh')^{-} \cdot \mathfrak{s}(hh') \\ &= c'(hh')^{-} \cdot c'(h)^{-} \cdot c'(hh') \cdot {}^{\mathfrak{s}(h)} c'(h')^{-} \cdot \mathfrak{s}(h) \cdot \mathfrak{s}(h') \\ &= c'(h)^{-} \cdot \mathfrak{s}(h) \cdot c'(h')^{-} \cdot \mathfrak{s}(h)^{-} \cdot \mathfrak{s}(h) \cdot \mathfrak{s}(h') \\ &= c'(h)^{-} \cdot \mathfrak{s}(h) \cdot c'(h')^{-} \cdot \mathfrak{s}(h') \\ &= s(h) \cdot s(h'). \end{aligned}$$

*Ad (2)  $\Rightarrow$  (1).* Wir haben  $H^2(H, A) \stackrel{!}{=} 1$  zu zeigen, i.e.  $Z^2(H, A) \stackrel{!}{=} B^2(H, A)$ .

Sei  $z \in Z^2(H, A)$  gegeben. Wir haben  $z \stackrel{!}{\in} B^2(H, A)$  zu zeigen.

---

<sup>2</sup>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

$$\begin{aligned} ((a, h) \cdot (a', h')) \cdot (a'', h'') &= (a {}^h a' z(h, h'), hh') \cdot (a'', h'') \\ &= (a {}^h a' {}^{hh'} a'' z(h, h') z(hh', h''), hh'h'') \\ &= (a {}^h a' {}^{hh'} a'' {}^{h_z} z(h', h'') z(h, h'h''), hh'h'') \\ &= (a, h) \cdot (a' {}^{h'} a'' z(h', h''), h'h'') \\ &= (a, h) \cdot ((a', h') \cdot (a'', h'')) \end{aligned}$$

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

$$\begin{array}{ccccc} A & \xrightarrow{i} & G & \xrightarrow{r} & H \\ a & \mapsto & (a z(1, 1)^-, 1) & & \\ & & (a, h) & \mapsto & h. \end{array}$$

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

$$\text{Im}(i) = \{(a z(1, 1)^-, 1) : a \in A\} = \{(\tilde{a}, 1) : \tilde{a} \in A\} = \text{Kern}(r).$$

Diese kurz exakte Sequenz induziere den Gruppenmorphismus  $\tilde{\alpha} : H \rightarrow \text{Aut}(A)$  im Sinne von Lemma 107. 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  $G \xleftarrow{s} H$  mit  $r \circ s = \text{id}_H$ , i.e. mit  $s(h) = (c(h)^-, h)$  für eine Abbildung  $c : H \rightarrow A$ . 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  $z \in B^2(H, A)$ . □

**Korollar 111** Sei  $G$  eine Gruppe. Sei  $A \trianglelefteq G$  ein abelscher Normalteiler.

Sei  $H^2(G/A, A)$  genommen bezüglich  $\alpha : G/A \rightarrow \text{Aut}(A)$  wie in Beispiel 106.

Ist  $H^2(G/A, A) = 1$ , dann hat  $A$  in  $G$  ein Komplement.

*Beweis.* Sei  $H^2(G/A, A) = 1$ .

Sei  $A \xrightarrow{i} G$  die Inklusion  $\text{id}_G|_A$ . Sei  $G \xrightarrow{r} G/A$ ,  $g \mapsto gA$ . Dies gibt die kurz exakte Sequenz  $A \xrightarrow{i} G \xrightarrow{r} G/A$ .

Dank Lemma 110 gibt es einen Gruppenmorphismus  $s : G/A \rightarrow G$  mit  $r \circ s = \text{id}_{G/A}$ .

Es ist  $s(G/A)$  ein Komplement zu  $A$  in  $G$ ; cf. Lemma 95.(1). □

**Beispiel 112** Sei  $G = \langle a : a^4 \rangle \simeq C_4$ . Es hat  $\langle a^2 \rangle$  in  $C_4$  kein Komplement; cf. Beispiel 94.(6). Der im Sinne von Lemma 105 induzierte Gruppenmorphismus  $G/\langle a^2 \rangle \rightarrow \text{Aut}(\langle a^2 \rangle)$  ist wegen  $G$  abelsch (oder wegen  $\text{Aut}(\langle a^2 \rangle) = 1$ ) gleich !.

Folglich ist  $H^2(C_2, C_2) > 1$ , genommen bezüglich ! :  $C_2 \rightarrow \text{Aut}(C_2)$ .

In der Tat ist  $H^2(C_2, C_2) \simeq C_2$ ; cf. Beispiel 103.(2).

**Bemerkung 113** Sei  $H$  eine endliche Gruppe. Sei  $A$  eine endliche abelsche Gruppe. Sei  $\alpha : H \rightarrow \text{Aut}(A)$  ein Gruppenmorphismus. Seien  $H^1(H, A)$  und  $H^2(H, A)$  genommen bezüglich  $\alpha$ .

- (1) Für  $\delta \in H^1(H, A)$  ist  $\delta^{\exp(A)} = 1$ .
- (2) Für  $\delta \in H^1(H, A)$  ist  $\delta^{|H|} = 1$ .
- (3) Für  $\zeta \in H^2(H, A)$  ist  $\zeta^{\exp(A)} = 1$ .
- (4) Für  $\zeta \in H^2(H, A)$  ist  $\zeta^{|H|} = 1$ .

*Beweis.*

*Ad (1).* Dies gilt in  $\text{Abb}(H, A)$ , also in der Untergruppe  $Z^1(H, A)$ , also in der Faktorgruppe  $H^1(H, A)$ .

*Ad (2).* Für  $\delta \in H^1(H, A)$  ist

$$\delta^{|H|} \stackrel{\text{L. 104.(2)}}{=} (\text{Cores } \downarrow_1^H \circ \text{Res } \downarrow_1^H)(\delta) = 1,$$

letzteres, da  $H^1(1, A) = 1$ ; cf. Beispiel 103.(3).

*Ad (3).* Dies gilt in  $\text{Abb}(H \times H, A)$ , also in der Untergruppe  $Z^2(H, A)$ , also in der Faktorgruppe  $H^2(H, A)$ .

*Ad (4).* Für  $\zeta \in H^2(H, A)$  ist

$$\zeta^{|H|} \stackrel{\text{L. 104.(4)}}{=} (\text{Cores } \downarrow_1^H \circ \text{Res } \downarrow_1^H)(\zeta) = 1,$$

letzteres, da  $H^2(1, A) = 1$ ; cf. Beispiel 103.(3). □

**Lemma 114 (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  $\alpha : G/A \rightarrow \text{Aut}(A)$  wie in Beispiel 106. Seien  $H^1(H, A)$  und  $H^2(H, A)$  genommen bezüglich  $\alpha$ .

Zeigen wir zunächst  $H^1(G/A, A) \stackrel{!}{=} 1$ . Sei  $\delta \in H^1(G/A, A)$ . Wir müssen  $|\langle \delta \rangle| \stackrel{!}{=} 1$  zeigen. Es ist  $\delta^{\exp(A)} = 1$ , also auch  $\delta^{|A|} = 1$ ; cf. Bemerkung 113.(1). Es ist  $\delta^{|G/A|} = 1$ ; cf. Bemerkung 113.(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  $H^2(H, A) = 1$  unter Verwendung von Bemerkung 113.(3, 4).

*Ad (1).* Da  $H^2(G/A, A) = 1$ , hat dank Korollar 111 der abelsche Normalteiler  $A$  in  $G$  ein Komplement.

*Ad (2).* Da  $H^1(G/A, A) = 1$ , gibt es dank Korollar 108 ein  $g \in G$  mit  $\tilde{K} = {}^gK$ . □

### 3.4.3 Zassenhaus

**Lemma 115 (Frattni)** *Sei  $G$  eine endliche Gruppe. Sei  $N \trianglelefteq G$ .*

*Sei  $p$  prim. Sei  $P \in \text{Syl}_p(N)$ .*

*Dann ist  $N_G(P) \cdot N = G$ .*

*Beweis.* Es ist  $\text{Syl}_p(N)$  eine transitive  $N$ -Menge; cf. Satz 37.(2). Sei  $g \in G$ . Sei  $P \in \text{Syl}_p(N)$ . Wegen  $N \trianglelefteq G$  ist auch  ${}^gP \in \text{Syl}_p(N)$ . Folglich gibt es ein  $n \in N$  mit  ${}^gP = {}^nP$ . Also ist  $n^{-1}g \in N_G(P)$  und somit  $g \in N_G(P) \cdot N$ .  $\square$

Lemma 115 kann auch aus Aufgabe 6.(1) gefolgert werden.

**Bemerkung 116** Sei  $G$  eine Gruppe. Seien  $H, K, L \leq G$ . Sei  $H \leq L$ . 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  $k = h^{-1}(hk)$  in  $L$ , da  $h^{-1}$  in  $L$  enthalten ist, und somit ist  $hk \in H(K \cap L)$ .  $\square$

**Definition 117** 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 118** Sei  $G$  eine endliche Gruppe. Sei  $N \trianglelefteq G$  hallsch. Sei  $K \leq G$ .

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 93.(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).  $\square$

**Satz 119 (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 93.

*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  $P \in \text{Syl}_p(N)$ ; cf. Satz 37.(1). Wir behaupten  $P \trianglelefteq G$ . Sei im Gegenteil *angenommen*, es ist  $N_G(P) < G$ . Es ist  $G = N_G(P) \cdot N$ ; cf. Lemma 115. Es ist  $N_N(P) = N \cap N_G(P)$  hallsch in  $N_G(P)$ , da  $|N_N(P)|$  ein Teiler von  $|N|$  ist und  $|N_G(P)/(N \cap N_G(P))| = |N_G(P) \cdot N/N| = |G/N|$  ist; cf. Aufgabe 12.(2). Wegen der Minimalität von  $|G|$  existiert ein Komplement  $K$  zu  $N_N(P)$  in  $N_G(P)$ , 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 118.(1). Wir haben einen *Widerspruch*. Also ist  $P \trianglelefteq G$ .

Schreibe  $Z := Z(P)$ . Es ist  $Z > 1$ ; beachte  $P > 1$  und Aufgabe 31.(1). Es ist  $Z \triangleleft P \trianglelefteq G$  und also  $Z \trianglelefteq G$ ; cf. Bemerkung 79.(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  $Z \leq L \leq G$ ; 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 114.(1). Insbesondere ist  $|M| = |L/Z| = |G/N|$ ; cf. Bemerkung 93.(2). Da  $N$  hallsch in  $G$  ist, ist  $M$  ein Komplement zu  $N$  in  $G$ ; cf. Bemerkung 118.(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 83. Aus  $N^{(1)} \triangleleft N \trianglelefteq G$  folgt ferner  $N^{(1)} \trianglelefteq G$ ; cf. Bemerkung 79.(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  $\bar{K}, \bar{L} \leq \bar{G}$ . Wegen  $K \cap N^{(1)} = 1$  und  $L \cap N^{(1)} = 1$  ist  $K \xrightarrow{\sim} \bar{K}$ ,  $k \mapsto kN^{(1)}$ , insgesamt also  $K \simeq \bar{K} \simeq G/N$ ; cf. Bemerkung 93.(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 118.(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,  ${}^y\bar{K} = \bar{L}$ , i.e. mit  $({}^yK)N^{(1)} = LN^{(1)} =: G'$ . 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 83. Es ist  $|N^{(1)}|$  ein Teiler von  $|N|$ , und dies teilerfremd zu  $|G/N| = |{}^yK| = |L| = |G'/N^{(1)}|$ . Also ist  $N^{(1)} \trianglelefteq G'$  hallsch, und es sind  ${}^yK$  und  $L$  Komplemente zu  $N^{(1)}$  in  $G'$ ; cf. Bemerkung 118.(1). Wegen der Minimalität von  $|G|$  folgt nun, daß es ein  $x \in G'$  gibt mit  $L = {}^x({}^yK) = {}^{xy}K$ , 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  $N \triangleleft G$  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 83, 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  $N \leq NG^{(1)} \leq M \triangleleft G$  mit  $|G/M| =: p > 1$  prim; cf. Aufgabe 17.(3). Wäre  $N = M$ , so wären  $K, L \in \text{Syl}_p(G)$  und also gemäß Satz 37.(2) zueinander konjugiert, was nicht der Fall ist. Also ist  $N < M$ . Insgesamt ist  $N \triangleleft M$ .

