

Kombinatorische Gruppentheorie

Vorlesung im Sommersemester 2022

Benjamin Sambale
Leibniz Universität Hannover

5. April 2025

$$M_{11} = \langle x, y, z \mid x^{11} = y^5 = z^4 = (xz)^3 = 1, \, xyx^{-1} = x^4, \, zyz^{-1} = y^2 \rangle$$

x	x^{-1}	y	y^{-1}	z	z^{-1}
2	3	1	1	4	4
5	1	6	7	8	9
1	10	11	12	11	13
14	15	4	4	1	1
6	2	13	11	5	5
7	5	10	2	16	16
17	6	2	17	14	18
19	9	9	18	10	2
8	16	14	8	2	10
3	11	17	6	9	8
10	12	5	3	12	3
11	13	3	13	13	11
12	17	12	5	3	12
20	4	16	9	17	7
4	18	21	22	21	19
9	20	18	14	6	6
13	7	7	10	18	14
15	21	8	16	7	17
22	8	22	20	15	22
16	14	19	21	20	20
18	22	20	15	22	15
21	19	15	19	19	21

Inhaltsverzeichnis

Vorwort	2
1 Freie Gruppen	3
2 Untergruppen freier Gruppen	11
3 Automorphismen freier Gruppen	17
4 Gruppen-Erweiterungen	20
5 Zentrale Erweiterungen	32
6 Erweiterungen der alternierenden Gruppen	46
7 Symplektische Gruppen	52
8 Unitäre Gruppen	58
9 Sporadische Gruppen	68
10 Coxetergruppen	77
11 Freie Produkte und Amalgame	97
12 Das Burnside-Problem	103
13 Gruppenklassen und Varietäten	115
14 p -Gruppen	122
15 Entscheidbarkeitsprobleme	129
Aufgaben	131
Stichwortverzeichnis	137

Vorwort

In der kombinatorischen Gruppentheorie werden Gruppen hauptsächlich mittels Erzeuger und Relationen studiert. Naturgemäß muss man sich daher größtenteils mit unendlichen Objekten auseinandersetzen. Eine der wichtigsten Motivationen ist das *Burnside-Problem*: Ist jede endlich erzeugte Gruppe mit endlichem Exponenten endlich? Da gelegentlich geometrische Argumente zum Einsatz kommen (zum Beispiel bei Coxetergruppen), spricht man alternativ auch von *geometrischer Gruppentheorie*.

Dieses Skript entstand im Rahmen einer 3 + 1 Vorlesung im Sommersemester 2022 an der Leibniz Universität Hannover. Die Vorlesung schließt an meine Gruppentheorie-Vorlesung im Wintersemester 2020/21 an und setzt entsprechende Kenntnisse voraus (Verweise sind mit GT gekennzeichnet). An einigen Stellen gibt es Doppelungen in beiden Vorlesungen. Die Gründe dafür sind:

- Kenntnisse ins Gedächtnis zurückrufen.

- Alternative Beweismethoden vorstellen.
- Themen, die zwar im Gruppentheorie-Skript stehen, aber dort aus Zeitgründen nicht behandelt wurden (Beispiel: Schur-Erweiterungen).

Die Kapitel 3, 5, 8 und 11–15 wurden nicht behandelt (darin sind also mehr Fehler zu erwarten). Um das Rechnen mit (realistischen) Beispielen praktikabel zu gestalten, geben wir an vielen Stellen Befehle für das kostenlose Computeralgebrasystem GAP an. An dieser Stelle vielen Dank an Thomas Breuer für nützliche Ratschläge. Ich bedanke mich ebenso bei Annika Bartelt, Luca Blaas, Adrian Homma, Scheima Obeidi und Tim Wittenberg für einige Fehlerhinweise.

Literatur:

- T. Camps, V. Rebel, G. Rosenberger, *Einführung in die kombinatorische und die geometrische Gruppentheorie*, Heldermann Verlag, Lemgo, 2008¹
- M. Hall, *The Theory of Groups*, 4th printing, The Macmillan Company, New York, 1963²
- D. J. S. Robinson, *A Course in the Theory of Groups*, 2nd edition, Springer, New York, 1996³
- W. Magnus, A. Karrass, D. Solitar, *Combinatorial Group Theory*, 2nd edition, Dover, Mineola, 2004⁴
- R. C. Lyndon, P. E. Schupp, *Combinatorial Group Theory*, Springer, Berlin, 1977
- J. E. Humphreys, *Reflection groups and Coxeter groups*, Cambridge University Press, Cambridge, 1994
- D. L. Johnson, *Presentations of Groups*, 2nd edition, Cambridge University Press, Cambridge, 1997
- H. S. M. Coxeter, W. O. J. Moser, *Generators and Relations for Discrete Groups*, 4th edition, Springer, Berlin, 1980
- The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.11.1*; 2021, (<http://www.gap-system.org>).

1 Freie Gruppen

Bemerkung 1.1. Eine Basis B eines Vektorraums V lässt sich durch folgende Eigenschaft charakterisieren: Für jeden Vektorraum W besitzt jede Abbildung $B \rightarrow W$ genau eine lineare Fortsetzung $V \rightarrow W$. Auf diese Weise kann man Basen für beliebige (nicht-abelsche) Gruppen definieren. Im Gegensatz zu Vektorräumen besitzen die meisten Gruppen aber keine Basen.

Definition 1.2 (Universelle Eigenschaft). Eine Gruppe F heißt *frei* bzgl. einer Teilmenge $X \subseteq F$, falls für jede Gruppe G und jede Abbildung $\sigma: X \rightarrow G$ genau ein Homomorphismus $\hat{\sigma}: F \rightarrow G$ mit $\hat{\sigma}(x) = \sigma(x)$ für alle $x \in X$ existiert (d. h. $\hat{\sigma}$ ist eine Fortsetzung von σ).

¹Fokus auf den geometrischen Aspekt.

²Behandelt endliche und unendliche Gruppen gleichberechtigt. Trotz seines Alters gut zu lesen.

³Etwas moderner und umfangreicher als Hall.

⁴Unveränderter Neudruck der 1975 erschienenen Ausgabe. Kleine Schrift, viel Fließtext, schwer zu lesen.

Beispiel 1.3.

- (i) Die triviale Gruppe $F = 1$ ist die einzige freie Gruppe bzgl. $X = \emptyset$, denn jede nicht-triviale Gruppe F besitzt mindestens zwei Endomorphismen.
- (ii) Die Gruppe \mathbb{Z} ist frei bzgl. $X = \{1\}$, denn jede Abbildung $\sigma: X \rightarrow G$ besitzt die eindeutige Fortsetzung $\mathbb{Z} \rightarrow G$, $n \mapsto \sigma(1)^n$.

Definition 1.4. Sei X eine Menge, die wir *Alphabet* nennen. Die Elemente von X heißen *Buchstaben*. Sei W die Menge aller *Worte* der Form $w = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ mit $n \in \mathbb{N}_0$, $x_1, \dots, x_n \in X$ und $\epsilon_1, \dots, \epsilon_n \in \{\pm 1\}$. Dabei heißt $|w| := n$ die *Länge* von w . Für $n = 0$ erhält man das *leere Wort* $w = 1$. Gilt $x_i \neq x_{i+1}$ oder $\epsilon_i = \epsilon_{i+1}$ für $i = 1, \dots, n-1$, so heißt w *reduziert*. Offenbar kann man jedes Wort w in ein reduziertes Wort überführen, indem man Teile der Form xx^{-1} oder $x^{-1}x$ sukzessiv streicht. Zwei Worte $v, w \in W$ heißen *äquivalent*, wenn man sie in das gleiche reduzierte Wort überführen kann. Dies ist eine Äquivalenzrelation auf W . Die Menge der Äquivalenzklassen $F_X := \{[w] : w \in W\}$ bildet dann eine Gruppe bzgl. Konkatination, d. h.

$$[w][v] := [wv] \quad [w], [v] \in F_X.$$

Das neutrale Element ist die Äquivalenzklasse des leeren Worts $[1]$. Das Inverse von $[x_1^{\epsilon_1} \dots x_n^{\epsilon_n}]$ ist $[x_n^{-\epsilon_n} \dots x_1^{-\epsilon_1}]$. Indem man $x \in X$ mit $[x] \in F_X$ identifiziert, kann man $X \subseteq F_X$ annehmen.

Satz 1.5.

- (i) F_X ist frei bzgl. X .
- (ii) Jede freie Gruppe bzgl. X ist zu F_X isomorph.
- (iii) Es gilt $F_X \cong F_Y$ genau dann, wenn X und Y gleichmächtig sind.

Beweis.

- (i) Sei G eine Gruppe und $\sigma: X \rightarrow G$. Für $w = x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \in W$ definieren wir

$$\hat{\sigma}(w) := \sigma(x_1)^{\epsilon_1} \dots \sigma(x_n)^{\epsilon_n} \in G.$$

Für äquivalente Wörter $v, w \in W$ gilt offenbar $\hat{\sigma}(v) = \hat{\sigma}(w)$. Somit induziert $\hat{\sigma}$ eine wohldefinierte Abbildung $F_X \rightarrow G$, die wir ebenfalls mit $\hat{\sigma}$ bezeichnen. Wegen $\hat{\sigma}(wv) = \hat{\sigma}(w)\hat{\sigma}(v)$ für $w, v \in W$ ist $\hat{\sigma}$ ein Homomorphismus. Wegen $F_X = \langle X \rangle$ ist $\hat{\sigma}$ eindeutig durch σ bestimmt.

- (iii) Sei $\sigma: X \rightarrow Y$ eine Bijektion. Dann existieren Homomorphismen $\alpha: F_X \rightarrow F_Y$ und $\beta: F_Y \rightarrow F_X$ mit $\alpha|_X = \sigma$ und $\beta|_Y = \sigma^{-1}$. Also ist $\alpha\beta: F_Y \rightarrow F_Y$ eine Fortsetzung von id_Y . Aus der universellen Eigenschaft folgt $\alpha\beta = \text{id}_{F_Y}$. Analog zeigt man $\beta\alpha = \text{id}_{F_X}$. Also ist α ein Isomorphismus zwischen F_X und F_Y .

Sei umgekehrt ein Isomorphismus $\alpha: F_X \rightarrow F_Y$ gegeben. Wir betrachten

$$N_X := \langle g^2, [g, h] : g, h \in F_X \rangle \trianglelefteq F_X$$

und $\overline{F_X} := F_X/N_X$. Wegen $\alpha(N_X) = \langle \alpha(g), [\alpha(g), \alpha(h)] : g, h \in F_X \rangle = N_Y$ ist $\overline{F_X} \cong \overline{F_Y}$. Nach Konstruktion ist $\overline{F_X}$ eine abelsche Gruppe mit $\bar{g}^2 = 1$ für alle $\bar{g} \in \overline{F_X}$. Durch die Skalarmultiplikation $\lambda \bar{g} := \bar{g}^\lambda$ für $\lambda \in \mathbb{F}_2$ wird $\overline{F_X}$ ein \mathbb{F}_2 -Vektorraum (eine unendliche Version der elementarabelschen Gruppen aus GT). Die Elemente $\bar{x} := xN_X$ mit $x \in X$ bilden ein Erzeugendensystem von $\overline{F_X}$. Nehmen wir an es gibt paarweise verschiedene $x_1, \dots, x_n \in X$ mit $x_1 \dots x_n \in N_X$. Sei $\sigma: X \rightarrow \mathbb{F}_2$ mit $\sigma(x_1) = 1$ und $\sigma(x_i) = 0$ für $i = 2, \dots, n$. Sei $\hat{\sigma}: F_X \rightarrow \mathbb{F}_2$

die Fortsetzung von σ . Wegen $\widehat{\sigma}(g^2) = 2\widehat{\sigma}(g) = 0$ und $\widehat{\sigma}([g, h]) = \widehat{\sigma}(g) + \widehat{\sigma}(h) - \widehat{\sigma}(g) - \widehat{\sigma}(h) = 0$ ist $x_1 \dots x_n \in N_X \subseteq \text{Ker}(\widehat{\sigma})$. Dies widerspricht $\widehat{\sigma}(x_1 \dots x_n) = \sigma(x_1) = 1$. Also ist $x_1 \dots x_n \notin N_X$. Dies zeigt, dass $\{\bar{x} : x \in X\}$ eine Basis von $\overline{F_X}$ ist. Also folgt $|X| = \dim \overline{F_X} = \dim \overline{F_Y} = |Y|$.⁵

(ii) Folgt wie in (iii) (es wird nur die universelle Eigenschaft benutzt). \square

Definition 1.6. Ist F frei bzgl. X , so nennt man $\text{rk } F := |X|$ den *Rang* von F . Nach Satz 1.5 gibt es bis auf Isomorphie nur eine freie Gruppe vom Rang $r \in \mathbb{N}$. Diese bezeichnen wir mit F_r .

Lemma 1.7 (vgl. GT-Aufgabe 57). *Jedes Wort $w \in W$ ist zu genau einem reduzierten Wort $\tilde{w} \in W$ äquivalent.*

Beweis (VAN DER WAERDEN). Wir wissen bereits, dass w zu mindestens einem reduzierten Wort äquivalent ist. Für die Eindeutigkeit sei $R \subseteq W$ die Menge aller reduzierten Wörter. Für $r = x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \in R$ und $x \in X$ sei

$$x_r := \begin{cases} xx_1^{\epsilon_1} \dots x_n^{\epsilon_n} & \text{falls } x \neq x_1^{-\epsilon_1}, \\ x_2^{\epsilon_2} \dots x_n^{\epsilon_n} & \text{falls } x = x_1^{-\epsilon_1}. \end{cases}$$

Offenbar induziert x eine Permutation $\sigma(x) \in \text{Sym}(R)$ mit Umkehrabbildung $\sigma(x^{-1})$. Nach der universellen Eigenschaft setzt sich σ zu einer Operation $F_X \rightarrow \text{Sym}(R)$ fort. Für äquivalente reduzierte Wörter $v, w \in R$ gilt

$$v = [v]_1 = [w]_1 = w. \quad \square$$

Bemerkung 1.8.

- (i) Für $r \geq 2$ ist F_r nicht-abelsch, denn $xyx^{-1}y^{-1} \neq 1$ ist reduziert für $x \neq y$.
- (ii) Sei $w = x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \in W$ reduziert mit endlicher Ordnung k in F_X . Indem man notfalls mit $x_1^{-\epsilon_1}$ konjugiert, kann man $x_1^{\epsilon_1} \neq x_n^{-\epsilon_n}$ annehmen. Dann ist auch w^k reduziert und es folgt $w = 1$. Also ist F_r torsionsfrei.

Folgerung 1.9. *Ist F frei bzgl. $X \subseteq F$, so lässt sich jedes Element von F eindeutig in der Form $x_1^{a_1} \dots x_n^{a_n}$ schreiben, wobei $n \in \mathbb{N}_0$, $x_1, \dots, x_n \in X$ mit $x_i \neq x_{i+1}$ für $i = 1, \dots, n-1$ und $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$. Insbesondere ist $F = \langle X \rangle$.*

Beweis. O.B.d.A. sei $F = F_X$. Jedes Element lässt sich nach Lemma 1.7 eindeutig in reduzierter Form schreiben. Indem man gleiche Buchstaben zusammenfasst, erhält man eine Darstellung in der gewünschten Form. \square

Bemerkung 1.10. Nach Cayley ist jede Gruppe zu einer Untergruppe einer symmetrischen Gruppe isomorph. Die freien Gruppen besitzen eine duale Eigenschaft.

Satz 1.11. *Jede Gruppe G ist zu einer Faktorgruppe einer freien Gruppe F isomorph. Lässt sich G durch n Elemente erzeugen, so kann man $\text{rk } F = n$ wählen.*

Beweis. Sei X ein Erzeugendensystem von G (notfalls $X = G$). Dann lässt sich die Inklusion $X \rightarrow G$ zu einem Epimorphismus $F_X \rightarrow G$ fortsetzen. Die Behauptung folgt aus dem Homomorphiesatz. \square

⁵benötigt das Auswahlaxiom, falls $|X| = \infty$

Beispiel 1.12. Sei

$$a := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad b := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Wir zeigen, dass $G := \langle a, b \rangle \leq \text{GL}(2, \mathbb{Q})$ frei bzgl. $\{a, b\}$ ist. Sei dafür $X = \{x, y\}$ und $\varphi: F_X \rightarrow G$ der Epimorphismus mit $\varphi(x) = a$ und $\varphi(y) = b$. Angenommen es gibt ein nicht-triviales reduziertes Wort $w := z_1^{k_1} \dots z_n^{k_n} \in \text{Ker}(\varphi)$ mit $z_1, \dots, z_n \in X$ und $k_1, \dots, k_n \in \mathbb{Z} \setminus \{0\}$. Nach Konjugation können wir $z_n = x$ und $k_n > 0$ annehmen. Dann gilt $1 = \varphi(w) = \dots a^{k_{n-2}} b^{k_{n-1}} a^{k_n}$. Für $k \in \mathbb{Z}$ gilt

$$a^k := \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}, \quad b^k := \begin{pmatrix} 1 & 0 \\ 2k & 1 \end{pmatrix}$$

(Induktion nach k). Sei

$$V_{>} := \{(s, t) \in \mathbb{Q}^2 : |s| > |t|\}, \quad V_{<} := \{(s, t) \in \mathbb{Q}^2 : |s| < |t|\}.$$

Für $v := (1, 1) \in \mathbb{Q}^2$ gilt $a^{k_n} v = (2k_n + 1, 1) \in V_{>}$ wegen $k_n > 0$. Für $v = (s, t) \in V_{>}$ gilt $b^{k_{n-1}} v = (s, 2k_{n-1}s + t) \in V_{<}$, denn $|2k_{n-1}s + t| \geq 2|k_{n-1}||s| - |t| > |s|$ (Dreiecksungleichung) wegen $k_{n-1} \neq 0$. Analog gilt $a^{k_{n-2}} v \in V_{>}$ für $v \in V_{<}$ usw.⁶ Dies ergibt den Widerspruch

$$(1, 1) = \varphi(w)(1, 1) = \dots a^{k_{n-2}} b^{k_{n-1}} a^{k_n} (1, 1) \in V_{>} \cup V_{<}.$$

Also ist φ injektiv und $G \cong F_X \cong F_2$.

Bemerkung 1.13.

- (i) Sei X ein Erzeugendensystem für G und $\sigma: F_X \rightarrow G$ mit $\sigma(x) = x$ wie in Satz 1.11. Die Elemente in $\text{Ker}(\sigma)$ nennt man *Relatoren* für G bzgl. X . Für $x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \in \text{Ker}(\sigma)$ gilt also $x_1^{\epsilon_1} \dots x_n^{\epsilon_n} = 1$ in G . Eine Gleichung dieser Form heißt *Relation* für G bzgl. X .
- (ii) Sei umgekehrt $R \subseteq F_X$. Sei $N := \langle R \rangle^{F_X} := \langle gRg^{-1} : g \in F_X \rangle \trianglelefteq F_X$ der normale Abschluss von R in F_X . Wir setzen

$$G := \langle X \mid R \rangle = \langle X \mid \{r = 1 : r \in R\} \rangle := F_X / N.$$

Man identifiziert Buchstaben $x \in X$ oft mit ihren Nebenklassen $xN \in G$ (im Allgemeinen nicht injektiv!). Ist $|X| + |R| < \infty$, so nennt man G *endlich präsentiert*. Auf diese Weise lässt sich jede Gruppe durch Erzeuger und Relationen beschreiben (dies entspricht der Aussage, dass jeder Vektorraum die Lösungsmenge eines linearen Gleichungssystems ist). Im Allgemeinen ist es jedoch schwierig die Eigenschaften von G aus X und R abzulesen.

Beispiel 1.14.

- (i) $\langle X \mid \emptyset \rangle \cong F_X$.
- (ii) $\langle x \mid x^n \rangle = \langle x \mid x^n = 1 \rangle \cong \mathbb{Z}/n\mathbb{Z} \cong C_n$.
- (iii) Jede endliche Gruppe G ist endlich präsentiert: Sei $X := \{x_g : g \in G\}$, $R := \{x_g x_h x_{gh}^{-1} : g, h \in G\}$ und $N := \langle R \rangle^{F_X}$. Dann existiert ein Epimorphismus $\varphi: F_X \rightarrow G$ mit $\varphi(x_g) = g$ und $R \subseteq \text{Ker}(\varphi)$. Wegen $\text{Ker}(\varphi) \trianglelefteq F_X$ ist auch $N \subseteq \text{Ker}(\varphi)$. Sei umgekehrt $w := x_{g_1}^{\epsilon_1} \dots x_{g_n}^{\epsilon_n} \in \text{Ker}(\varphi)$. Wegen $x_1 = x_1 x_1 x_1^{-1} \in R$ und $x_g x_{g^{-1}} x_1^{-1} \in R$ ist $x_g x_{g^{-1}} \in \langle R \rangle$ und $x_g^{-1} \equiv x_{g^{-1}} \pmod{N}$. Es folgt

$$w \equiv x_{g_1}^{\epsilon_1} \dots x_{g_n}^{\epsilon_n} \equiv x_{g_1}^{\epsilon_1} x_{g_2}^{\epsilon_2} x_{g_3}^{\epsilon_3} \dots \equiv x_{g_1}^{\epsilon_1} \dots x_{g_n}^{\epsilon_n} \equiv x_1 \equiv 1 \pmod{N}.$$

Also ist $\text{Ker}(\varphi) \subseteq N$ und $G = \langle X \mid R \rangle$.