Da  $N \triangleleft G$  hallsch ist, ist auch  $N \triangleleft M$  hallsch. Es ist  $N \cap (K \cap M) = 1$  und  $N(K \cap M) = NK \cap M = G \cap M = M$ ; cf. Bemerkung 116. 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 93.(2). Es ist  $U \triangleleft L$ , i.e.  $L \leq N_G(U)$ . Genauso ist  ${}^mK \leq N_G(U)$ .

*Subfall*  $N_G(U) < G$ . Es ist  $N \cap N_G(U) =: N' \triangleleft N_G(U)$ . Es ist  $L \cap N' = 1$  und  $LN' = L(N \cap N_G(U)) = LN \cap N_G(U) = N_G(U)$ ; cf. Bemerkung 116. Genauso ist  ${}^mK \cap N' = 1$  und  $({}^mK) \cdot N' = N_G(U)$ . Also sind  $L$  und  ${}^mK$  Komplemente zu  $N'$  in  $N_G(U)$ . Da  $N' \leq N$ , ist  $|N'|$  teilerfremd zu  $|N_G(U)/N'| = |L|$ . Somit ist  $N' \triangleleft N_G(U)$  hallsch. Ferner ist  $N_G(U)/N' \simeq L \simeq G/N$  auflösbar; cf. Bemerkung 93.(2). Wegen der Minimalität von  $|G|$  gibt es ein  $x \in N_G(U) \leq G$  mit  $L = {}^x({}^mK) = {}^{xm}K$ . Da  $xm \in G$ , haben wir diesenfalls einen *Widerspruch*.

*Subfall*  $N_G(U) = G$ . Es ist  $U \triangleleft G$ . Es ist  $N \cap U = N \cap (L \cap M) = 1$ . Also ist  $N \xrightarrow{\sim} NU/U$ ,  $n \mapsto nU$ . Es ist  $NU/U \triangleleft G/U$  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 118.(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*.  $\square$

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 119.(2) weggelassen werden darf.

**Beispiel 120** Sei  $G$  eine endliche Gruppe. Sei  $p \in \pi(G)$ . Sei  $\text{Syl}_p(G) = \{P\}$ . Dann ist  $P \triangleleft G$  hallsch. Dank Satz 119 hat  $P$  also ein Komplement in  $G$ , und alle solchen Komplemente sind konjugiert in  $G$ ; cf. Bemerkungen 74.(1) und 75.

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 118. Diesenfalls können wir die Existenz eines Komplements zu  $P$  in  $G$  also auch aus Satz 37.(1) folgern; ferner folgt die Tatsache, daß zwei Komplemente zu  $P$  in  $G$  dort zueinander konjugiert sind, dann auch aus Satz 37.(2).

# Kapitel 4

## Kleine Untergruppen

### 4.1 Die Frattiniuntergruppe

Sei  $G$  eine endliche Gruppe.

**Definition 121** Sei  $U_{\max}(G) := \{U < G : \text{es gibt kein } V \text{ mit } U < V < G\}$  die Menge der maximalen echten Untergruppen von  $G$ .

Sei

$$\Phi(G) := \bigcap_{U \in U_{\max}(G)} U$$

die *Frattiniuntergruppe* von  $G$ .

#### Bemerkung 122

- (1) *Es ist  $\Phi(G) \triangleleft G$ .*
- (2) *Sei  $V \leq G$  mit  $V\Phi(G) = G$  gegeben. Dann ist  $V = G$ .*

*Beweis.*

*Ad (1).* Sei  $\beta \in \text{Aut}(G)$ . Sei  $U \in U_{\max}(G)$ . Dann ist  $U_{\max}(G) \rightarrow U_{\max}(G)$ ,  $U \mapsto \beta(U)$  eine Bijektion. Also ist  $\beta(\Phi(G)) = \bigcap_{U \in U_{\max}(G)} \beta(U) = \bigcap_{\tilde{U} \in U_{\max}(G)} \tilde{U} = \Phi(G)$ .

*Ad (2).* *Annahme*, es ist  $V < G$ . Dann gibt es ein  $U \in U_{\max}(G)$  mit  $V \leq U < G$ . Es ist auch  $\Phi(G) \leq U$ . Also ist  $V\Phi(G) \leq U < G$  und wir haben einen *Widerspruch*.  $\square$

**Lemma 123** *Es ist  $\Phi(G)$  nilpotent.*

*Beweis.* Sei  $p \in \pi(\Phi(G))$  und  $P \in \text{Syl}_p(\Phi(G))$  gegeben. Wir haben  $P \triangleleft \Phi(G)$  zu zeigen; cf. Satz 88.

Es ist  $N_G(P)\Phi(G) = G$ ; cf. Lemma 115. Also ist  $N_G(P) = G$ ; cf. Bemerkung 122.(2). Also ist  $P \triangleleft G$  und somit  $P \triangleleft \Phi(G)$ .  $\square$

**Lemma 124** *Es ist  $\Phi(G/\Phi(G)) = 1$ .*

In diesem Sinne ist es möglich, die Frattinigruppe aus einer Gruppe zu entfernen.

*Beweis.* Es ist  $U_{\max}(G/\Phi(G)) = \{U/\Phi(G) : U \in U_{\max}(G)\}$ , da jede Untergruppe  $U \in U_{\max}(G)$  die Frattiniuntergruppe  $\Phi(G)$  enthält; cf. Aufgabe 17.(1). Also wird

$$\begin{aligned}\Phi(G/\Phi(G)) &= \bigcap_{U \in U_{\max}(G)} (U/\Phi(G)) \\ &= (\bigcap_{U \in U_{\max}(G)} U)/\Phi(G) \\ &= \Phi(G)/\Phi(G) \\ &= 1.\end{aligned}$$

□

**Lemma 125** *Sei  $p > 0$  prim. Sei  $P$  eine  $p$ -Gruppe.*

*Schreibe  $P^p := \langle x^p : x \in P \rangle$ .*

- (1) *Es ist  $P^p \triangleleft P$ .*
- (2) *Es ist  $\Phi(P) = P^{(1)}P^p$ .*
- (3) *Falls  $p = 2$  ist, ist  $\Phi(P) = P^2$ .*
- (4) *Sei  $U \leq P$ . Es ist  $\Phi(U) \leq \Phi(P)$ .*
- (5) *Sei  $N \triangleleft P$ . Es ist  $\Phi(P/N) = \Phi(P)N/N$ .*
- (6) *Sei  $|P/\Phi(P)| =: p^n$ , wobei  $n \geq 0$ . Dann ist  $n = \min\{|S| : S \subseteq P, \langle S \rangle = P\}$ .*

Cf. Aufgabe ??.

*Beweis.*

*Ad (1).* Sei  $\beta \in \text{Aut}(P)$ . 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  $\geq$ .* Sei  $U \in U_{\max}(G)$ . Zu zeigen ist  $P^{(1)}P^p \stackrel{!}{\leq} U$ , i.e.  $P^{(1)} \stackrel{!}{\leq} U$  und  $P^p \stackrel{!}{\leq} U$ .

Es ist  $U < N_P(U) \leq P$ ; cf. Aufgabe 40.(1). Da  $U$  maximale echte Untergruppe von  $P$  ist, folgt  $N_P(U) = P$ , i.e.  $U \triangleleft P$ . 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.  $P/U \simeq C_p$ . Folglich ist  $P^{(1)} \leq U$ ; 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  $P^p \leq U$ .

*Ad*  $\leq$ . 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  $C_p^{\times \ell} \xrightarrow{\sim} P/Q$  wählen, wobei  $\ell \geq 0$ ; cf. Aufgabe 3.(4). Sei  $c_i$  ein Erzeuger des  $i$ -ten direkten Faktors und  $d_i Q$  sein Bild unter diesem Isomorphismus.

Sei  $x \in P \setminus Q$ . Wir haben  $x \notin \Phi(P)$  zu zeigen. Dafür ist zu zeigen, daß es ein  $U \in U_{\max}(P)$  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  $t_j \neq 0$ . Sei  $Q \trianglelefteq U \trianglelefteq P$  mit  $U/Q := \langle d_i : i \in [1, \ell] \setminus \{j\} \rangle$ ; 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  $U \in U_{\max}(P)$ .

*Ad* (3). Dank (2) bleibt  $P^{(1)} \leq P^2$  zu zeigen. Seien  $x, y \in P$ . Es ist  $[x, y] \stackrel{!}{\in} P^2$  zu zeigen. Tatsächlich wird

$$P^2 \ni (x^- y^- x)^2 (x^-)^2 (xy)^2 = x^- y^- x x^- x y x y = x^- y^- x y = [x, y].$$

*Ad* (4). Wir wenden (2) auf  $U$  und  $P$  an. Aus  $U^p \leq P^p$  und  $U^{(1)} \leq P^{(1)}$  folgt

$$\Phi(U) = U^{(1)}U^p \leq P^{(1)}P^p = \Phi(P).$$

*Ad* (5). Wir wenden (2) auf  $P$  und  $P/N$  an. Es wird

$$\Phi(P/N) = (P/N)^{(1)}(P/N)^p = (P^{(1)}N/N)(P^p N/N) = P^{(1)}P^p N/N = \Phi(P)N/N;$$

cf. Aufgabe 13.(1).

*Ad* (6). Wir behaupten

$$\min\{|S| : S \subseteq P, \langle S \rangle = P\} \stackrel{!}{=} \min\{|T| : T \subseteq P/\Phi(P), \langle T \rangle = P/\Phi(P)\}.$$

*Ad*  $\geq$ . Ist  $S \subseteq P$  mit  $\langle S \rangle = P$  gegeben, dann ist mit  $T := \{s\Phi(P) : s \in S\}$  zum einen  $|S| \geq |T|$ , zum anderen  $T \subseteq P/\Phi(P)$  mit  $\langle T \rangle = P/\Phi(P)$ .

*Ad*  $\leq$ . 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 122.(2).

Dies zeigt die *Behauptung*.

Zu zeigen ist nun also  $n \stackrel{!}{=} \min\{|T| : T \subseteq P/\Phi(P), \langle T \rangle = P/\Phi(P)\}$ .

Es ist  $P/\Phi(P) = P/(P^{(1)}P^p) \simeq C_p^{\times n}$ ; 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 126**

- (1) Es ist  $\Phi(S_3) = 1$ , da bereits die maximalen echten Untergruppen  $\langle(1, 2, 3)\rangle$  und  $\langle(1, 2)\rangle$  den Schnitt 1 haben.
- (2) Betrachte  $D_8 = \langle a, b : a^4, b^2, (ab)^2 \rangle$ ; cf. Beispiel 55. Es ist  $D_8^2 = \Phi(D_8)$ ; cf. Lemma 125.(3). Es ist  $\langle a^2 \rangle \leq D_8^2$ . Es ist  $\langle a^2 \rangle \trianglelefteq D_8$  und  $D_8/\langle a^2 \rangle \simeq C_2 \times C_2$ , mithin  $D_8^2 \leq \langle a^2 \rangle$ . Insgesamt ist  $\Phi(D_8) = \langle a^2 \rangle$ .
- (3) Betrachte  $S_4$ . Es ist  $S_3$  eine maximale echte Untergruppe von  $S_4$ ; cf. Beispiel 29. 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  $\Phi(S_4) = 1$ ; cf. Bemerkung 122.(1).
- (4) Sei  $p$  prim. Betrachte  $G = \langle a : a^{p^3} \rangle \simeq C_{p^3}$ . Es ist  $\Phi(G) = \langle a^{p^2} \rangle$ ; cf. Lemma 125.(2). In der Tat ist  $\langle a^{p^2} \rangle$  die einzige maximale Untergruppe von  $G$ .