⁶Das Argument nennt sich *Ping-Pong-Lemma*.

Satz 1.15 (VON DYCK). Seien $G = \langle x_i : i \in I \rangle$ und $H = \langle y_i : i \in I \rangle$ Gruppen, sodass für jede Relation $x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n} = 1$ in G auch die Relation $y_{i_1}^{\epsilon_1} \dots y_{i_n}^{\epsilon_n} = 1$ in H gilt. Dann existiert ein Epimorphismus $G \rightarrow H$ mit $f(x_i) = y_i$ für $i \in I$.

Beweis. Nach der universellen Eigenschaft existieren Epimorphismen $f_G: F_I \rightarrow G$ und $f_H: F_I \rightarrow H$ mit $f_G(i) = x_i$ und $f_H(i) = y_i$ für $i \in I$. Nach Voraussetzung gilt $\text{Ker}(f_G) \leq \text{Ker}(f_H)$. Also ist

$$G \cong F_I / \text{Ker}(f_G) \rightarrow (F_I / \text{Ker}(f_G)) / (\text{Ker}(f_H) / \text{Ker}(f_G)) \cong F_I / \text{Ker}(f_H) \cong H$$

der gesuchte Epimorphismus. □

Bemerkung 1.16. Man kann den Satz von von-Dyck benutzen, um undurchsichtige Gruppenpräsentationen durch bekannte Gruppen zu approximieren.

Beispiel 1.17.

- (i) Sei $G := \langle x_1, \dots, x_n \mid [x_i, x_j] = 1 \ \forall i, j \rangle$. Offenbar ist G abelsch und jedes Element in G hat die Form $x_1^{a_1} \dots x_n^{a_n}$ mit $a_1, \dots, a_n \in \mathbb{Z}$. Sei nun $H := \langle y_1 \rangle \oplus \dots \oplus \langle y_n \rangle \cong C_\infty^n$. Nach Satz 1.15 existiert ein Epimorphismus $f: G \rightarrow H$ mit $f(x_i) = y_i$ für $i = 1, \dots, n$. Offenbar ist f auch injektiv und $G \cong H \cong C_\infty^n$. Dies zeigt auch $F_n / F'_n \cong C_\infty^n$.
- (ii) Sei $G = \langle x, y \rangle$ mit $x \neq y$ und $|\langle x \rangle| = |\langle y \rangle| = 2$. Dann besteht G aus den Elementen der Form $xyxy \dots$ und $xyxy \dots$. Ist G endlich, so gilt $n := |\langle xy \rangle| \in \mathbb{N}$ und jedes Element hat die Form $x^i(xy)^j$ mit $0 \leq i \leq 1$ und $0 \leq j \leq n-1$. Dann folgt

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

wobei $D_4 = C_2^2$.

Bemerkung 1.18 (GAP).

```
F:=FreeGroup("x","y"); #das doppelte Semikolon überdrückt die Ausgabe
AssignGeneratorVariables(F);
G:=F/[x^2,y^3,(x*y)^5]; #endlich präsentierte Gruppe
Size(G);
H:=Image(IsomorphismPermGroup(G)); #isomorphe Permutationsgruppe (effizienter)
StructureDescription(H);

#Der umgekehrte Weg:
G:=Image(IsomorphismFpGroup(H)); #isomorphe endlich präsentierte Gruppe
RelatorsOfFpGroup(G); #neue Relationen

#Rechnen in der freien Gruppe:
x:=(1,2,3,4,5,6,7,8,9,10,11);; y:=(3,7,11,8)(4,10,5,6);; #Permutationen von S11
G:=Group(x,y);;
epi:=GroupHomomorphismByImages(F,G,GeneratorsOfGroup(F),[x,y]);
z:=Random(G);
PreImagesRepresentative(epi,z); #Darstellung von z als Wort in x,y
```

Satz 1.19 (NEUMANN). Sei G endlich präsentiert und X ein beliebiges Erzeugendensystem von G . Dann existiert eine endliche Präsentation $G = \langle X_0 \mid R \rangle$ mit $X_0 \subseteq X$.

Beweis. Sei $G = \langle y_1, \dots, y_n \mid s_1, \dots, s_m \rangle$ eine endliche Präsentation. Jedes y_i lässt sich durch endlich viele $x \in X$ ausdrücken, sagen wir $y_i = w_i(x)$. Daher existiert eine endliche Teilmenge $X_0 = \{x_1, \dots, x_k\} \subseteq X$ mit $G = \langle X_0 \rangle$. Umgekehrt lassen sich die x_i durch y_j ausdrücken, sagen wir $x_i = v_i(y)$. Man erhält folgende Relationen in X_0 :

$$s_i(w_1(x), \dots, w_n(x)) = 1, \quad x_i = v_i(w_1(x), \dots, w_n(x)).$$

Sei R die Menge dieser Relatoren und $H := \langle X_0 \mid R \rangle$. Nach von-Dyck existiert ein Epimorphismus $\varphi: H \rightarrow G$ mit $\varphi(x_i) = x_i$ für $i = 1, \dots, k$. Man kann nun $y_i := w_i(x)$ in H definieren. Wegen $x_i = v_i(y_1, \dots, y_n)$ ist dann $H = \langle y_1, \dots, y_n \rangle$. Da die Relationen in s_i auch in H gelten, existiert ein Epimorphismus $\psi: G \rightarrow H$ mit $\psi(y_i) = y_i$ für $i = 1, \dots, n$. Wegen

$$\begin{aligned} \psi(\varphi(x_i)) &= \psi(x_i) = \psi(v_i(y)) = v_i(y) = x_i, \\ \varphi(\psi(y_i)) &= \varphi(y_i) = \varphi(w_i(x)) = w_i(x) = y_i \end{aligned}$$

sind φ und ψ zueinander inverse Isomorphismen. □

Satz 1.20 (HALL). *Sei $N \trianglelefteq G$. Sind N und G/N endlich präsentiert, so auch G .*

Beweis. Sei $N = \langle x_1, \dots, x_n \mid r_1, \dots, r_m \rangle$ und $G/N = \langle y_1N, \dots, y_kN \mid s_1, \dots, s_l \rangle$. Sicher ist $G = \langle x_1, \dots, x_n, y_1, \dots, y_k \rangle$. Wegen $s_i(y) \in N$ gelten Relationen $s_i(y) = t_i(x)$. Die Normalteiler-Eigenschaft lässt sich durch Relationen $y_i x_j y_i^{-1} = u_{ij}(x)$ und $y_i^{-1} x_j y_i = v_{ij}(x)$ ausdrücken. Wir definieren

$$H := \langle x_1, \dots, x_n, y_1, \dots, y_k \mid r_i, s_i(y)t_i(x)^{-1}, u_{ij}(x)y_i x_j^{-1} y_i^{-1}, v_{ij}(x)y_i^{-1} x_j^{-1} y_i \ \forall i, j \rangle.$$

Dann existiert ein Epimorphismus $\varphi: H \rightarrow G$ mit $\varphi(x_i) = x_i$ und $\varphi(y_j) = y_j$. Sei $\tilde{N} := \langle x_1, \dots, x_n \rangle \leq H$. Die Relationen u_{ij} und v_{ij} zeigen $\tilde{N} \trianglelefteq H$. Für $h \in \tilde{N} \cap \text{Ker}(\varphi)$ gilt $h \in \langle r_1, \dots, r_m \rangle^{F_X}$. Dies zeigt $h = 1$ und $\tilde{N} \cap \text{Ker}(\varphi) = 1$. Offenbar induziert φ einen Epimorphismus $\bar{\varphi}: H/\tilde{N} \rightarrow G/N$ mit $\bar{\varphi}(y_i \tilde{N}) = y_i N$. Die Relationen r_i , t_i , u_{ij} und v_{ij} werden in H/\tilde{N} trivial. Also erfüllen H/\tilde{N} und G/N die gleichen Relationen ($s_i(y) = 0$) und $\bar{\varphi}$ ist ein Isomorphismus. Für $h \in \text{Ker}(\varphi)$ gilt $h\tilde{N} \in \text{Ker}(\bar{\varphi}) = 1$, also $h \in \tilde{N} \cap \text{Ker}(\varphi) = 1$. Also ist φ ein Isomorphismus. □

Satz 1.21. *Sei $G = \langle X \mid R \rangle$ mit $X = \{x_1, \dots, x_n\}$ und $R = \{r_1, \dots, r_k\}$. Für $i = 1, \dots, n$ sei $r_i \equiv x_1^{a_{i1}} \dots x_n^{a_{in}} \pmod{F'_X}$. Seien $d_1 \mid \dots \mid d_l$ die Elementarteiler von $A = (a_{ij}) \in \mathbb{Z}^{n \times k}$, wobei $l := \min\{n, k\}$. Dann ist $G/G' \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_l\mathbb{Z} \times \mathbb{Z}^{n-l}$. Insbesondere ist $|G| = |G/G'| = \infty$, falls $k < n$.*

Beweis. Sei $F := F_X$. Nach Beispiel 1.17 ist F/F' eine freie abelsche Gruppe vom Rang n . Für $N := \langle rF' : r \in R \rangle \leq F/F'$ gilt nun $G/G' \cong (F/F')/(F/N) \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$ (siehe Satz 24.21 in Algebra-Skript). □

Bemerkung 1.22.

- (i) Nach Satz 1.21 kann man algorithmisch entscheiden, ob eine Gruppe endlich präsentierte Gruppe perfekt ist (dennoch weiß man nicht, ob die Gruppe trivial ist).
- (ii) Es sind nur wenige *endliche* Gruppen $G = \langle X \mid R \rangle$ mit $|X| = |R|$ bekannt (zum Beispiel Q_{2^n} nach Aufgabe 2).⁷ Man vermutet sogar, dass sich jede solche Gruppe mit drei Elementen erzeugen lässt. Dies wurde für p -Gruppen bewiesen (vgl. Satz 5.25 und Aufgabe 22).

⁷Man spricht von einer *balancierten* Präsentation.

Beispiel 1.23. Sei $G = \langle x, y \mid x^2 = y^3 = (xy)^7 = 1 \rangle$. Dann erhält man die Matrix

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 7 & 7 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 2 & 0 \\ 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 0 & -2 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Also ist $G = G'$ perfekt. Man kann nachrechnen, dass die Matrizen

$$x = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

in $\text{GL}(3, 2)$ die Relationen erfüllen. Also gilt $G \neq 1$. Wir werden in Satz 10.50 zeigen, dass G unendlich ist.

Lemma 1.24. Sei N der normale Abschluss von $Y \subseteq X$ in F_X . Dann ist F_X/N frei bzgl. $X \setminus Y$.

Beweis. O.B.d.A. sei $\emptyset \neq Y \subset X$. Jedes Element von N ist ein Produkt von Elementen der Form gwg^{-1} mit $w \in \langle Y \rangle$ und $g \in F_X$. Die Summe der Exponenten eines Buchstaben $x \in X \setminus Y$ in gwg^{-1} ist 0, denn x kann nur in g und g^{-1} auftreten. Dies zeigt, dass die Abbildung $\sigma: X \setminus Y \rightarrow F/N$, $x \mapsto xN$ injektiv ist. Wir zeigen, dass F_X/N frei bezüglich $\sigma(X \setminus Y)$ ist. Sei G eine beliebige Gruppe und $\alpha: X \setminus Y \rightarrow G$ eine Funktion. Setzt man

$$\bar{\alpha}(x) := \begin{cases} 1 & \text{falls } x \in Y \\ \alpha(x) & \text{falls } x \notin Y \end{cases}$$

für $x \in X$, so erhält man eine Fortsetzung $\bar{\alpha}: X \rightarrow G$ von α . Da F frei bzgl. X ist, gibt es einen Homomorphismus $\bar{\beta}: F \rightarrow G$ mit $\bar{\beta}(x) = \bar{\alpha}(x)$ für alle $x \in X$. Offenbar ist dann $N \leq \text{Ker}(\bar{\beta})$. Daher gibt es einen Homomorphismus $\beta: F/N \rightarrow (F/N)/(\text{Ker}(\bar{\beta})/N) \rightarrow F/\text{Ker}(\bar{\beta}) \rightarrow G$ mit $\beta(\sigma(x)) = \alpha(x)$ für alle $x \in X \setminus Y$. Sei nun $\beta': F/N \rightarrow G$ ein weiterer Homomorphismus mit $\beta'(\sigma(x)) = \alpha(x)$ für alle $x \in X \setminus Y$. Wegen

$$F/N = \langle xN : x \in X \rangle = \langle xN : x \in X \setminus Y \rangle = \langle \sigma(x) : x \in X \setminus Y \rangle$$

folgt dann sofort $\beta = \beta'$. □

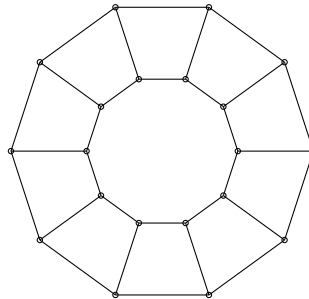
Bemerkung 1.25.

- (i) Der *Cayley-Graph* $\Omega(G, X)$ einer endlich erzeugten Gruppe $G = \langle X \mid R \rangle$ ist ein Graph mit Eckenmenge G , sodass $g, h \in G$ genau dann eine Kante bilden, wenn $g^{-1}h \in X \cup X^{-1}$ (durch $g^{-1}h \in X$ erhält man einen gerichteten Graphen). Offenbar hängt $\Omega(G, X)$ von X ab. Um Schleifen zu vermeiden, setzen wir $1 \notin X$ voraus. In jeden Fall ist $\Omega(G, X)$ zusammenhängend und regulär (d. h. alle Ecken haben die gleiche Anzahl an Kanten).
- (ii) Ein Kreis in $\Omega(G, X)$ entspricht einem reduzierten Wort $x_1^{\epsilon_1} \dots x_n^{\epsilon_n} = 1$. Daher ist $\Omega(G, X)$ genau dann ein Baum (d. h. kreisfrei), wenn G bzgl. X frei ist.
- (iii) Die Gruppe G permutiert durch Linksmultiplikation die Ecken und Kanten von $\Omega(G, X)$. Daher ist G eine Untergruppe von $\text{Aut}(\Omega(G, X))$. Auf dieser Grundlage lässt sich zeigen, dass jede endliche Gruppe die Automorphismengruppe eines Graphen ist (Satz von FRUCHT).

- (iv) Nach dem Satz von Euler-Hierholzer, ist $\Omega(G, X)$ genau dann eulersch, wenn $|X \cup X^{-1}|$ gerade ist. Das bedeutet es gibt einen geschlossenen Weg, der jede Kante von $\Omega(G, X)$ genau einmal besucht. Die offene Lovász-Vermutung besagt, dass $\Omega(G, X)$ für $2 < |G| < \infty$ hamiltonsch ist. Das bedeutet es gibt einen geschlossenen Weg, der jede Ecke von $\Omega(G, X)$ genau einmal besucht.
- (v) Ist G endlich, so lassen sich die Eigenwerte der Adjazenzmatrix von $\Omega(G, X)$ untersuchen. Man kann zeigen, dass sie in enger Verbindung zu den Werten der komplexen irreduziblen Charaktere von G stehen.

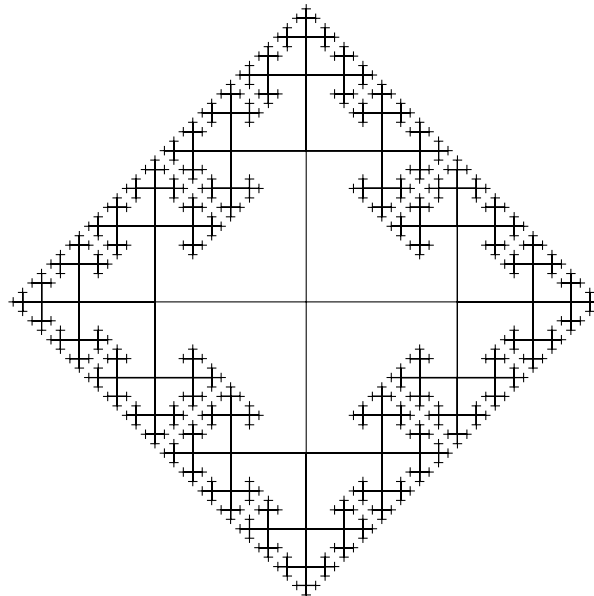
Beispiel 1.26.

- (i) Der Cayley-Graph von $G = \langle x \mid x^n \rangle$ bzgl. $X = \{x\}$ ist ein n -Eck. Wählt man $X = G$, so erhält man den vollständigen Graphen mit n Ecken.
- (ii) Sei $G = D_{2n}$ erzeugt von zwei Spiegelungen $X = \{x, y\}$. Dann ist $\Omega(G, X)$ eine $2n$ -Eck genau wie für C_{2n} . Der Cayley-Graph bestimmt also nicht, ob G abelsch ist. Wählt man hingegen $X = \{x, z\}$ mit einer Drehung z um $360^\circ/n$, so erhält man (mit $n = 10$):



Die beiden Kreise entsprechen den Nebenklassen $\langle z \rangle$ und $x\langle z \rangle$.

- (iii) Der Cayley-Graph von F_2 lässt sich (näherungsweise) als Fraktal zeichnen:



Interaktive Beispiele findet man unter <https://juliapoo.github.io/Cayley-Graph-Plotting/>.

- (iv) Sei $G = \langle X \rangle$ die Gruppe des $3 \times 3 \times 3$ -Zauberwürfel (Rubik's Cube) und X die Menge der 90° - und 180° -Drehungen der sechs Seitenflächen. Dann ist *God's Number* (20) der Durchmesser von $\Omega(G, X)$, also die maximale Länge eines kreisfreien Wegs (siehe Weihnachtsvorlesung Gruppentheorie).

Bemerkung 1.27 (GAP).

```
LoadPackage("grape",false);
G:=AlternatingGroup(5);;
Y:=[(1,2,3),(3,4,5)];; #X ist schreibgeschützt
C:=CayleyGraph(G,Y); #ersetzt Y durch  $Y \cup Y^{-1}$ 
Diameter(C);

LoadPackage("hap",false); #lädt weitere Pakete
G:=DihedralGroup(22);;
Y:=GeneratorsOfGroup(G);
CayleyGraphOfGroupDisplay(G,Y,"chromium"); #im Browser chromium ausgeben, benötigt GraphViz
```

2 Untergruppen freier Gruppen

Bemerkung 2.1. Wir wissen bereits, dass jede Gruppe eine Untergruppe (bzw. Faktorgruppe) einer symmetrischen (bzw. freien) Gruppe ist. Die Faktorgruppen einer endlichen symmetrischen Gruppe sind selbst symmetrisch (da A_n für $n \geq 5$ einfach ist). Wir zeigen dual dazu, dass die Untergruppen einer freien Gruppe selbst frei sind. Wir starten mit einer Variation der universellen Eigenschaft.

Lemma 2.2 (STEINBERG). *Eine Gruppe F ist genau dann frei bzgl. $X \subseteq F$, falls für jede nicht-leere Menge Ω und jede Abbildung $\sigma: X \rightarrow \text{Sym}(\Omega)$ genau eine Operation $F \rightarrow \text{Sym}(\Omega)$ mit ${}^x\omega = \sigma(x)(\omega)$ für alle $x \in X$ und $\omega \in \Omega$ existiert.*

Beweis. Ist F frei bzgl. X , so lässt sich σ nach der universellen Eigenschaft zu einer Operation mit der angegebenen Eigenschaft fortsetzen. Für die Umkehrung zeigen wir zunächst $F = \langle X \rangle$. Die Abbildung $\sigma: X \rightarrow \text{Sym}(\langle X \rangle)$ durch Linksmultiplikation (d. h. $\sigma(x)(y) = xy$) lässt sich zu einer Operation $\rho: F \rightarrow \text{Sym}(\langle X \rangle)$ fortsetzen. Man kann aber auch $\sigma: X \rightarrow \text{Sym}(F)$ betrachten und erhält wegen der Eindeutigkeit genau die gleiche Fortsetzung $\rho: F \rightarrow \text{Sym}(F)$. Da die Operation durch Linksmultiplikation transitiv ist, gilt $\langle X \rangle = F$.