## 4.2 Eine Bemerkung

**Bemerkung 127** Sei  $G$  eine Gruppe. Sei  $H \trianglelefteq G$ .

Der Gruppenmorphismus

$$\begin{aligned} G &\longrightarrow \text{Aut}(H) \\ g &\longmapsto (h \longmapsto {}^g h) \end{aligned}$$

hat den Kern  $C_G(H) \trianglelefteq G$ . Er induziert somit den injektiven Gruppenmorphismus

$$\begin{aligned} G/C_G(H) &\xrightarrow{\iota} \text{Aut}(H) \\ gC_G(H) &\longmapsto (h \longmapsto {}^g h) \end{aligned}$$

Falls

$$C_G(H) \leq H$$

ist, dann ist  $C_G(H) = C_G(H) \cap H = C_H(H) = Z(H)$ . Wir können unseren injektiven Gruppenmorphismus also

$$\begin{aligned} G/Z(H) &\xrightarrow{\iota} \text{Aut}(H) \\ gZ(H) &\longmapsto (h \longmapsto {}^g h) . \end{aligned}$$

schreiben.

Um  $G$  zu kennen, genügt es **diesenfalls** also,  $Z(H)$  zu kennen, das Bild  $\text{Im}(\iota) \leq \text{Aut}(H)$  zu kennen und die kurz exakte Sequenz

$$Z(H) \hookrightarrow G \xrightarrow{r} \text{Im}(\iota)$$

zu untersuchen, wobei  $r(g) := \iota(gZ(H))$  für  $g \in G$ . Symbolisch wird

$$\begin{array}{c} G \\ | \\ H \\ | \\ Z(H) \\ | \\ 1 \end{array} \Bigg) \leq \text{Aut}(H)$$

### 4.3 Die Fittinguntergruppe

Sei  $G$  eine endliche Gruppe. Schreibe  $k := |\pi(G)|$  und  $\pi(G) = \{p_i : i \in [1, k]\}$ .

**Definition 128** Für  $p \in \pi(G)$  sei

$$O_p(G) := \bigcap_{P \in \text{Syl}_p(G)} P.$$

Sei

$$F(G) := O_{p_1}(G) \cdots O_{p_k}(G)$$

die *Fittinguntergruppe* von  $G$ .

**Bemerkung 129**

- (1) Sei  $p \in \pi(G)$ . Es ist  $O_p(G) \triangleleft G$ .
- (2) Es ist  $F(G) \triangleleft G$ .
- (3) Es ist  $F(G)$  das terminale Element von  $\{N \triangleleft G : N \text{ ist nilpotent}\}$ .  
Kurz, für  $N \triangleleft G$  ist  $N$  genau dann nilpotent, wenn  $N \leq F(G)$  ist.
- (4) Es ist  $\Phi(G) \leq F(G)$ .

*Beweis.*

*Ad (1).* Sei  $\beta \in \text{Aut}(G)$ . Es ist  $\text{Syl}_p(G) \rightarrow \text{Syl}_p(G), P \mapsto \beta(P)$  wohldefiniert und bijektiv. Damit folgt

$$\beta(O_p(G)) = \bigcap_{P \in \text{Syl}_p(G)} \beta(P) = \bigcap_{\tilde{P} \in \text{Syl}_p(G)} \tilde{P} = O_p(G).$$

*Ad (2).* Allgemein ist in einer Gruppe  $H$  mit  $N, \tilde{N} \triangleleft H$  auch  $N\tilde{N} \triangleleft H$ , da für  $\beta \in \text{Aut}(H)$  sich  $\beta(N\tilde{N}) = \beta(N) \cdot \beta(\tilde{N}) = N\tilde{N}$  ergibt; cf. Aufgabe 12.(2,3).

Daher folgt  $F(G) \triangleleft G$  aus (1).

*Ad (3).* Wir behaupten, daß  $F(G)$  nilpotent ist. Sei  $p \in \pi(G)$ . Wir müssen zeigen, daß  $|\text{Syl}_p(F(G))| \stackrel{!}{=} 1$  ist; cf. Satz 88. Es genügt zu zeigen, daß es eine  $p$ -Sylowgruppe in  $F(G)$  gibt, die normal in  $F(G)$  liegt; cf. Satz 37.(2).

Sei o.E.  $p = p_k$ ; cf. Aufgabe 12.(2). Schreibe  $F'(G) := O_{p_1}(G) \cdots O_{p_{k-1}}(G)$ . Es ist  $|F'(G)|$  ein Teiler von  $|O_{p_1}(G)| \cdots |O_{p_{k-1}}(G)|$ , wie eine iterierte Anwendung von Aufgabe 12.(2) ergibt, und also nicht durch  $p$  teilbar. Somit ist  $F(G)/O_p(G) = F'(G)O_p(G)/O_p(G) \simeq F'(G)/(F'(G) \cap O_p(G))$  von Ordnung teilerfremd zu  $p$ ; cf. Aufgabe 12.(2). Also ist  $O_p(G)$  eine  $p$ -Sylowgruppe von  $F(G)$ . Aus  $O_p(G) \triangleleft G$  folgt  $O_p(G) \triangleleft F(G)$ ; cf. (1). Dies zeigt die Behauptung; cf. Satz 88.

Sei andererseits  $N \triangleleft G$  mit  $N$  nilpotent gegeben. Wir haben  $N \stackrel{!}{\leq} F(G)$  zu zeigen.

Es ist  $|\text{Syl}_p(N)| = 1$  für  $p \in \pi(N)$  und auch für  $p \in \pi(G) \setminus \pi(N)$ ; cf. Satz 88. Schreibe also  $\text{Syl}_p(N) = \{Q_p\}$  für  $p \in \pi(G)$ . Es ist  $\prod_{i \in [1, k]} Q_{p_i} \xrightarrow{\sim} N$ ,  $(q_i)_i \mapsto q_1 \cdots q_k$ ; cf. Satz 88. Insbesondere ist  $N = Q_{p_1} \cdots Q_{p_k}$ .

Sei  $p \in \pi(G)$ . Wir haben nun  $Q_p \stackrel{!}{\leq} F(G)$  zu zeigen. Es genügt,  $Q_p \stackrel{!}{\leq} O_p(G)$  zu zeigen. Es ist  $Q_p = O_p(N) \triangleleft N \triangleleft G$  und also  $Q_p \triangleleft G$ ; cf. Bemerkung 129.(1). Es ist  $Q_p \leq P$  für ein  $P \in \text{Syl}_p(G)$ ; cf. Satz 37.(4). Für jedes  $\tilde{P} \in \text{Syl}_p(G)$  gibt es ein  $g \in G$  mit  $\tilde{P} = {}^gP$ , cf. Satz 37.(2), es wird also  $Q_p = {}^gQ_p \leq {}^gP = \tilde{P}$ . Somit ist in der Tat  $Q_p \leq \bigcap_{\tilde{P} \in \text{Syl}_p(G)} \tilde{P} = O_p(G)$ .

*Ad (4).* Es ist  $\Phi(G)$  nilpotent; cf. Lemma 123. Es ist  $\Phi(G) \triangleleft G$ ; cf. Bemerkung 122.(1). Also ist  $\Phi(G) \leq F(G)$ ; cf. (3). □

### Beispiel 130

- (1) Es ist  $O_2(S_3) = 1$ . Es ist  $O_3(S_3) = \langle (1, 2, 3) \rangle = A_3$ . Also ist  $F(S_3) = A_3$ . Es ist  $F(S_3/F(S_3)) > 1$ . Cf. auch Beispiel 126.(1) und Lemma 124.
- (2) Es ist  $O_2(S_4) = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle =: V$ . Es ist  $O_3(S_4) = 1$ . Also ist  $F(S_4) = V$ . Cf. auch Beispiel 126.(3).
- (3) Sei  $n \geq 5$ . Unter den Normalteilern  $1, A_n, S_n$  von  $S_n$  ist nur  $1$  nilpotent; cf. Aufgabe 20.(3), Beispiel 76.(3). Also ist  $F(S_n) = 1$ ; cf. Bemerkung 129.(3).
- (4) Sei  $N$  nilpotent. Es ist  $F(N) = N$ , da  $F(N)$  der terminale nilpotente Normalteiler von  $N$  ist; cf. Bemerkung 129.(3). Cf. auch Lemma 125.(2).

**Lemma 131** Sei  $G$  eine endliche Gruppe. Schreibe  $C := C_G(F(G))$ .

- (1) Ist  $G$  auflösbar und ist  $F(G) = 1$ , dann ist auch  $G = 1$ .
- (2) Es ist  $F(C/(C \cap F(G))) = 1$ .

*Beweis.*

*Ad (1).* *Annahme,* es ist  $G > 1$ . Also gibt es ein  $i \geq 0$  mit  $G^{(i)} > 1$  und  $G^{(i+1)} = 1$ ; cf. Satz 83. Somit ist  $G^{(i)}$  ein abelscher Normalteiler von  $G$ ; cf. Bemerkung 81.(2). Also ist  $1 < G^{(i)} \leq F(G)$ ; cf. Bemerkung 129.(3), Bemerkung 75. Wir haben einen *Widerspruch*.

*Ad (2).* Schreibe  $F(C/(C \cap F(G))) =: U/(C \cap F(G))$  mit  $C \cap F(G) \trianglelefteq U \trianglelefteq C$ ; cf. Aufgabe 17.(1,2). Wir haben  $U \stackrel{!}{\leq} F(G)$  zu zeigen. Dank Bemerkung 129.(3) genügt es hierfür zu zeigen, daß  $U$  ein nilpotenter Normalteiler von  $G$  ist.

Es ist  $C = C_G(F(G)) \trianglelefteq G$ , da  $F(G) \trianglelefteq G$  ist; cf. Bemerkungen 17 und 129.(2).

Es ist  $U/(C \cap F(G)) \trianglelefteq C/(C \cap F(G)) \trianglelefteq G/(C \cap F(G))$ ; cf. Bemerkung 129.(2). Also ist  $U/(C \cap F(G)) \trianglelefteq G/(C \cap F(G))$ ; cf. Bemerkung 79.(2). Somit ist  $U \trianglelefteq G$ .

Für  $x \in C \cap F(G) \leq F(G)$  ist für  $u \in U \leq C = C_G(F(G))$  dann  ${}^u x = x$ , aber auch  $x \in U$ , also insgesamt  $x \in Z(U)$ . Somit ist  $C \cap F(G) \leq Z(U)$ .

Es ist  $U/(C \cap F(G)) = F(C/(C \cap F(G)))$  nilpotent; cf. Bemerkung 129.(3).

Hieraus folgt  $U$  nilpotent; cf. Aufgabe 32.(6). □

### Satz 132 (Zentralisator der Fittinguntergruppe)

*Sei  $G$  eine auflösbare endliche Gruppe.*

*Es ist  $C_G(F(G)) \leq F(G)$ .*

Damit sind wir in der Situation, die in Bemerkung 127 beschrieben wird.