Seien nun eine Gruppe G und eine Abbildung $\sigma: X \rightarrow G$ gegeben. Sei $\tau: G \rightarrow \text{Sym}(G)$ der Monomorphismus aus dem Satz von Cayley. Nach Voraussetzung existiert genau eine Operation $\rho: F \rightarrow \text{Sym}(G)$ mit $\rho(x) = \tau(\sigma(x))$ für alle $x \in X$. Dabei gilt $\rho(F) = \rho(\langle X \rangle) \leq \tau(G)$. Offenbar ist $\tau^{-1}\rho: F \rightarrow G$ ein Homomorphismus, der σ fortsetzt. Ist auch $\gamma: F \rightarrow G$ eine Fortsetzung von σ , so ist $\tau\gamma = \rho$ nach Voraussetzung. Dies zeigt $\gamma = \tau^{-1}\rho$. \square

Definition 2.3. Sei F frei bzgl. $X \subseteq F$ und $G \leq F$. Eine *Schreier-Transversale* für G ist ein Repräsentantensystem S für F/G mit folgender Eigenschaft: Ist $x^\epsilon s \in S$ reduziert mit $x \in X$ und $\epsilon = \pm 1$, so ist auch $s \in S$.

Lemma 2.4. *Jede Untergruppe einer freien Gruppe besitzt eine Schreier-Transversale.*

Beweis. Sei F frei bzgl. $X \subseteq F$ und $G \leq F$. Die Länge einer Nebenklasse aG sei die minimale Länge eines reduzierten Worts in aG . Wir konstruieren eine Schreier-Transversale S von G durch Induktion nach der Länge der Nebenklassen. Offenbar ist $1G$ die einzige Nebenklasse mit Länge 0. Sei also $1 \in S$. Sei nun aG mit Länge $l \geq 1$. Dabei habe a Länge l . Sei $a = x^\epsilon b$ reduziert mit $x \in X$ und $\epsilon = \pm 1$. Nach Induktion existiert $s \in S$ mit $sG = bG$. Wir wählen $x^\epsilon s \in S$ als Repräsentanten von aG . Offenbar entsteht auf diese Weise eine Schreier-Transversale. \square

Satz 2.5 (NIELSEN-SCHREIER). *Untergruppen von freien Gruppen sind frei.*

Beweis. Sei F frei bzgl. $X \subseteq F$ und $G \leq F$. Sei T eine Schreier-Transversale von G . Für $a \in F$ sei $\bar{a} \in T$ mit $aG = \bar{a}G$. Wir zeigen mit Lemma 2.2, dass G frei bzgl.

$$Y := \{(\bar{xt})^{-1}xt : (x, t) \in (X, T), xt \neq \bar{xt}\} \subseteq G$$

ist. Sei dafür $\sigma: Y \rightarrow \text{Sym}(\Omega)$ eine beliebige Abbildung. Wir erweitern σ durch die Vorschrift $\sigma(1) := \text{id}_\Omega$. Die Abbildung $f: X \rightarrow \text{Sym}(\Omega \times T)$ mit $f(x)(\omega, t) = (\sigma((\bar{xt})^{-1}xt)(\omega), \bar{xt})$ setzt sich zu einer Operation $\hat{f}: F \rightarrow \text{Sym}(\Omega \times T)$ fort. Wir zeigen, dass die Einschränkung $\hat{\sigma}: G \rightarrow \text{Sym}(\Omega \times \{1\})$ von \hat{f} die einzige homomorphe Fortsetzung von σ ist. Wir zeigen zunächst ${}^t(\omega, 1) = (\omega, t)$ für alle $t \in T$. Dies ist klar für $t = 1$. Sei also $t = x^\epsilon s$ reduziert mit $x \in X$, $\epsilon = \pm 1$. Da T eine Schreier-Transversale ist, gilt $s \in T$. Durch Induktion nach der Länge von t können wir ${}^s(\omega, 1) = (\omega, s)$ annehmen. Im Fall $\epsilon = 1$ folgt

$${}^t(\omega, 1) = {}^x(\omega, s) = (\sigma((\bar{xs})^{-1}xs)(\omega), t) = (\sigma(1)(\omega), t) = (\omega, t).$$

Sei nun $\epsilon = -1$. Dann gilt ${}^x(\omega, t) = (\sigma((\bar{xt})^{-1}xt)(\omega), xt) = (\omega, s)$ und

$${}^t(\omega, 1) = {}^{x^{-1}s}(\omega, 1) = {}^{x^{-1}}(\omega, s) = (\omega, t).$$

Sei nun $y := (\bar{xt})^{-1}xt \in Y$ beliebig. Dann gilt

$${}^{xt}(\omega, 1) = {}^x(\omega, t) = (\sigma(y)(\omega), \bar{xt}) = \bar{xt}(\sigma(y)(\omega), 1)$$

und $\hat{\sigma}(y) = \sigma(y)$. Also ist $\hat{\sigma}$ eine Fortsetzung von σ . Sei auch $\tau: G \rightarrow \text{Sym}(\Omega)$ eine Fortsetzung. Dann ist $\rho: F \rightarrow \text{Sym}(\Omega \times T)$ mit $\rho(a)(\omega, t) := (\tau((\bar{at})^{-1}at)(\omega), \bar{at})$ eine Operation, denn für $a, b \in F$ und $t \in T$ gilt

$$\begin{aligned} (\rho(a)\rho(b))(\omega, t) &= \rho(a)(\tau((\bar{bt})^{-1}bt)(\omega), \bar{bt}) = (\tau((\overline{abt})^{-1}\overline{abt})(\tau((\bar{bt})^{-1}bt)(\omega)), \overline{abt}) \\ &= (\tau((\overline{abt})^{-1}abt)(\omega), \overline{abt}) = \rho(ab)(\omega, t). \end{aligned}$$

Für $x \in X$ ist

$$\rho(x)(\omega, t) = (\tau((\bar{xt})^{-1}xt)(\omega), \bar{xt}) = (\sigma((\bar{xt})^{-1}xt)(\omega), \bar{xt}) = {}^x(\omega, t).$$

Wegen $F = \langle X \rangle$ stimmt ρ also mit der oben definierten Operation überein. Insbesondere ist $\tau = \hat{\sigma}$. \square

Bemerkung 2.6. Für Vektorräume (oder freie abelsche Gruppen) $U \leq V$ gilt bekanntlich $\dim U \leq \dim V$. Für freie Gruppen ist dies völlig falsch.

Satz 2.7 (SCHREIERS Formel). *Ist F frei und $G \leq F$ mit $|F : G| < \infty$, so gilt*

$$\boxed{\text{rk}(G) = |F : G|(\text{rk}(F) - 1) + 1.}$$

Beweis. Es genügt die Mächtigkeit der Menge Y in Satz 2.5 zu bestimmen. Seien $s, t \in T$ und $x, y \in X$ mit

$$(\overline{xt})^{-1}xt = (\overline{ys})^{-1}ys \neq 1.$$

Dann ist $xt, ys \notin T$. Da T eine Schreier-Transversale ist, müssen xt und ys reduziert sein. Angenommen $\overline{xt} = xt'$ ist reduziert. Dann folgt $t' \in T$ mit

$$t'G = x^{-1}xt'G = x^{-1}\overline{xt}G = x^{-1}xtG = tG,$$

also $t = t'$. Dies widerspricht der Wahl von x und t . Daher beginnt \overline{xt} nicht mit x . Folglich kann sich x nicht aus $(\overline{xt})^{-1}xt$ kürzen. Analog kürzt sich y nicht aus $(\overline{ys})^{-1}ys$. Da xt und ys reduziert sind, muss xt am Ende von ys vorkommen (oder ys am Ende von xt). Wäre xt tatsächlich kürzer als ys , so würde xt bereits in s vorkommen und man erhält den Widerspruch $xt \in T$. Also ist $xt = ys$ und es folgt $(x, t) = (y, s)$. Die aufgezählten Elemente von Y sind also paarweise verschieden.

Sei nun $t \in T \setminus \{1\}$. Sei $t = x^\epsilon s$ in reduzierter Form mit $x \in X$ und $\epsilon = \pm 1$. Da T eine Schreier-Transversale ist, gilt $s \in T$. Im Fall $\epsilon = 1$ ist $xs \in T$ und anderenfalls ist $xt \in T$. Daher bestimmt jedes $t \neq 1$ genau ein Paar $(x', t') \in X \times T$ mit $x't' \in T$. Umgekehrt entsteht jedes solche Paar auf diese Weise. Dies liefert

$$|Y| = |X \times T| - |T \setminus \{1\}| = |T|(|X| - 1) + 1 = |F : G|(\text{rk}(F) - 1) + 1. \quad \square$$

Beispiel 2.8. Sei $F_2 = \langle x, y \rangle$ und sei N der normale Abschluss von $\{x^2, y^2, (xy)^2\}$ in F_2 . Nach Beispiel 1.17 ist F_2/N die Kleinsche Vierergruppe. Nach Schreiers Formel ist $\text{rk } N = 4(2 - 1) + 1 = 5$. Wir wählen die Schreier-Transversale $\{1, x, y, xy\}$ von N in F_2 und berechnen

$$\begin{aligned} (\overline{xx})^{-1}xx &= x^2, & (\overline{xy})^{-1}xy &= y^{-1}x^2y, & (\overline{yy})^{-1}yy &= y^2, \\ (\overline{yx})^{-1}yx &= y^{-1}x^{-1}yx, & (\overline{yxy})^{-1}yxy &= x^{-1}yxy \end{aligned}$$

Also ist N frei bzgl. $\{x^2, y^2, y^{-1}x^2y, y^{-1}x^{-1}yx, x^{-1}yxy\}$.

Folgerung 2.9. Die Gruppe F_2 besitzt (freie) Untergruppen von jedem endlichen oder abzählbaren Rang. Für jede abzählbare Gruppe G existieren $N \trianglelefteq H \leq F_2$ mit $G \cong H/N$ (vgl. Satz 11.25).

Beweis. Sei $F_2 = \langle x, y \rangle$. Dann ist $G := \langle x \rangle \leq F_2$ mit $\text{rk } G = 1$ (Schreiers Formel gilt hier nicht wegen $|F : G| = \infty$). Für $n \in \mathbb{N}$ existiert $N \trianglelefteq F$ mit $F/N \cong C_n$ nach Satz 1.11. Schreiers Formel zeigt $\text{rk } N = n + 1$. Sei schließlich $N := F' = [F, F]$. Nach Beispiel 1.17 ist $F/N \cong \mathbb{Z}^2$. Daher bilden die Elemente $x^a y^b$ mit $a, b \in \mathbb{Z}$ eine Schreier-Transversale von N in F . Die im Beweis von Satz 2.5 konstruierte Menge Y umfasst die paarweise verschiedenen reduzierten Wörter $(\overline{yxy^b})^{-1}yxy^b = y^{-b-1}x^{-1}yxy^b$ mit $b \in \mathbb{Z}$. Daher ist $\text{rk } N = \infty$. Die zweite Aussage folgt aus Satz 1.11. \square

Bemerkung 2.10.

(i) Der Beweis von Folgerung 2.9 zeigt, dass nicht jede Untergruppe einer endlich erzeugten Gruppe endlich erzeugt sein muss ($\text{rk}(F_2') = \infty$).

(ii)

```
F:=FreeGroup("x","y");;
AssignGeneratorVariables(F);;
H:=Subgroup(F,[x^2,y^3,(x*y)^5]);;
IsFreeGroup(H);
Rank(H); #= 3
FreeGeneratorsOfGroup(H);
Index(F,H); #= \infty
```

```

N:=NormalClosure(F,H);;
Index(F,N); #= 60
GeneratorsOfGroup(N);; #Zwischenberechnung
Rank(N);

```

Satz 2.11. *Ist G endlich erzeugt und $H \leq G$ mit $|G : H| < \infty$, so ist auch H endlich erzeugt.*

Beweis. Sei $X = X^{-1}$ ein endliches Erzeugendensystem von G und R ein Repräsentantensystem für G/H mit $1 \in R$. Für $x \in X$ und $r \in R$ existieren $\alpha(x, r) \in H$ und $\gamma(x, r) \in R$ mit $xr = \gamma(x, r)\alpha(x, r)$. Jedes Element in H hat die Form $h = x_1 \dots x_n$ mit $x_1, \dots, x_n \in X$. Dabei gilt

$$\begin{aligned}
h &= x_1 \dots x_n 1 = x_1 \dots x_{n-1} \gamma(x_n, 1) \alpha(x_n, 1) = x_1 \dots x_{n-2} \gamma(x_{n-1}, \gamma(x_n, 1)) \alpha(x_{n-1}, \gamma(x_n, 1)) \alpha(x_n, 1) \\
&= \dots = \gamma(x_1, \dots) \alpha(x_1, \dots) \dots \alpha(x_n, 1).
\end{aligned}$$

Wegen $h \in H$ gilt dabei $\gamma(x_1, \dots) = 1$. Es folgt $H = \langle \alpha(x, r) : x \in X, r \in R \rangle$. \square

Bemerkung 2.12. Der Beweis von Satz 2.11 zeigt, dass man H mit $|G : H||X|$ Elementen erzeugen kann. Der nächste Satz gibt eine optimale Abschätzung.

Satz 2.13 (REIDEMEISTER-SCHREIER). *Sei $G = \langle X \mid R \rangle$ eine Gruppe und $H \leq G$. Dann lässt sich eine Präsentation $H = \langle Y \mid S \rangle$ aus X und R ableiten. Im Fall $|G : H| < \infty$ gilt $|Y| \leq |G : H|(|X| - 1) + 1$ und $|S| \leq |G : H||R|$.*

Beweis. Sei $F := F_X$ und $N := \langle R \rangle^F \trianglelefteq F$. Sei $\varphi : F \rightarrow G$ der Epimorphismus mit $\text{Ker}(\varphi) = N$. Sei $\tilde{H} = \varphi^{-1}(H) \leq F$. Dann ist $|F : \tilde{H}| = |F/N : \tilde{H}/N| = |G : H|$. Sei T eine Schreier-Transversale von \tilde{H} in F . Wie im Beweis von Satz 2.5 ist \tilde{H} frei bzgl.

$$Y := \{y_{xt} := (\overline{xt})^{-1}xt : (x, t) \in (X, T), y_{xt} \neq 1\} \subseteq \tilde{H}.$$

Insbesondere ist $\langle \varphi(Y) \rangle = \varphi(\tilde{H}) = H$. Sei zusätzlich

$$y_{x^{-1}t} = (\overline{x^{-1}t})^{-1}x^{-1}t = (t^{-1}\overline{xx^{-1}t})^{-1} = y_{x, x^{-1}t}^{-1}.$$

Für ein reduziertes Wort $w := x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \in F$ sei

$$\psi(w) := y_{x_n^{\epsilon_n}, x_1^{\epsilon_1} \dots x_{n-1}^{\epsilon_{n-1}}} y_{x_{n-1}^{\epsilon_{n-1}}, x_1^{\epsilon_1} \dots x_{n-2}^{\epsilon_{n-2}}} \dots y_{x_2^{\epsilon_2}, x_1^{\epsilon_1}} y_{x_1^{\epsilon_1}, 1} \in \tilde{H}$$

ein Wort in Y . Sei $S := \{\psi(t^{-1}rt) : t \in T, r \in R\}$. Wir zeigen $H \cong \langle Y \mid S \rangle$. Sei dafür $M := \langle S \rangle^{\tilde{H}} \trianglelefteq \tilde{H}$. Zunächst verifizieren wir $\psi(w) = \overline{w}^{-1}w$ für $w \in F$ durch Induktion nach $|w|$. Dies ist klar für $|w| \leq 1$. Sei nun $w = zx^\epsilon$ reduziert. Dann ist

$$\psi(w) = y_{x^\epsilon, \bar{z}} \psi(z) = (\overline{x^\epsilon z})^{-1} x^\epsilon \bar{z} \cdot \bar{z}^{-1} z = \overline{w}^{-1} w.$$

Für $h \in \tilde{H}$ folgt $\psi(h) = (\bar{h})^{-1}h = h$. Insbesondere ist $\psi(t^{-1}rt) = t^{-1}rt \in N$ für $r \in R$ und $t \in T$. Also gilt $S \subseteq N$ und $M \subseteq N$ wegen $N \trianglelefteq \tilde{H}$. Für die umgekehrte Inklusion genügt es $g^{-1}rg \in M$ für $g \in F$ und $r \in R$ zu zeigen. Sei $g = th$ mit $t \in T$ und $h \in \tilde{H}$. Dann ist $g^{-1}rg = h^{-1}t^{-1}rth = h^{-1}\psi(t^{-1}rt)h \in M$. Also ist $H \cong \tilde{H}/N = \tilde{H}/M = \langle Y \mid S \rangle$.

Die zweite Behauptung folgt aus Schreiers Formel und der Konstruktion von S . \square

Bemerkung 2.14 (GAP).

```
G:=SymmetricGroup(6);;
FG:=Image(IsomorphismFpGroup(G));;
FH:=DerivedSubgroup(FG);; #= $A_6$ 
P:=PresentationSubgroup(FG,FH,"y"); #Präsentation mit Erzeugern  $y_i$ 
TzPrintPresentation(P); #Statistik über Erzeuger und Relationen
```

Satz 2.15 (COXETER-TODD-Algorithmus). Sei $G = \langle X \mid R \rangle$ endlich präsentiert und $H \leq G$ mit $|G : H| < \infty$. Dann existiert ein Algorithmus, der die Operation von G auf G/H bestimmt. Insbesondere lässt sich $|G : H|$ aus einem Erzeugendensystem von H berechnen.

Beweisskizze. Nach Reidemeister-Schreier existiert ein endliches Erzeugendensystem Y von H . Sei $G/H = \{H = H_1, \dots, H_n\}$. Für $y = x_1^{\epsilon_1} \dots x_k^{\epsilon_k} \in Y$ sei $t_y := (t_1, \dots, t_k)$ mit $x_i^{\epsilon_i} \dots x_k^{\epsilon_k} H = H_{t_i}$ für $i = 1, \dots, k$. Wegen $y \in H$ ist $t_1 = 1$. Für $r = x_1^{\epsilon_1} \dots x_l^{\epsilon_l} \in R$ sei $T_r = (t_{ij}) \in \mathbb{N}^{n \times l}$ mit $x_m^{\epsilon_m} \dots x_l^{\epsilon_l} H_i = H_{t_{im}}$ für $m = 1, \dots, l$. Wegen $r = 1$ in G ist $t_{i1} = i$ für $i = 1, \dots, n$. Wir füllen die Vektoren t_y ($y \in Y$) und Matrizen T_r ($r \in R$) von links nach rechts und von oben nach unten, indem wir neue Nebenklassen zuweisen und alle logischen Folgerungen dabei berücksichtigen. Für jede neue Nebenklasse wird eine neue Zeile in T_r angefügt. Wegen $|G : H| < \infty$ sind irgendwann alle Einträge in t_y und T_r gefüllt. Außerdem kommt jedes $x \in X$ in einem $r \in R$ oder in einem Erzeuger von H vor. Auf diese Weise kann man die Operation von G auf G/H ablesen. Da G transitiv operiert, tauchen wirklich alle Nebenklassen in den Tabellen auf, d. h. man kann $n = |G : H|$ ablesen. \square

Beispiel 2.16. Sei $G = \langle x, y \mid x^3 = y^5 = (xy)^2 = 1 \rangle$ und $H := \langle y \rangle$. Der Vektor $t_y = (1)$ enthält hier keinerlei Information. Die erste Zeile von T_{y^5} ist $(1, 1, 1, 1, 1)$. Die Festlegung $H_2 := x^{-1}H_1 = x^2H$ ergibt folgende Einträge in T_{x^3} , T_{y^5} und $T_{(xy)^2}$:

x	x	x	y	y	y	y	y	x	y	x	y
1	2		1	1	1	1	1	1	2		1
2			2					2			

Sei nun $H_3 := x^{-1}H_2 = xH$. Dann ist $x^{-1}H_3 = H_1$ und $y^4H_2 = y^{-1}x^{-1}H = xyH = H_3$.

x	x	x	y	y	y	y	y	x	y	x	y
1	2	3	1	1	1	1	1	1	2	3	1
2	3	1	2	3				2	3		
3	1	2	3					3	1	1	2

Wir definieren weiter $H_4 := y^{-1}H_3$, $H_5 := x^{-1}H_4$, $H_6 := y^{-1}H_4$, $H_7 := x^{-1}H_5$ usw.

x	x	x	y	y	y	y	y	x	y	x	y
1	2	3	1	1	1	1	1	1	2	3	1
4	5	7	2	3	4	6	5	2	3	4	5
6	9	8	7	8	10	11	9	5	7	8	6
10	11	12	12	12	12	12	12	6	9	7	4
								9	8	10	11
								11	12	12	10

(redundante Zeilen wurden gestrichen). Man kann nun ablesen $|G| = |G : H||H| = 12|H| \leq 60$. In der Tat erfüllen die Permutationen $x = (1, 2, 3)$ und $y := (1, 4, 3, 5, 2)$ in A_5 die Relationen. Nach von-Dyck ist $G \cong \langle (1, 2, 3), (1, 4, 3, 5, 2) \rangle = A_5$.