*Beweis.* Schreibe  $C := C_G(F(G))$ . Es ist  $F(G) \trianglelefteq G$ ; cf. Bemerkung 129.(2). Also ist  $C \trianglelefteq G$ ; cf. Bemerkung 17.

Es genügt,  $C/(C \cap F(G)) \stackrel{!}{=} 1$  zu zeigen.

Da  $G$  auflösbar ist, gilt dies auch für  $C$  und damit für  $C/(C \cap F(G))$ ; cf. Aufgabe 32.(2). Somit genügt es,  $F(C/(C \cap F(G))) \stackrel{!}{=} 1$  zu zeigen; cf. Lemma 131.(1). Dies aber folgt mit Lemma 131.(2). □

**Beispiel 133** Betrachte  $S_4$ . Es ist  $S_4$  auflösbar; cf. Aufgabe 30, Bemerkung 73.(1). Es ist  $F(S_4) = \langle \underbrace{(1, 2)(3, 4)}_{=: a}, \underbrace{(1, 3)(2, 4)}_{=: b} \rangle =: V$ ; cf. Beispiel 130.(2).

Es ist  $C_{S_4}(V) \leq V$ ; cf. Satz 132. Da  $V$  abelsch ist, ist also  $C_{S_4}(V) = Z(V) = V$ . Somit ist  $V$  der Kern des Gruppenmorphismus

$$\begin{array}{ccc} S_4 & \longrightarrow & \text{Aut}(V) \\ \sigma & \longmapsto & (v \mapsto {}^\sigma v) \end{array}$$



Wir haben den Isomorphismus

$$\begin{aligned} \mathrm{GL}_2(\mathbf{F}_2) &\xrightarrow{\simeq} \mathrm{Aut}(V) \\ \begin{pmatrix} i+2\mathbf{Z} & j+2\mathbf{Z} \\ k+2\mathbf{Z} & \ell+2\mathbf{Z} \end{pmatrix} &\mapsto (a \mapsto a^i b^k, b \mapsto a^j b^\ell). \end{aligned}$$

Insbesondere ist  $|\mathrm{Aut}(V)| = 6$ . Somit ist der induzierte injektive Gruppenmorphismus

$$\begin{aligned} \mathrm{S}_4/V &\xrightarrow{\iota} \mathrm{Aut}(V) \\ \sigma V &\mapsto (v \mapsto \sigma v) \end{aligned}$$

auch surjektiv, zusammen also ein Isomorphismus. Cf. Bemerkung 127.

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 134** *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  $G^{(1)} \leq G^{(2)}$ ; cf. Aufgabe 13.(4). Insgesamt ist also  $G^{(1)} = G^{(2)}$ .  $\square$

**Definition 135** Es heißt  $G$  *quasieinfach*, wenn  $G$  perfekt ist und  $G/Z(G)$  einfach ist.

Insbesondere ist  $G/Z(G)$  dann nichtabelsch, da ansonsten  $G$  auflösbar und  $> 1$  und also nicht perfekt wäre; cf. Aufgabe 32.(1), Satz 83.

Somit ist  $G$  dann nichtauflösbar; cf. Aufgabe 32.(2), Bemerkung 73.(1).

**Beispiel 136** Sei  $F$  ein Körper. Sei  $n \geq 2$ . Sei  $(n, |F|) \notin \{(2, 2), (2, 3)\}$ .

Es ist  $\mathrm{SL}_n(F)$  quasieinfach; cf. Aufgabe 18.(1, 2), Satz 47.

**Definition 137** Sei  $H \leq G$ . Es heißt  $H$  *subnormal* in  $G$ , geschrieben  $H \trianglelefteq\trianglelefteq G$ , wenn es  $s \geq 0$  und  $U_i \leq G$  für  $i \in [0, s]$  gibt mit

$$H = U_s \trianglelefteq U_{s-1} \trianglelefteq \dots \trianglelefteq U_1 \trianglelefteq U_0 = G.$$

**Bemerkung 138** Sei  $G$  *quasieinfach*. Sei  $H \trianglelefteq\trianglelefteq G$ . Dann ist  $H \leq Z(G)$  oder  $H = G$ .

*Beweis.* Es ist auch  $HZ(G) \trianglelefteq\trianglelefteq G$  und also  $HZ(G)/Z(G) \trianglelefteq\trianglelefteq G/Z(G)$ . Da aber  $G/Z(G)$  einfach ist, ist  $HZ(G) = Z(G)$  oder  $HZ(G) = G$ . Ersterenfalls ist  $H \leq Z(G)$ . Letzterenfalls ist  $HZ(G) = G$ , also  $H \trianglelefteq HZ(G) = G$  und  $G/H = HZ(G)/H \simeq Z(G)/H \cap Z(G)$  abelsch, was  $G = G^{(1)} \leq H \leq G$  und also  $H = G$  zur Folge hat; cf. Aufgabe 13.(4).  $\square$

**Bemerkung.** Sei  $H \trianglelefteq\trianglelefteq G$ . Dann ist  $F(H) \leq F(G)$ .

*Beweis.* Dank möglicher Iteration genügt es, die Aussage im Falle  $H \trianglelefteq G$  zu zeigen.

Aus  $F(H) \triangleleft H \trianglelefteq G$  folgt  $F(H) \trianglelefteq G$ ; cf. Bemerkungen 129.(2) und 79.(2). Da zudem  $F(H)$  nilpotent ist, folgt  $F(H) \leq F(G)$ ; cf. Bemerkung 129.(3).  $\square$

### Definition 139

Es heißt  $K \leq G$  eine *Komponente* von  $G$ , wenn  $K$  quasieinfach und  $K \trianglelefteq\trianglelefteq G$  ist.

Sei  $\text{Komp}(G) := \{ K \leq G : K \text{ ist Komponente von } G \}$ .

**Bemerkung 140** Sei  $K \in \text{Komp}(G)$ .

- (1) Sei  $K \leq H \leq G$ . Dann ist  $K \in \text{Komp}(H)$ .
- (2) Sei  $K \not\leq N \trianglelefteq G$ . Dann ist  $KN/N \in \text{Komp}(G/N)$ .
- (3) Ist  $G \trianglelefteq\trianglelefteq \tilde{G}$ , dann ist  $K \in \text{Komp}(\tilde{G})$ .

*Beweis.*

*Ad (1).* Zu zeigen ist  $K \trianglelefteq\trianglelefteq H$ . Aber ist  $K = U_s \trianglelefteq \dots \trianglelefteq U_0 = G$ , dann ist auch  $K = K \cap H = U_s \cap H \trianglelefteq \dots \trianglelefteq U_0 \cap H = G \cap H = H$ .

*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  $K = U_s \trianglelefteq \dots \trianglelefteq U_0 = G$ , dann ist auch  $KN = U_s N \trianglelefteq \dots \trianglelefteq U_0 N = GN = N$ ; beachte hierbei für  $i \in [1, s]$ , für  $u_i \in U_i$  und  $n \in N$ , daß  ${}^n u_i = u[u^-, n] \in U_i N$  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  $(K/(K \cap N))/Z(K/(K \cap N))$  einfach ist. Schreibe  $Z(K/(K \cap N)) = Z/(K \cap N)$  mit  $K \cap N \trianglelefteq Z \trianglelefteq K$ . Es ist  $Z(K) \leq Z$ . Also ist  $Z = Z(K)$  oder  $Z = K$ ; cf. Bemerkung 138. 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  $K \leq N$ , was *nicht* der Fall ist. Somit ist  $Z = Z(K)$ .

Es folgt, daß  $(K/(K \cap N))/Z(K/(K \cap N)) = (K/(K \cap N))/(Z(K)/(K \cap N)) \simeq K/Z(K)$  eine einfache Gruppe ist.  $\square$

*Ad* (3). Subnormalität ist transitiv.  $\square$

**Lemma 141** *Seien  $Z \leq Z(G) \leq G$ . Sei  $E \leq G$ . Sei  $EZ/Z \in \text{Komp}(G/Z)$ .*

*Dann ist  $E^{(1)} \in \text{Komp}(G)$ .*

*Beweis.* Aus  $EZ/Z \trianglelefteq G/Z$  folgt  $E^{(1)} \trianglelefteq E \trianglelefteq EZ \trianglelefteq G$ .

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 134.

Bleibt zu zeigen, daß  $E^{(1)}/Z(E^{(1)})$  einfach ist. Sei  $Z(E^{(1)}) \trianglelefteq N \trianglelefteq E^{(1)}$ . Es ist zu zeigen, daß  $N = E^{(1)}$  oder  $Z(E^{(1)}) = N$  ist; cf. Aufgabe 17.(3).

Es ist  $NZ \trianglelefteq E^{(1)}Z$  und also  $NZ/Z \trianglelefteq E^{(1)}Z/Z = EZ/Z$ . Da  $EZ/Z$  quasieinfach ist, folgt  $NZ/Z \leq Z(EZ/Z)$  oder  $NZ/Z = EZ/Z$ ; cf. Bemerkung 138.

Letzterenfalls ist  $N \leq E^{(1)} \leq E \leq NZ$ , also  $N(Z \cap E^{(1)}) = NZ \cap E^{(1)} = E^{(1)}$ ; cf. Bemerkung 116. Da  $E^{(1)}/N = N(Z \cap E^{(1)})/N \simeq (Z \cap E^{(1)})/(Z \cap E^{(1)} \cap N)$  abelsch ist, folgt  $E^{(1)} = E^{(2)} \leq N \leq E^{(1)}$ , also  $N = E^{(1)}$ ; cf. Aufgabe 13.(4).

Ersterenfalls ist  $NZ/Z \leq Z(EZ/Z) = Z(E^{(1)}Z/Z)$  und also  $[N, E^{(1)}] \leq Z$ . 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  $N \leq Z(E^{(1)})$ . Insgesamt ist  $Z(E^{(1)}) = N$ .  $\square$

**Lemma 142** *Sei  $K \in \text{Komp}(G)$ . Sei  $L \trianglelefteq G$ .*

*Dann ist  $K \leq L$  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  $K \in \text{Komp}(G)$  und  $L \trianglelefteq G$  mit  $K \not\leq L$  und  $[K, L] > 1$ .

Ist  $K = G$ , dann ist  $G$  quasieinfach und also  $L \leq Z(G)$  oder  $L = G$ ; cf. Bemerkung 138. Ersterenfalls ist  $[K, L] = 1$ , zweiterenfalls ist  $K \leq G$ . Dies tritt also nicht auf, i.e. es ist  $K < G$ . Somit gibt es  $K \trianglelefteq N \triangleleft G$ .

Ist  $L = G$ , dann ist  $K \leq L$ . Dies tritt also nicht auf, i.e. es ist  $L < G$ . Somit gibt es  $L \trianglelefteq N \triangleleft G$ .

Daher ist  $L' := [L, K] \leq N \cap M$ . Ferner ist  $K \leq N_M([L, K]) = N_M(L') =: G'$ ; cf. Aufgabe ??.(5).

Es ist  $K \in \text{Komp}(G')$ ; cf. Bemerkung 140.(1). Es ist  $L' \trianglelefteq G'$ , also  $L' \trianglelefteq\trianglelefteq G'$ . Wegen der Minimalität von  $|G|$  und wegen  $|G'| \leq |M| < |G|$  folgt nun  $K \leq L'$  oder  $[K, L'] = 1$ .

Ersterenfalls folgt  $K \leq L' \leq N$  und also  $K \in \text{Komp}(N)$  ist; cf. Bemerkung 140.(1). Ferner ist  $L \trianglelefteq\trianglelefteq N$ . Wegen der Minimalität von  $|G|$  und wegen  $|N| < |G|$  liefert dies  $K \leq L$  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).  $\square$

**Korollar 143** Seien  $K, \tilde{K} \in \text{Komp}(G)$ .

Dann ist  $K = \tilde{K}$  oder  $[K, \tilde{K}] = 1$ .

*Beweis.* Sei  $[K, \tilde{K}] > 1$ . Zu zeigen ist  $K \stackrel{!}{=} \tilde{K}$ . Wegen Symmetrie genügt es,  $K \stackrel{!}{\leq} \tilde{K}$  zu zeigen. Dies aber folgt wegen  $[K, \tilde{K}] > 1$  aus Lemma 142.  $\square$

**Definition 144** Sei  $t := |\text{Komp}(G)|$ . Schreibe  $\text{Komp}(G) = \{K_i : i \in [1, t]\}$ .

Sei  $E(G) := K_1 K_2 \cdots K_t \cdot 1$  die *Schicht* von  $G$ .

Sei  $\text{FE}(G) := F(G)E(G)$  die *erweiterte Fittinguntergruppe* von  $G$ ; cf. Definition 128.

Oft wird  $\text{FE}(G)$  auch  $F^*(G)$  geschrieben und als *verallgemeinerte Fittinguntergruppe* bezeichnet.

**Bemerkung 145**

- (1) Es ist  $E(G) \triangleleft G$ . Es ist  $K \trianglelefteq E(G)$  für  $K \in \text{Komp}(G)$ .
- (2) Ist  $G$  auflösbar, dann ist  $\text{Komp}(G) = \emptyset$ , sowie  $E(G) = 1$  und  $\text{FE}(G) = F(G)$ .
- (3) Es ist  $[E(G), F(G)] = 1$ .
- (4) Es ist  $\text{FE}(G) \triangleleft G$ .

*Beweis.*

*Ad (1).* Wir haben den Gruppenmorphismus  $\prod_{i \in [1, t]} K_i \rightarrow G, (k_i)_i \mapsto k_1 k_2 \cdots k_t$ ; cf. Aufgabe 2.(3), Korollar 143. Sein Bild ist die Untergruppe  $E(G) \leq G$ ; cf. auch Aufgabe 12.

Sei  $\beta \in \text{Aut}(G)$ . Sei  $i \in [1, t]$ . Es genügt,  $\beta(K_i) \stackrel{!}{\leq} E(G)$  zu zeigen. Es genügt,  $\beta(K_i) \stackrel{!}{\in} \text{Komp}(G)$  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  $\beta(K_i)^{(1)} \stackrel{\text{A. 13.(1)}}{=} \beta(K_i^{(1)}) = \beta(K_i)$  und  $\beta(K_i)/Z(\beta(K_i)) = \beta(K_i)/\beta(Z(K_i))$  ist isomorph zu  $K_i/Z(K_i)$  via des von  $\beta$  induzierten Isomorphismus, mithin einfach. Also ist  $\beta(K_i)$  tatsächlich eine Komponente von  $G$ .

Sei nun  $K \in \text{Komp}(G)$ . Wir haben  $K \stackrel{!}{\trianglelefteq} E(G)$  zu zeigen. Sei  $\tilde{K} \in \text{Komp}(G)$ . Sei  $\tilde{x} \in \tilde{K}$ . Sei  $y \in K$ . Wir haben  $\tilde{x}y \stackrel{!}{\in} K$  zu zeigen. Ist  $\tilde{K} = K$ , so folgt dies aus  $K \leq G$ . Ist  $\tilde{K} \neq K$ , dann ist  $[K, \tilde{K}] = 1$  dank Korollar 143 und also  $\tilde{x}y = y \in K$ .

*Ad (2).* Sei  $G$  auflösbar. Wir haben  $\text{Komp}(G) = \emptyset$  zu zeigen. Wäre  $K \in \text{Komp}(G)$ , dann wäre wegen  $K \leq G$  auch  $K$  auflösbar dank Aufgabe 32.(2), was *nicht so ist*. Da  $K \leq G$ , ist  $K$  auflösbar.

*Ad (3).* Ist  $E(G) = 1$ , so ist nichts zu zeigen.

Sei also  $E(G) > 1$ . Dann können wir  $K \in \text{Komp}(G)$  wählen. *Annahme*, es ist  $E(G) \leq F(G)$ . Dann ist  $K \leq F(G)$  und somit  $K \in \text{Komp}(F(G))$ ; cf. Bemerkung 140.(1). Aber  $F(G)$  ist nilpotent und also auflösbar; cf. Bemerkungen 129.(3) und 75. Also ist  $\text{Komp}(F(G)) = \emptyset$ . Wir haben einen *Widerspruch*. Also ist  $E(G) \not\leq F(G)$ .

Da  $F(G) \triangleleft G$ , ist insbesondere  $F(G) \triangleleft\triangleleft G$ ; cf. Bemerkung 129.(2). Mit Lemma 142 folgt  $[E(G), F(G)] = 1$ .

*Ad (4).* Da  $F(G) \triangleleft G$  und  $E(G) \triangleleft G$ , ist  $FE(G) = F(G)E(G) \triangleleft G$ ; cf. Beweis zu Bem78.(2). □

### Lemma 146

- (1) *Ist  $N$  minimal in  $\{M \triangleleft G : M > 1\}$ , dann ist  $N \leq FE(G)$ .*
- (2) *Ist  $K \in \text{Komp}(G)$  und ist  $Z(K) = 1$ , dann ist das Normalteilererzeugnis  ${}^G\langle K \rangle$  minimal in  $\{M \triangleleft G : M > 1\}$ .*
- (3) *Ist  $G > 1$ , dann ist  $FE(G) > 1$ .*

Cf. Aufgabe 37.

*Beweis.*

*Ad (1).* Ist  $N$  abelsch, so ist  $N$  nilpotent und also  $N \triangleleft F(G) \leq FE(G)$ ; cf. Bemerkungen 75 und 129.(3).

Sei nun  $N$  nichtabelsch. Gemäß Aufgabe 37.(1,2) gibt es einen Isomorphismus  $f : S^{\times k} \xrightarrow{\sim} N$  für ein  $k \geq 1$  und eine einfache Gruppe  $S$ . Sei

$$S_j := \{(s_i)_i \in S^{\times k} : s_i = 1 \text{ für } i \in [1, k] \setminus \{j\}\}$$

für  $j \in [1, k]$ . Für  $j \in [1, k]$  ist  $S_j \triangleleft S^{\times k}$ , also  $f(S_j) \triangleleft N$  und somit  $f(S_j) \triangleleft\triangleleft N$ ; da  $f(S_j)$  einfach und nichtabelsch ist, ist  $f(S_j)$  zudem perfekt; insgesamt  $f(S_j) \in \text{Komp}(G)$ . Es folgt  $N = f(S) = f(\langle S_j : j \in [1, k] \rangle) \leq E(G) \leq FE(G)$ .

*Ad (2).* Nach Konstruktion ist  $N := {}^G\langle K \rangle \triangleleft G$ .

Sei  $G = \sqcup_{i \in [1, \ell]} g_i N_G(K)$ , wobei  $\ell := [G : N_G(K)]$  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  ${}^iK$  eine Komponente von  $G$  ist, folgt  $[{}^iK, {}^jK] = 1$ ; cf. Korollar 143. Somit gibt es einen surjektiven Gruppenmorphismus  $u : K^{\times \ell} \rightarrow G$ ,  $(x_i)_i \mapsto {}^{g_1}x \cdot {}^{g_2}x \cdots {}^{g_\ell}x$ ; cf. Aufgabe 2.(3). Ferner ist  ${}^iK \trianglelefteq N$  für  $i \in [1, k]$ .

Sei  $i \in [1, k]$ . *Annahme*, es ist  ${}^iK \leqslant {}^{g_1}K \cdots {}^{g_{i-1}}K =: L$ . Da  $[{}^iK, L] = 1$  ist, folgt  ${}^iK \leqslant Z({}^{g_1}K \cdots {}^{g_{i-1}}K)$ . Aber  $K$  ist nichtabelsch. Wir haben einen *Widerspruch*. Es folgt  ${}^iK \not\leqslant L$ , i.e.  ${}^iK \cap L \triangleleft {}^iK$ . Da  ${}^iK$  einfach ist, folgt  ${}^iK \cap L = 1$ .

Also ist  $u$  ein Isomorphismus; cf. Lösung zu Aufgabe 2.(3).

Sei nun  $M \trianglelefteq G$  mit  $1 < M \leqslant N$  gegeben. Wir haben  $M \stackrel{!}{=} N$  zu zeigen. Es genügt,  ${}^gK \stackrel{!}{\leqslant} M$  zu zeigen für ein  $g \in G$ , da daraus wegen  $M \trianglelefteq G$  dann  ${}^gK \leqslant M$  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

$$K_j := \{(x_i)_i : x_i = 1 \text{ für } i \in [1, \ell] \setminus \{j\}\} \leqslant u^{-1}(M);$$

cf. Aufgabe 37.(3). Folglich ist  ${}^jK = u(K_j) \leqslant M$ .

*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  $\text{FE}(G) \geqslant N > 1$ .  $\square$

**Lemma 147** *Sei  $H \trianglelefteq G$ . Dann ist  $E(H) \leqslant E(G)$  und  $\text{FE}(H) \leqslant \text{FE}(G)$ .*

*Beweis.* Es ist  $F(H) \leqslant F(G)$ ; cf. Bemerkung oben. Also genügt es,  $E(H) \stackrel{!}{\leqslant} E(G)$  zu zeigen.

Sei  $K \in \text{Komp}(H)$ . Wir haben  $K \stackrel{!}{\leqslant} E(G)$  zu zeigen. Aber in der Tat ist  $K \in \text{Komp}(G)$  und somit  $K \leqslant E(G)$ ; cf. Bemerkung 140.(3).  $\square$

### Satz 148 (Zentralisator der erweiterten Fittinguntergruppe)

*Wir erinnern an die endliche Gruppe  $G$  und an ihre erweiterte Fittinguntergruppe  $\text{FE}(G)$ ; cf. Definition 144.*

*Es ist  $C_G(\text{FE}(G)) \leqslant \text{FE}(G)$ .*

Damit sind wir in der Situation, die in Bemerkung 127 beschrieben wird.

Cf. Satz 132 und Bemerkung 145.(4).

*Beweis.* Schreibe  $C := C_G(\text{FE}(G))$ . Da  $\text{FE}(G) \trianglelefteq G$ , ist  $C \trianglelefteq G$ ; cf. Bemerkungen 145.(4) und 17. Also ist  $\text{FE}(C) \leqslant \text{FE}(G)$ ; cf. Lemma 147.

Es ist  $Z := Z(C) \trianglelefteq C$  abelsch, mithin nilpotent und somit  $Z \leqslant F(C) \leqslant \text{FE}(C)$ ; cf. Bemerkung 129.(3).

Es genügt,  $\text{FE}(C/Z) \stackrel{!}{=} 1$  zu zeigen, da dann  $C/Z = 1$ , i.e.  $C \leq Z$  folgt, was  $C \leq \text{FE}(G)$  nach sich zieht.

Für  $x \in \text{FE}(C)$  und  $c \in C$  ist  $x \in \text{FE}(G)$  und also  $[x, c] = 1$ . Somit ist  $\text{FE}(C) \leq Z$ . Insgesamt ist also  $\text{FE}(C) = Z$ .

Schreibe  $\text{F}(C/Z) = N/Z$  mit  $Z \triangleleft N \triangleleft C$ ; cf. Aufgabe 17.(3). Mit  $N/Z$  ist auch  $N$  nilpotent; cf. Bemerkung 129.(3), Aufgabe 32.(6). Also ist  $Z \leq N \leq \text{F}(C) = Z$  und somit  $N = Z$ , i.e.  $\text{F}(C/Z) = N/Z = 1$ ; cf. Bemerkung 129.(3).