Bemerkung 2.17 (GAP).

```
F:=FreeGroup(2);;
G:=F/[F.1^3,F.2^5,(F.1*F.2)^2];; #F.n ist der n-te Erzeuger
H:=Subgroup(G,[G.2]);;
CT:=CosetTable(G,H);;
Display(TransposedMat(CT)); #nur Spalten F.1^±1 und F.2^±1
f:=FactorCosetAction(G,H); #Operation auf G/H
StructureDescription(Image(f)); #entsprechende Permutationsgruppe

G:=F/[F.1^2,F.2^3,(F.1*F.2)^7];;
CT:=CosetTable(G,TrivialSubgroup(G));; #bricht nach 4096000 Nebenklassen ab (|G| = ∞)
```

Für kompliziertere Beispiele und bessere grafische Umsetzung kann man die Pakete ACE bzw. ICT (benötigt `xgap`) benutzen. Auf dem Cover ist die Tabelle für $A_6 \leq M_{11}$ angegeben.

Satz 2.18 (MOORE). Für $n \geq 2$ gilt

$$S_n \cong \langle x_1, \dots, x_{n-1} \mid 1 = x_i^2 = (x_j x_{j+1})^3 = (x_k x_l)^2 \text{ für } k < l - 1 \rangle.$$

Beweis. Sei G die Gruppe auf der rechten Seite. Für $n = 2$ gilt $G \cong C_2 \cong S_2$. Sei also $n > 2$ und $H := \langle x_1, \dots, x_{n-2} \rangle \leq G$. Nach Induktion ist H eine Faktorgruppe von S_{n-1} . Insbesondere ist $|H| \leq (n-1)!$. Wir zeigen, dass G folgende Nebenklassen permutiert:

$$H, x_{n-1}H, x_{n-2}x_{n-1}H, \dots, x_1 \dots x_{n-1}H.$$

Sicher ist

$$\begin{aligned} x_i(x_i x_{i+1} \dots x_{n-1}H) &= x_{i+1} \dots x_{n-1}H, \\ x_{i-1}(x_i x_{i+1} \dots x_{n-1}H) &= x_{i-1}x_i \dots x_{n-1}H. \end{aligned}$$

Für $j < i - 1$ gilt $x_i x_j = (x_i x_j)^{-1} = x_j x_i$ und

$$x_j(x_i x_{i+1} \dots x_{n-1}H) = x_i x_{i+1} \dots x_{n-1} x_j H = x_i x_{i+1} \dots x_{n-1}H.$$

Sei nun $j > i$. Wegen $(x_{j-1}x_j)^3 = 1$ gilt $x_{j-1}x_j x_{j-1} = x_j x_{j-1} x_j$. Es folgt

$$\begin{aligned} x_j(x_i x_{i+1} \dots x_{n-1}H) &= x_i \dots x_{j-2} (x_j x_{j-1} x_j) x_{j+1} \dots x_{n-1}H = x_i \dots x_{j-2} (x_{j-1} x_j x_{j-1}) x_{j+1} \dots x_{n-1}H \\ &= x_i \dots x_{n-1} x_{j-1} H = x_i \dots x_{n-1}H. \end{aligned}$$

Da G im Allgemeinen transitiv auf G/H operiert, ist $|G : H| \leq n$ und $|G| \leq n!$.

Umgekehrt erfüllen die Transpositionen $x'_i := (i, i+1) \in S_n$ für $i = 1, \dots, n-1$ die gleichen Relationen und wegen $S_n = \langle x'_1, \dots, x'_{n-1} \rangle$ folgt die Behauptung. \square

Satz 2.19 (MOORE). Für $n \geq 2$ gilt

$$A_n \cong \langle x_1, \dots, x_{n-2} \mid 1 = x_1^3 = x_2^2 = \dots = x_{n-2}^2 = (x_i x_{i+1})^3 = (x_k x_l)^2 \text{ für } k < l - 1 \rangle.$$

Beweis. Sei wieder G die rechte Seite. Für $n \leq 3$ stimmt die Behauptung. Sei $n \geq 4$ und $H := \langle x_1, \dots, x_{n-3} \rangle \leq G$. Nach Induktion ist $|H| \leq \frac{1}{2}(n-1)!$. Wir zeigen, dass G die folgenden n Nebenklassen permutiert

$$H, x_{n-2}H, x_{n-3}x_{n-2}H, \dots, x_1 \dots x_{n-2}H, x_1^2 x_2 \dots x_{n-2}H.$$

Solange kein x_1 involviert ist, geht dies wie in Satz 2.18. Für $i \geq 3$ gilt $x_1 x_i = x_i x_1^{-1}$ und

$$\begin{aligned} x_1 x_i \dots x_{n-2} H &= x_i \dots x_{n-2} x_1^{\pm 1} H = x_i \dots x_{n-2} H, \\ x_i x_1^{\pm 1} x_2 \dots x_{n-2} H &= x_1^{\mp 1} x_i x_2 \dots x_{n-2} H = x_1^{\mp 1} x_2 \dots x_{n-2} H. \end{aligned}$$

Aus $(x_1 x_2)^3 = 1$ folgt $x_2 x_1 x_2 = x_1^{-1} x_2 x_1^{-1}$ und

$$x_2 x_1^{\pm 1} \dots x_{n-2} H = x_1^{\mp 1} x_2 x_1^{\mp 1} x_3 \dots x_{n-2} H = x_1^{\mp 1} x_2 \dots x_{n-2} H.$$

Wie in Satz 2.18 erhält man $|G| \leq n|H| \leq |A_n|$. Umgekehrt erfüllen die Elemente $x_1 = (1, 2, 3)$, $x_i = (1, 2)(i+1, i+2)$ ($i = 2, \dots, n-2$) von A_n die angegebenen Relationen. \square

Bemerkung 2.20. GURALNICK-KANTOR-KASSABOV-LUBOTZKY haben gezeigt, dass man alle symmetrischen und alternierenden Gruppen mit zwei Erzeugern und acht Relationen präsentieren kann (oder drei Erzeuger und sieben Relationen⁸).

Definition 2.21. Ein reduziertes Wort $x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ einer freien Gruppe heißt *zyklisch reduziert*, falls $x_1^{\epsilon_1} \neq x_n^{-\epsilon_n}$.

Bemerkung 2.22. Für eine Gruppe $\langle X \mid r \rangle$ mit nur einer Relation kann man nach Konjugation stets annehmen, dass r zyklisch reduziert ist. Es gilt nun die folgende Verallgemeinerung von Lemma 1.24.

Satz 2.23 (MAGNUS' Freiheitssatz). *Sei $G = \langle X \mid r \rangle$, wobei r zyklisch reduziert sei. Kommt $x \in X$ in r vor, so ist $\langle X \setminus \{x\} \rangle \leq G$ frei bzgl. $X \setminus \{x\}$.*

Beweis. Siehe Satz 7.1 in [Camps et al., *Einführung in die kombinatorische und geometrische Gruppentheorie*, Heldermann Verlag, Lemgo, 2008] \square

3 Automorphismen freier Gruppen

Definition 3.1. Seien $X \subseteq X'$ Alphabete und $R \subseteq F_X$ mit normalem Abschluss $N \trianglelefteq F$. Die Transformationen

- $(X, R) \rightarrow (X, R \cup \{r\})$ mit $r \in N \setminus R$,
- $(X, R) \rightarrow (X \cup \{x\}, R \cup \{x^{-1}w\})$ mit $x \in X' \setminus X$ und $w \in F_X$

und ihre Umkehrabbildungen werden *Tietze-Transformationen* genannt.

Satz 3.2. *Zwei endlich präsentierte Gruppen $\langle X_1 \mid R_1 \rangle$ und $\langle X_2 \mid R_2 \rangle$ sind genau dann isomorph, wenn man (X_1, R_1) durch endlich viele Tietze-Transformationen in (X_2, R_2) überführen kann.*

⁸Die Präsentation war fehlerhaft und wurde von HUXFORD korrigiert.

Beweis. O.B.d.A. sei $X_1 \cap X_2 = \emptyset$. Sei $F_i := F_{X_i}$ und $N_i := \langle R_i \rangle^{F_i} \trianglelefteq F_i$. Für $r \in N_i$ gilt sicher $\langle R_i \cup \{r\} \rangle^{F_i} = N_i$ und $G_i := \langle X_i \mid R_i \rangle \cong \langle X_i \mid R_i \cup \{r\} \rangle$. Sei nun $x \in X' \setminus X_i$ und $w \in F_i$. Dann existiert ein Epimorphismus $\varphi: F_{X_i \cup \{x\}} \rightarrow G_i$ mit $\varphi(x_i) = x_i N_i$ für $x_i \in X_i$ und $\varphi(x) = w N_i$. Offenbar ist

$$N'_i := \langle R_i \cup \{x^{-1}w\} \rangle^{F_{X_i \cup \{x\}}} \subseteq \text{Ker}(\varphi).$$

Sei umgekehrt $y := y_1^{\epsilon_1} \dots y_n^{\epsilon_n} \in \text{Ker}(\varphi)$ mit $y_1, \dots, y_n \in X_i \cup \{x\}$. Sei $k := |\{1 \leq j \leq n : y_j = x\}|$. Gilt $k = 0$, so ist $y \in \text{Ker}(\varphi) \cap F_i = N_i \subseteq N'_i$. Sei nun $k > 0$. Um $y \in N'_i$ zu zeigen, können wir $y_n^{\epsilon_n} = x$ nach Konjugation annehmen. Es genügt dann $yx^{-1}w \in N'_i$ zu zeigen, aber das folgt mit Induktion nach k . Also ist $\text{Ker}(\varphi) = N'_i$ und $G_i \cong \langle X_i \cup \{x\} \mid R_i \cup \{x^{-1}w\} \rangle$. Wenn man $(X_1 \mid R_1)$ durch Tietze-Transformationen nach $(X_2 \mid R_2)$ überführen kann, so sind also G_1 und G_2 isomorph (dafür braucht man keine endliche Präsentation).