Es bleibt  $\text{E}(C/Z) \stackrel{!}{=} 1$  zu zeigen, i.e.  $\text{Komp}(C/Z) \stackrel{!}{=} \emptyset$ . *Annahme*, es gibt  $K \in \text{Komp}(C/Z)$ . Schreibe  $K = L/Z$  mit  $Z \leq L \leq C$ ; cf. Aufgabe 17.(1). Es ist  $L^{(1)} \in \text{Komp}(C)$ ; cf. Lemma 141. Es ist  $L^{(1)} > 1$  perfekt, also nichtabelsch. Andererseits ist  $L^{(1)} \leq \text{FE}(C) = Z$ , was wegen  $Z$  abelsch auch  $L^{(1)}$  abelsch nach sich zieht. Wir haben einen *Widerspruch*.  $\square$

**Beispiel 149** Sei  $Q$  eine quasiainfache endliche Gruppe; cf. e.g. Beispiel 136.

Sei  $H$  eine endliche Gruppe. Sei  $m \geq 1$ . Sei  $\beta : H \rightarrow S_m$  ein Gruppenmorphismus, mittels dessen  $[1, m]$  zu einer  $H$ -Menge wird; cf. Beispiel 2.(2).

Sei  $\text{Kern}(\beta)$  als auflösbar vorausgesetzt.

Wir bilden das Kranzprodukt

$$G := Q \wr_{\beta} H ;$$

cf. Definition 96.

Schreibe  $Q_j := \{ ((q_i)_i, h) \in G : q_i = 1 \text{ für } i \in [1, m] \setminus \{j\}, \text{ sowie } h = 1 \}$  für  $j \in [1, m]$ .

Schreibe  $N := \{ ((q_i)_i, h) \in G : h = 1 \}$ .

Schreibe  $B := \{ ((q_i)_i, h) \in G : q_i = 1 \text{ für } i \in [1, m], \text{ sowie } h \in \text{Kern}(\beta) \}$ .

Sei  $j \in [1, m]$ . Es ist  $Q_j \triangleleft N \triangleleft G$ . Folglich ist  $Q_j \triangleleft\triangleleft G$ . Desweiteren ist  $Q_j \xrightarrow{\sim} Q$ ,  $((q_i)_i, h) \mapsto q_j$ . Also ist  $Q_j \in \text{Komp}(G)$ .

Insgesamt folgt  $\{ Q_i : i \in [1, m] \} \leq \text{Komp}(G)$ .

Es ist  $B \xrightarrow{\sim} \text{Kern}(\beta)$ ,  $((q_i)_i, h) \mapsto h$ . Also ist  $B$  auflösbar.

Es ist  $B \leq C_G(N)$ . Also ist  $NB \leq G$ ; cf. Aufgabe 12.(2). Es ist auch  $B \leq C_G(Z(N))$ . Also ist auch  $Z(N)B \leq G$ .

Wir *behaupten*, es ist  $C_G(N) = Z(N)B$ . Zu zeigen ist nur  $C_G(N) \stackrel{!}{\leq} Z(N)B$ . Sei  $((q_i)_i, h) \in C_G(N)$ . Wir haben  $\beta(h) \stackrel{!}{=} \text{id}$  und  $q_i \stackrel{!}{\in} Z(Q)$  für  $i \in [1, m]$  zu zeigen.

*Annahme*, es gibt  $k \in [1, m]$  mit  $h \cdot k \neq k$ . Wähle  $x \in Q \setminus \{1\}$ . Betrachte  $n := ((1, \dots, 1, x, 1, \dots, 1), 1) \in N$ , wobei der Eintrag  $x$  sich an Position  $k$  des Tupels befinde. Es ist

$$((1, \dots, 1, x, 1, \dots, 1), 1) \cdot ((q_i)_i, h) = ((q_1, \dots, q_{k-1}, xq_k, q_{k+1}, \dots, q_m), h)$$

und

$$((q_i)_i, h) \cdot ((1, \dots, 1, x, 1, \dots, 1), 1) = ((q_1, \dots, q_{h \cdot k - 1}, q_{h \cdot k} x, q_{h \cdot k + 1}, \dots, q_m), h).$$

Da  $h \cdot k \neq k$ , folgt  $xq_k = q_k$  und also  $x = 1$ . Wir haben einen *Widerspruch*. Somit ist  $\beta(h) = \text{id}$ .

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  $q_i \in Z(Q)$  für  $i \in [1, n]$ . Dies zeigt die *Behauptung*.

Insbesondere ist  $C_G(N) = Z(N)B$  auflösbar; cf. Aufgabe 32.(3).

Gäbe es ein  $K \in \text{Komp}(G)$  mit  $K \notin \{Q_i : i \in [1, m]\}$ , so wäre  $[K, Q_i] = 1$  für  $i \in [1, m]$  dank Korollar 143 und also  $K \leq C_G(N) = Z(N)B$ , was aber wegen  $K$  nichtauflösbar *nicht geht*; cf. Aufgabe 32.(2).

Also ist  $\text{Komp}(G) = \{Q_i : i \in [1, m]\}$  und somit

$$E(G) = N.$$

Es ist  $[Z(N), B] = 1$  und  $Z(N) \cap B = 1$ , also  $Z(N) \times B \xrightarrow{\sim} Z(N)B$ ,  $(z, b) \mapsto zb$ ; cf. Aufgabe 2.(3). Es ist  $F(Z(N) \times B) = F(Z(N)) \times F(B) = Z(N) \times F(B)$ ; cf. Beispiel 130.(4), UeXXX. Also ist auch  $F(Z(N)B) = Z(N)F(B)$ .

Es ist  $Z(N) \trianglelefteq N \trianglelefteq G$ , also  $Z(N) = F(Z(N)) \leq F(G)$ ; cf. Bemerkung 75, Beispiel 130.(4), Bemerkung oben.

Es ist  $B \trianglelefteq Z(N)B = C_G(N) \trianglelefteq G$ ; cf. Bemerkung 17. Also ist  $F(B) \leq F(G)$ ; cf. Bemerkung oben.

Zusammen ist  $Z(N)F(B) \leq F(G)$ .

Da  $1 = [E(G), F(G)] = [N, F(G)]$  nach Bemerkung 145.(3) und da  $F(G) \trianglelefteq G$  nach Bemerkung 129.(2), ist  $F(G) \trianglelefteq C_G(N) = Z(N)B$ . Es folgt  $F(G) \leq F(Z(N)B) = Z(N)F(B)$ ; cf. Bemerkung oben.

Insgesamt ist also

$$F(G) = Z(N)F(B).$$

Also wird

$$FE(G) = F(G) \cdot E(G) = Z(N)F(B) \cdot N = NF(B).$$



# Anhang A

## Aufgaben und Lösungen

### A.1 Aufgaben

**Aufgabe 1 (Definition)** Sei  $G$  eine Menge. Sei  $(\cdot) : G \times G \rightarrow G$  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  $n \geq 0$  und eine Gruppe  $G$  schreiben wir  $G^{\times n} := \prod_{i \in [1, n]} G$ , mit  $G^{\times 0} = 1$ . Betrachte den Gruppenmorphismus  $\delta : G \rightarrow G \times G$ ,  $g \mapsto (g, g)$ . Unter welcher Bedingung an  $G$  ist  $\delta(G) \trianglelefteq G \times G$ ?
- (3) Sei  $G$  eine Gruppe. Sei  $n \geq 0$ . Seien  $U_i \leq G$ . 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  $\prod_{i \in [1, n]} U_i \rightarrow G$ ,  $(u_i)_i \mapsto u_1 \cdots u_n$  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  $N \times M \xrightarrow{\sim} G$ ,  $(n, m) \mapsto nm$ . Ist die Aussage noch richtig, wenn die Normalität der Untergruppe  $M$  nicht verlangt wird?

**Aufgabe 3 (abelsche Gruppen)**

- (1) Sei  $n \geq 1$ . Sei  $x = (x_i)_i \in \mathbf{Z}^{n \times 1}$ . Sei  $g := \text{ggT}(x_1, \dots, x_n)$ .

Zeige, daß es ein  $S \in \text{SL}_n(\mathbf{Z})$  gibt mit  $Sx = \begin{pmatrix} g \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ .

- (2) Seien  $m, n \geq 1$ . Sei  $A \in \mathbf{Z}^{m \times n}$ . Zeige, daß es  $S \in \text{SL}_m(\mathbf{Z})$  und  $T \in \text{SL}_n(\mathbf{Z})$  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  $n \geq 0$ . Sei  $B \leq \mathbf{Z}^n$ . Zeige, daß  $B$  endlich erzeugt ist.
- (4) Sei  $C$  eine additiv geschriebene abelsche Gruppe. Sei  $C$  endlich erzeugt.  
 Zeige, daß  $C \simeq \prod_{i \in [1, k]} \mathbf{Z}/c_i\mathbf{Z}$  ist als abelsche Gruppen für geeignete  $k \in \mathbf{Z}_{\geq 0}$  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 Gruppenmorphisamen gegeben.

$$\begin{array}{ccccc}
 A' & \xrightarrow{a'} & A & \xrightarrow{a''} & A'' \\
 f' \downarrow & & f \downarrow & & \downarrow f'' \\
 B' & \xrightarrow{b'} & B & \xrightarrow{b''} & B''
 \end{array}$$

Zeige, daß es eine abelsche Gruppe  $P$ , eine linksexakte Sequenz  $P \rightarrow A \times B' \rightarrow B$  und kurz exakte Sequenzen  $P \rightarrow A \rightarrow \text{Im}(f'')$  und  $A' \rightarrow P \rightarrow \text{Kern}(f'')$  gibt.

- (6) Berechne im Sinne von (4) unter Verwendung von (5) Kern und Bild des Gruppenmorphisamen

$$\begin{array}{ccccccc}
 \mathbf{Z}/4\mathbf{Z} & \times & \mathbf{Z}/8\mathbf{Z} & \times & \mathbf{Z}/8\mathbf{Z} & \longrightarrow & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/16\mathbf{Z} \\
 (x + 4\mathbf{Z} & , & y + 8\mathbf{Z} & , & z + 8\mathbf{Z}) & \longmapsto & (0 & , & z + 2\mathbf{Z} & , & 4x + 4y + 8z + 16\mathbf{Z}) .
 \end{array}$$

**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  $N$  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  $\text{Abb}(M, N)$  eine  $(G \times H)$ -Menge via  $((g, h)f)(m) := hf(g^-m)$  für  $g \in G, h \in H, f \in \text{Abb}(M, N)$ .
- (4) Es ist  $\text{Pot}(M)$  eine  $G$ -Menge, unter Verwendung von (3).
- (5) Die Menge der Untergruppen von  $G$  ist eine  $G$ -Menge, unter Verwendung von (4).
- (6) Sei  $U \leq G$ . Sei  $N_G(U) := C_G(\{U\})$  der *Normalisator* von  $U$  in  $G$ ; cf. (5).  
 Dann ist  $C_G(U) \trianglelefteq N_G(U)$  und  $U \trianglelefteq N_G(U)$ . Ist stets  $UC_G(U) = N_G(U)$ ?

- (7) Sei  $k \geq 1$ . Die Menge der Untergruppen von Ordnung  $k$  von  $G$  bildet eine  $G$ -Menge, unter Verwendung von (4).
- (8) Ist  $\Omega$  eine  $G$ -Teilmenge von  $\text{Pot}(M)$ , dann auch die Menge  $\Omega_{\max}$  der maximalen Elemente von  $\Omega$ .

**Aufgabe 5 (§1.1)** Sei  $n \geq 3$ . 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  $H \leq G$ .  
Genau dann ist  $HC_G(m) = G$ , wenn  $M|_H^G$  eine transitive  $H$ -Menge ist.
- (2) Sei  $G$  endlich. Sei  $U \leq G$ . Sei  $p$  der kleinste Primteiler von  $|U|$ . Sei  $p \geq [G : U]$ .  
Es ist  $U \trianglelefteq G$ . (Hinweis:  $\text{Fix}_U(G/U)$ .)

**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  $|\text{Fix}_P(M)| \equiv_p |M|$ .
- (2) Sei  $G$  eine endliche Gruppe. Sei  $p$  ein Primteiler von  $|G|$ .  
Es gibt in  $G$  ein Element von Ordnung  $p$ .  
(Hinweis: Es ist  $M := \{(g_i)_i \in G^{\times p} : g_1 g_2 \cdots g_p = 1\}$  eine  $C_p$ -Menge. Wieso ist  $|\text{Fix}_{C_p}(M)| \geq p$ ?)

**Aufgabe 8 (§1.1)** Zeige.

- (1) Sei  $n \geq 1$  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  $G \rightarrow S_G$ . Zykeltyp von Element von Ordnung 2? Ist das Kompositum  $G \rightarrow S_G \rightarrow \{\pm 1\}$  surjektiv? Kern?)
- (2) Sei  $G$  eine endliche Gruppe. Sei  $U \leq G$ . Es gibt  $N \trianglelefteq G$  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  $G := \langle (1, 2, 3, 4, 5, 6, 7, 8, 9), (1, 9)(2, 8)(3, 7)(4, 6) \rangle \leq S_9$ .

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  $k \geq 1$ . 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  $GL_2(K)$ -Menge  $P^1(K)$  ist dreifach transitiv.
- (2) Genau dann ist die  $GL_2(K)$ -Menge  $P^1(K)$  vierfach transitiv, wenn  $|K| = 3$  ist.
- (3) Sei  $K$  endlich. Genau dann ist die  $SL_2(K)$ -Menge  $P^1(K)$  dreifach transitiv, wenn  $\text{char } K = 2$  ist.
- (4) Sei  $n \geq 3$ . Die  $GL_n(K)$ -Menge  $P^{n-1}(K)$  ist nicht dreifach transitiv.
- (5) Sei  $n \geq 2$ . Der Kern der Operation von  $GL_n(K)$  auf  $P^{n-1}(K)$  ist  $Z(GL_n(K)) = K \times E_n$ .

**Aufgabe 12 (Aufgabe 4.(6))** Sei  $G$  eine Gruppe. Seien  $U, V \leq G$ . Zeige.

- (1) Seien  $U$  und  $V$  endlich. Es ist  $|UV| = |U| \cdot |V| / |U \cap V|$ .
- (2) Ist  $U \leq N_G(V)$ , dann ist  $V \trianglelefteq UV = VU \leq G$  und  $U \cap V \trianglelefteq U$  und  $U/(U \cap V) \xrightarrow{\sim} (UV)/V$ ,  $u(U \cap V) \mapsto uV$  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  $G/H \xrightarrow{\sim} (G/N)/(H/N)$ ,  $gH \mapsto (gN)(H/N)$ .

**Aufgabe 13 (§2.2.1)** Seien  $G$  und  $H$  Gruppen. Sei  $G \xrightarrow{f} H$  ein Gruppenmorphismus.

Sei  $G^{(1)} := \langle [g, h] : g \in G, h \in G \rangle$  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  $G \xrightarrow{r} G/G^{(1)}$ ,  $g \mapsto gG^{(1)}$ . Sei  $H$  abelsch.  
Es gibt genau einen Gruppenmorphismus  $\bar{f} : G/G^{(1)} \rightarrow H$  mit  $\bar{f} \circ r = f$ .
- (4) Sei  $N \trianglelefteq G$ . Genau dann ist  $G/N$  abelsch, wenn  $G^{(1)} \leq N$  liegt.
- (5) Es ist  $A_4/A_4^{(1)} \simeq C_3$ .

**Aufgabe 14 (§1.5, §2.2.2)** Sei  $G_0 := \langle (1, 2)(3, 4), (1, 2)(3, 5), (1, 3)(4, 5) \rangle \leq A_5$ .

Betrachte die  $G_0$ -Menge  $M = [1, 5]$ ; cf. Beispiel 2.(1).

- (1) Bestimme Erzeuger für  $G_1 := C_{G_0}(1)$ .
- (2) Bestimme Erzeuger für  $G_2 := C_{G_1}(2)$ .
- (3) Zeige  $G_0 = A_5$  unter Verwendung von (1) und (2).

**Aufgabe 15 (§1.5)** Zeige.

- (1) Sei  $G$  endlich erzeugt. Sei  $H \leq G$  mit  $[G : H]$  endlich.  
Dann ist auch  $H$  endlich erzeugt.
- (2) Sei  $n \geq 1$ . Sei  $k \geq 1$ . Sei  $p$  prim. Sei  $U \leq S_n$  mit  $U \simeq C_p^{\times k}$ . Dann ist  $[S_n : U] \geq k/2$ .

**Aufgabe 16 (§2.2.1)** 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  $\Gamma_X$  der gerichtete Graph mit Eckenmenge  $M$  und Kantenmenge  $X$ . Definiere den Begriff eines Morphismus von gerichteten Graphen (ohne Kantenmultiplizitäten). Konstruiere einen Gruppenmorphismus  $G \rightarrow \text{Aut}_{\text{Graph}}(\Gamma_X)$ .
- (2) Zeige, daß der Graph  $\Gamma_X$  genau dann zusammenhängend ist für alle Bahnen  $X$  von  $M^{\times 2, \neq}$ , wenn  $M$  primitiv ist.
- (3) Erstelle einen Graphen  $\Gamma_X$  im Sinne von (1) für die Situation aus Aufgabe 9, welcher nicht zusammenhängend ist.

**Aufgabe 17 (§2.2.1)** Sei  $G$  eine Gruppe. Sei  $K \trianglelefteq G$ .

Schreibe den Restklassenmorphismus  $r : G \rightarrow G/K$ ,  $g \mapsto gK$ . Zeige.

- (1) Wir haben die inklusionserhaltende Bijektion

$$\begin{array}{ccc} \{U \subseteq G : K \leq U \leq G\} & \longrightarrow & \{V \subseteq G/K : V \leq G/K\} \\ U & \longmapsto & r(U) \\ r^{-1}(V) & \longleftarrow & V. \end{array}$$

- (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  $U'/U \xrightarrow{\simeq} r(U')/r(U)$ ,  $u'U \mapsto r(u')r(U)$ .
- (3) Die Bijektion aus (1) schränkt ein zu einer Bijektion von  $\{U \subseteq G : K \leq U \trianglelefteq G\}$   
nach  $\{V \subseteq G/K : V \trianglelefteq G/K\}$ .

**Aufgabe 18 (§2.2.3)** Sei  $F$  ein Körper. Zeige.

- (1) Sei  $n \geq 3$ . Es ist  $\mathrm{SL}_n(F)^{(1)} = \mathrm{SL}_n(F)$ .
- (2) Sei  $|F| \geq 4$ . Es ist  $\mathrm{SL}_2(F)^{(1)} = \mathrm{SL}_2(F)$ .
- (3) Sei  $n \geq 2$ . Sei  $A := \begin{pmatrix} 1 & \\ & \mathbf{0}_{\mathbb{E}_{n-1}} \end{pmatrix} \in \mathrm{C}_{\mathrm{SL}_n(F)}(\bar{e}_1)$ . Es ist  $\langle {}^g A : g \in \mathrm{SL}_n(F) \rangle = \mathrm{SL}_n(F)$ .
- (4) Sei  $n \geq 2$ . Es ist  $Z(\mathrm{SL}_n(F)) = F^\times \mathbf{E}_n \cap \mathrm{SL}_n(F)$ . Cf. Aufgabe 11.(5).

**Aufgabe 19 (§2.2.3)**

- (1) Bestimme den Kern der Operation  $\mathrm{GL}_2(\mathbf{F}_3) \rightarrow \mathrm{S}_{\mathbb{P}^1(\mathbf{F}_3)}$ ; cf. Beispiel 30.  
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 (§2.2.2, §2.1)** Zeige.

- (1) Sei  $n \geq 5$ . Es hat  $A_n$  keine echte Untergruppe von Index  $< n$ .
- (2) Sei  $n \geq 3$ . Es ist  $Z(S_n) = 1$ .
- (3) Sei  $n \geq 5$ . 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. Annahme,  $|\mathrm{Syl}_2(G)| = 15$ . Wieso gibt es dann ein  
 $x \in G$ , das im Schnitt zweier 2-Sylowgruppen liegt? Warum ist dann 4 ein echter  
Teiler von  $|C_G(x)|$ ? Betrachte dann  $G \rightarrow \mathrm{S}_{(C_x)}$ .)

**Aufgabe 21 (§1.4)** Sei  $G$  eine endliche Gruppe.

Sei  $M$  eine primitive  $G$ -Menge mit  $|M| \equiv_2 0$  und  $|M| \geq 3$ . Zeige  $|G| \equiv_4 0$ .

(Hinweis: Annahme, nicht. Wende Aufgabe 8.(1) an, dann Block als Bahn unter Normalteiler.)

**Aufgabe 22 (§2.3.2)** Sei  $n \geq 1$ .

Setze

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

cf. Beispiel 57.

Zeige die Existenz des Gruppenisomorphismus

$$\begin{array}{ccc} S_{P,n} & \xrightarrow{f} & S_n \\ s_i & \mapsto & (i, i+1) \quad \text{für } i \in [1, n-1]. \end{array}$$

**Aufgabe 23 (§2.3.2)** Sei  $G$  eine Gruppe.

Ein Automorphismus  $\alpha$  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  $\text{Inn}(G)$  bezeichnet.

Die Menge der Automorphismen von  $G$  wird mit  $\text{Aut}(G)$  bezeichnet.

- (1) Zeige  $\text{Inn}(G) \trianglelefteq \text{Aut}(G) \leq S_G$ .
- (2) Ist  $\text{Inn}(S_4) = \text{Aut}(S_4)$ ?
- (3) Konstruiere einen Gruppenendomorphismus von  $S_4$  mit Bild von Ordnung 6.
- (4) Ist  $\text{Inn}(S_6) = \text{Aut}(S_6)$ ?  
(Hinweis:  $(1, 2) \mapsto (1, 2)(3, 4)(5, 6)$ ,  $(1, 2, 3, 4, 5, 6) \mapsto (1, 2, 3)(4, 5)$ .)

**Aufgabe 24 (§2.2.3, §2.1)**

- (1) Konstruiere einen Isomorphismus  $\text{PSL}_2(\mathbf{F}_4) \xrightarrow{\sim} A_5$ .
- (2) Konstruiere einen Isomorphismus  $\text{PSL}_2(\mathbf{F}_5) \xrightarrow{\sim} A_5$ . (Hinweis:  $\text{Syl}_2(\text{PSL}_2(\mathbf{F}_5))$ .)

**Aufgabe 25 (§2.1)**

- (1) Sei  $G$  eine Gruppe von Ordnung 77. Zeige  $G \simeq C_{77}$ .
- (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  $\text{GL}_2(\mathbf{F}_{11})$ .

- (5) Finde zu jedem Primteiler der Gruppenordnung eine Sylowgruppe von  $\mathrm{GL}_3(\mathbf{F}_5)$ .

### Aufgabe 26 (§2.3.3)

- (1) Finde eine endlich präsentierte Gruppe mit 2 Erzeugern isomorph zu  $A_4$ .
- (2) Finde eine endlich präsentierte Gruppe isomorph zu  $Q_8 := \langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle \leq \mathrm{GL}_2(\mathbf{C})$ . 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  $H \leq G$ . Zeige, daß  $(H \cap U_i)_{i \in [0, s]}$  eine Subnormalreihe von  $H$  ist. Gib einen injektiven Gruppenmorphismus  $(H \cap U_i)/(H \cap U_{i+1}) \rightarrow U_i/U_{i+1}$  an für  $i \in [0, s-1]$ .
- (2) Sei  $N \trianglelefteq G$ . Schreibe  $\bar{U}_i := (U_i N)/N$  für  $i \in [0, s]$ . Zeige, daß  $(\bar{U}_i)_{i \in [0, s]}$  eine Subnormalreihe von  $G/N$  ist. Gib einen surjektiven Gruppenmorphismus  $U_i/U_{i+1} \rightarrow \bar{U}_i/\bar{U}_{i+1}$  an für  $i \in [0, s-1]$ .

### Aufgabe 28 (§2.3.2)

- (1) Zeige, daß es genau einen Gruppenmorphismus  $f : S_4 \rightarrow \mathrm{GL}_3(\mathbf{Z})$  mit  $(1, 2) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$  und  $(1, 2, 3, 4) \mapsto \begin{pmatrix} -2 & 1 & 0 \\ -3 & 0 & 1 \\ -4 & 0 & 1 \end{pmatrix}$  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 (§2.3.2)

- (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,  $G = \langle x_1, \dots, x_n : r_1, \dots, r_m \rangle$ .  
Schreibe  $X := \{x_1, \dots, x_n\}$ . 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  $\varphi : F(X) \rightarrow A$ , welcher jedes  $x \in X$  nach  $x$  abbildet. Sei  $U := \langle \varphi(r_j) : j \in [1, m] \rangle \leq A$ . Zeige die Existenz des Gruppenisomorphismus

$$\begin{array}{ccc} G/G^{(1)} & \xrightarrow{\bar{\varphi}} & A/U \\ xG^{(1)} & \mapsto & x + U \quad \text{für } x \in X. \end{array}$$

- (3) Berechne  $S_5/S_5^{(1)}$  einmal direkt und einmal mittels (2).



**Aufgabe 30 (§3.1)** Bestimme alle Kompositionsreihen der Gruppe  $G$ .

- (1)  $G = C_{20}$
- (2)  $G = S_4$

**Aufgabe 31 (§3.2)** Sei  $p$  eine Primzahl. Sei  $P$  eine  $p$ -Gruppe. Zeige.

- (1) Ist  $P > 1$ , dann ist  $Z(P) > 1$ . (Hinweis: Aufgabe 7.(1).)
- (2) Ist  $P$  einfach, dann ist  $P \simeq C_p$ .

**Aufgabe 32 (§3.2)**

Sei  $G$  eine endliche Gruppe. Sei  $H \leq G$ . 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  $N \leq Z(G)$  und ist  $G/N$  überauflösbar, dann auch  $G$ .
- (5) Ist  $G$  überauflösbar, dann auch  $H$  und  $G/N$ .
- (6) Ist  $N \leq Z(G)$  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  $k \geq 0$ , dann ist  $G$  auflösbar.
- (6) Ist  $|G| < 60$ , dann ist  $G$  auflösbar.

**Aufgabe 34 (§3.2)** Seien  $G$  und  $H$  Gruppen. Sei  $f : G \rightarrow H$  ein Gruppenmorphismus. Zeige oder widerlege.

- (1) Seien  $U, V \leq G$ . Es ist  $[f(U), f(V)] = f([U, V])$ .
- (2) Es ist  $f(Z(G)) \leq Z(H)$ .
- (3) Es ist  $f(Z(G)) \leq Z(f(G))$ .
- (4) Es ist  $f(Z(G)) = Z(f(G))$ .

**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.  $s \leq t$ . 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  $i \geq 0$ .
- (4) Es ist  $(G \times H)^{]i[} = G^{]i[} \times H^{]i[}$  für  $i \geq 0$ .
- (5) Sind  $G$  und  $H$  nilpotent, so auch  $G \times H$ .  
Folgere dies separat aus (2), aus (3) resp. aus (4).

**Aufgabe 36 (§2.3.2, §3.2)** Sei  $D_{16} := \langle a, b : a^8, b^2, (ab)^2 \rangle$ . Sei  $G := D_{16} \times C_2$ .

- (1) Zeige  $|D_{16}| = 16$ .
- (2) Zeige, daß die Kommutatorreihe, die absteigende Zentralreihe und die aufsteigende Zentralreihe von  $G$  paarweise verschieden sind.

**Aufgabe 37 (§3.2)** Eine Gruppe  $H$  heie *charakteristisch-einfach*, wenn  $H > 1$  ist und wenn  $H$  auer 1 und  $H$  keine weiteren charakteristischen Untergruppen hat.

In einer Gruppe  $H$  heit 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, da  $N$  charakteristisch-einfach ist.
- (2) Sei  $N$  eine charakteristisch einfache endliche Gruppe. Sei  $S$  ein minimaler Normalteiler von  $N$ . Zeige, da  $S$  einfach ist und es ein  $k \geq 1$  mit  $N \simeq S^{\times k}$  gibt.  
(Hinweis:  $S \trianglelefteq N$  minimal;  $k \geq 1$  maximal mit Automorphismen  $(\alpha_i)_{i \in [1, k]}$  so, da  $S^{\times k} \rightarrow N$ ,  $(s_i)_i \mapsto \alpha_1(s_1) \cdots \alpha_k(s_k)$  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  $k \geq 1$ . Sei  $X \trianglelefteq S^{\times k}$ . Zeige die Existenz einer Teilmenge  $I \subseteq [1, k]$  mit  $X = \{(s_i)_i \in S^{\times k} : s_i = 1 \text{ für } i \in [1, k] \setminus I\}$ . 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  ${}^G\langle S \rangle = N$  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  $|\text{Aut}(G)|$ .
- (3) Bestimme die charakteristischen Untergruppen von  $G$ .

**Aufgabe 39 (§3.2)** Sei  $G$  eine endliche Gruppe. Zeige.

- (1) Sei  $N \trianglelefteq G$ . Sei  $\text{Aut}(N)$  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  $U < N_P(U)$ . (Hinweis: aus  $P^{i|} \leq U$  folgt  $P^{i+1|} \leq N_P(U)$ .)
- (2) Sei  $U < P$  maximale echte Untergruppe. Es ist  $U \trianglelefteq P$ .
- (3) Sei  $P$  nichtabelsch. Es ist  $[P : Z(P)] \equiv_{p^2} 0$ .

**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  $p \geq 3$  prim.

Sei  $G$  eine nichtabelsche Gruppe von Ordnung  $p^3$ .

- (1) Zeige  $Z(G) \simeq C_p$ . 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  $C_p \times C_p$  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  $Z(G)$  kein Komplement, also  $Z(G) = \langle b^p \rangle$  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  $\langle bc^{-1} \rangle$  gibt den Widerspruch.)

**Aufgabe 45 (§3.3)** Sei  $H$  eine Gruppe.

- (1) Sei  $M$  eine  $H$ -Menge, mit Operation  $\beta : H \rightarrow S_M$ . Sei  $K$  eine Gruppe, aufgefaßt als  $H$ -Menge via  $! : H \rightarrow S_K$ . Wir haben die  $H$ -Menge  $\text{Abb}(M, K)$ , mit der Operationsabbildung  $\alpha_0 : H \rightarrow S_{\text{Abb}(M, K)}$ ; cf. Aufgabe 4.(3). Zeige, daß der Gruppenmorphismus  $\alpha := \alpha_0|_{\text{Aut}(\text{Abb}(M, K))}$  definiert ist. Inwiefern verallgemeinert dies Definition 96? Schreibe auch hier  $H \wr K = K \wr_{\beta} H := \text{Abb}(M, K) \rtimes_{\alpha} H$ .

- (2) Sei  $L \leq H$  eine Untergruppe von endlichem Index. Sei  $\beta$  die Operation von  $H$  auf  $H/L$ ; cf. Beispiel 2.(3). Seien  $R, N \trianglelefteq L$  mit  $N \trianglelefteq H$ .

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  $u_h : H/L \rightarrow L/R, xL \mapsto \lambda(x) \cdot \lambda(h^{-1}x)^{-1}R$ . Zeige die Wohldefiniertheit dieses Elements der Gruppe  $\text{Abb}(H/L, L/R)$ . Zeige die Existenz des Gruppenmorphismus

$$\begin{array}{ccc} H & \xrightarrow{f} & (L/R) \wr_{\beta} (H/N) \\ h & \mapsto & (u_h, hN) \end{array}$$

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  $L := C_H(u(x))$ . 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  $\beta : H \rightarrow S_m$  ein Gruppenmorphismus; schreibe  $(\beta(h))(i) = hi$  für  $h \in H$  und  $i \in [1, m]$ .

- (1) Zeige, daß  $X^{\times m}$  via  $((k_i)_i, h) \cdot (x_i)_i := (k_i x_{h^{-1}i})_i$  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 104.(3).
- (2) Zeige Lemma 104.(4).

**Aufgabe 48 (§3.4.1)**

- (1) Sei  $H$  eine endliche Gruppe. Sei  $A$  eine endliche abelsche Gruppe.

Sei  $\alpha : H \rightarrow \text{Aut}(A)$  ein Gruppenmorphismus.

Sei  $1 < K \trianglelefteq H$  ein abelscher Normalteiler mit  $|K|$  teilerfremd zu  $|A|$ .

So wird  $A \setminus \{1\}$  zu einer  $K$ -Menge. Sei  $C_K(a) = 1$  für  $a \in A \setminus \{1\}$ .

Zeige  $H^2(H, A) = 1$  und  $H^1(H, A) = 1$ , genommen bezüglich  $\alpha$ .

(Hinweis: Sei  $E$  eine Erweiterung von  $A$  mit  $H$ . Sei  $F \leq E$  das Urbild von  $K \leq H$ . Es hat  $A$  in  $F$  ein Komplement. Sei  $Q$  eine Sylowgruppe von  $F$ , konstruiert als Bild einer Sylowgruppe von  $K$ . Verwende Frattini, um  $A \cdot N_E(Q) = E$  zu zeigen.)

- (2) Sei  $n \geq 1$ . Sei  $q \geq 3$  eine Primpotenz. Sei  $H = \text{GL}_n(\mathbf{F}_q)$ . Sei  $A := \mathbf{F}_q^{n \times 1}$ , additiv geschrieben. Sei  $\alpha : H \rightarrow \text{Aut}(A)$ ,  $h \mapsto (a \mapsto ha)$  gegeben via Matrixmultiplikation von  $h \in \text{GL}_n(\mathbf{F}_q) \subseteq \mathbf{F}_q^{n \times n}$  mit  $a \in \mathbf{F}_q^{n \times 1}$ .

Zeige  $H^2(H, A) = 0$  und  $H^1(H, A) = 0$ , genommen bezüglich  $\alpha$ , ebenfalls additiv geschrieben.

**Aufgabe 49 (Aufgabe ??)** Sei  $A$  eine abelsche Gruppe. Sei  $B \leq A$ . 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 Gruppenmorphis men  $B \xrightarrow{g} Q$  gibt es einen Gruppenmorphis mus  $A \xrightarrow{f} Q$  mit  $f|_B = g$ .  
(Hinweis: Zorn über  $\{(C, h) : B \leq C \leq A, h \text{ Gruppenmorphis mus mit } h|_B = g\}$ .)
- (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  $U(\mathbf{C})$  divisibel.  
Es ist  $U_1(\mathbf{C}) := \{u \in U(\mathbf{C}) : |u| = 1\}$  eine divisible Untergruppe von  $U(\mathbf{C})$ .

## 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.