Sei nun umgekehrt $G := G_1 \cong G_2$. Dann existieren Epimorphismen $\varphi_i: F_i \rightarrow G$ mit Kern N_i für $i = 1, 2$. Sei $X := X_1 \cup X_2$ und $F := F_X$. Dann existiert ein Homomorphismus $\varphi: F \rightarrow G$, der φ_1 und φ_2 fortsetzt. Für $x \in X_1$ wählen wir $w_x \in F_2$ mit $\varphi(x) = \varphi_2(w_x) = \varphi(w_x)$. Sei $S_1 := \{s_x := x^{-1}w_x : x \in X_1\} \subseteq F$. Analog definieren wir S_2 . Durch eine offensichtliche (endliche) Folge von Tietze-Transformationen überführen wir (X_1, R_1) in $(X, R_1 \cup S_2)$. Sicher ist $N := \langle R_1 \cup S_2 \rangle^F \subseteq \text{Ker}(\varphi)$. Wie oben zeigt man $\text{Ker}(\varphi) \subseteq N$. Insbesondere ist $R_2 \cup S_1 \subseteq N$. Man kann also durch Tietze-Transformationen von $(X, R_1 \cup S_2)$ nach $(X, R_1 \cup R_2 \cup S_1 \cup S_2)$ übergehen. Die Situation ist nun symmetrisch. Man kann daher auch von (X_2, R_2) nach $(X, R_1 \cup R_2 \cup S_1 \cup S_2)$ übergehen. Die umgekehrten Tietze-Transformationen überführen schließlich (X_1, R_1) nach (X_2, R_2) . \square

Bemerkung 3.3. Die Befehle

`SimplifyPresentation (= TzGo), SimplifiedFpGroup, IsomorphismSimplifiedFpGroup`

führen stillschweigend Tietze-Transformationen durch, um eine endliche Präsentation $\langle X \mid R \rangle$ zu vereinfachen, d. h. $|X|$, $|R|$, und $\sum_{r \in R} l(r)$ werden minimiert. Man kann die Transformationen aber auch gezielt anwenden.

```
G:=PerfectGroup(768000,10); #perfekte Gruppe aus Datenbank
H:=Image(IsomorphismFpGroup(G));
P:=PresentationFpGroup(H,2); #Präsentation, print level=2, also mehr Ausgabe
TzGoGo(P); #iteriert Vereinfachungen mit Tietze-Transformation
TzPrintPresentation(P); #5 Erzeuger, 33 Relationen, Gesamtlänge 224
gen:=SmallGeneratingSet(G); #geht auch mit 2 Erzeugern
H:=Image(IsomorphismFpGroupByGenerators(G,gen)); #benutze diese
P:=PresentationFpGroup(H,2);
TzGoGo(P);
TzPrintPresentation(P); #2 Erzeuger, 59 Relationen, Gesamtlänge 3220

gen:=GeneratorsOfPresentation(P);
TzSubstitute(P,gen[1]^2*gen[2]); #führe zweite Tietze-Transformation mit w = x^2y durch
```

Definition 3.4. Sei $F = F_X$ und $x, y \in X$ mit $x \neq y$. Die Automorphismen

$$\alpha_x: F \rightarrow F, \quad z \mapsto \begin{cases} x^{-1} & \text{falls } z = x \\ z & \text{falls } z \neq x \end{cases},$$

$$\beta_{xy}: F \rightarrow F, \quad z \mapsto \begin{cases} xy & \text{falls } z = x \\ z & \text{falls } z \neq x \end{cases}$$

(wobei $z \in X$) heißen *Nielsen-Transformationen* (man beachte die Analogie zum Gauß-Algorithmus). Sei $\text{Aut}_N(F) := \langle \alpha_x, \beta_{xy} : x, y \in X, x \neq y \rangle \leq \text{Aut}(F)$.

Bemerkung 3.5. Für verschiedene $x, y \in X$ gilt

$$\begin{aligned}\alpha_y \beta_{xy} \alpha_x \beta_{yx} \alpha_y \beta_{xy}(x, y) &= \alpha_y \beta_{xy} \alpha_x \beta_{yx} \alpha_y(xy, y) = \alpha_y \beta_{xy} \alpha_x \beta_{yx}(xy^{-1}, y^{-1}) \\ &= \alpha_y \beta_{xy} \alpha_x(y^{-1}, x^{-1}y^{-1}) = \alpha_y \beta_{xy}(y^{-1}, xy^{-1}) = \alpha_y(y^{-1}, x) = (y, x).\end{aligned}$$

Also lässt sich jede Permutation auf X durch Nielsen-Transformationen realisieren.

Satz 3.6. Seien $w_1, \dots, w_n \in F = F_X$ und $\gamma \in \text{Aut}(F)$. Dann existiert ein $\delta \in \text{Aut}_N(F)$ mit $\delta(w_i) = \gamma(w_i)$ für $i = 1, \dots, n$. Insbesondere ist $\text{Aut}(F) = \text{Aut}_N(F)$, falls $|X| < \infty$.

Beweis. Sei $Y \subseteq X$ mit $|Y| < \infty$ und $w_1, \dots, w_n \in F_Y$. Es genügt ein $\delta \in \text{Aut}_N(F)$ mit $\gamma(y) = \delta(y)$ für alle $y \in Y$ zu konstruieren. Wegen $\langle \gamma^{-1}(X) \rangle = F$ existiert eine endliche Teilmenge $Z \subseteq X$ mit $Y \subseteq \langle \gamma^{-1}(Z) \rangle$. Wir können $Y \subseteq Z = \{x_1, \dots, x_n\}$ annehmen. Sei $w_i := \gamma^{-1}(x_i)$ reduziert für $i = 1, \dots, n$. Angenommen es existieren $1 \leq i, j \leq n$ mit $|w_i w_j| < |w_i|$. Offenbar ist dann $i \neq j$. Indem wir γ durch $\beta_{x_i x_j}^{-1} \gamma$ ersetzen, wird w_i durch $w_i w_j$ ersetzt, während sich w_k für $k \neq i$ nicht verändert. Auf diese Weise wird $\sum_{i=1}^n |w_i|$ kleiner. Im Fall $|w_i w_j| < |w_j|$ kann man analog die Transformationen $w_i \mapsto w_j \mapsto w_i w_j$ mittels Bemerkung 3.5 durchführen. Wir können also

$$|w_i w_j| \geq \max\{|w_i|, |w_j|\}$$

für $1 \leq i, j \leq n$ annehmen. Dies bedeutet, dass sich höchstens die Hälfte von w_i und w_j im Produkt $w_i w_j$ kürzen kann. Nehmen wir nun an, dass i, j, k existieren mit $|w_i w_j w_k| \leq |w_i| - |w_j| + |w_k|$. Sei dabei $w_i = as^{-1}$, $w_j = sbt^{-1}$ und $w_k = tc$, sodass $w_i w_j = abt^{-1}$ und $w_j w_k = sbc$ reduziert sind (beachte, dass sich jeweils nur die Hälfte von w_j links und rechts kürzen kann). Es gilt

$$|a| + |b| + |c| = |w_i w_j w_k| \leq |w_i| - |w_j| + |w_k| = |a| - |b| + |c|,$$

d. h. $b = 1$ und $|s| = |t|$. Wegen $|w_i| = |a| + |s| = |w_i w_j| \geq |w_j| = 2|s|$ gilt $|s| \leq \frac{1}{2}|w_i|$ und analog $|s| \leq \frac{1}{2}|w_k|$. Wir können nun w_i durch $w_i w_j$ ersetzen oder w_k durch $w_j w_k$ (tauschen von w_j und w_k ist machbar), ohne dass sich $\sum_{i=1}^n |w_i|$ ändert. Für $w \in F_Z$ sei $L(w)$ das linke Teilwort von w der Länge $\lfloor (|w| + 1)/2 \rfloor$. Sei \leq die lexikographische (Wohl-)Ordnung auf F_Z mit

$$1 < x_n^{-1} < x_{n-1} < \dots < x_1 < x_2 < \dots < x_n < x_n^{-2} < x_n^{-1} x_{n-1}^{-1} < \dots$$

Wir schreiben $w \prec v$, falls $\min\{L(w), L(w^{-1})\} < \min\{L(v), L(v^{-1})\}$ oder $(\min\{L(w), L(w^{-1})\} = \min\{L(v), L(v^{-1})\} \text{ und } \max\{L(w), L(w^{-1})\} < \max\{L(v), L(v^{-1})\})$, wobei das Minimum/Maximum bzgl. \leq zu bilden ist. Gilt in der obigen Situation $s < t$, so ist $w_j w_k = sc \prec tc = w_k$, denn $L(c^{-1}s^{-1}) = L(c^{-1}) = L(c^{-1}t^{-1})$. Ist $t < s$, so folgt $w_i w_j = at^{-1} \prec as^{-1} = w_i$. Durch geeignete Nielsen-Transformationen können wir also erreichen, dass die w_i möglichst klein bzgl. \prec sind (da \leq eine Wohlordnung ist, können die w_i nicht beliebig klein werden). Die Eigenschaft $|w_i w_j| \geq \max\{|w_i|, |w_j|\}$ bleibt dabei erhalten. Am Ende ist

$$|w_i w_j w_k| > |w_i| - |w_j| + |w_k|$$

für $1 \leq i, j, k \leq n$, d. h. w_j kürzt sich nicht vollständig in $w_i w_j w_k$. Das gleiche Verfahren lässt sich allgemeiner mit den Elementen $w_i^{\pm 1}$ durchführen.

Wegen $Y \subseteq \langle \gamma^{-1}(Z) \rangle$ lässt sich jedes $x_i \in Y$ als Produkt der w_j darstellen, sagen wir $x_i = w_{j_1}^{\epsilon_1} \dots w_{j_k}^{\epsilon_k}$. Nach Konstruktion gilt aber $1 = |x_i| = |w_{j_1}^{\epsilon_1} \dots w_{j_k}^{\epsilon_k}| \geq k$, d. h. $x_i = w_{j_1}^{\epsilon_1}$. Nach weiteren Nielsen-Transformationen wie in Bemerkung 3.5 erreicht man schließlich $w_i = x_i$ für $i = 1, \dots, n$. \square

Bemerkung 3.7.

- (i) NIELSEN hat eine endliche Präsentation von $\text{Aut}(F_n)$ bzgl. der Nielsen-Transformationen angegeben. NEWMAN hat gezeigt, dass man $\text{Aut}(F_n)$ mit nur zwei Automorphismen (unendlicher Ordnung) erzeugen kann.
- (ii) In GAP kann man Nielsen-Transformationen wie folgt konstruieren:

```

F:=FreeGroup("x","y");;
AssignGeneratorVariables(F);;
FreeGroupAutomorphismsGeneratorO(F); #Nielsen-Transformation  $\alpha_x$ 
FreeGroupAutomorphismsGeneratorU(F); # $\beta_{xy}$ 
FreeGroupAutomorphismsGeneratorP(F); # $(x,y) \mapsto (y,x)$ 
A:=AutomorphismGroup(F);; #Aut(F)
iso:=IsomorphismFpGroup(A);; #Isomorphismus von A zu einer endlich präsentierten
    Gruppe
a:=GroupHomomorphismByImages(F,F,[x,y],[x~y,x*y]); # $a \in A$ 
a~iso; #a als Wort in  $\alpha_x$ ,  $\beta_{xy}$  und  $(x,y) \mapsto (y,x)$ 

```

Satz 3.8. Sei $\Phi: \text{Aut}(F_n) \rightarrow \text{GL}(n, \mathbb{Z})$, wobei $\Phi(\alpha)_{ij}$ die Exponentensumme von x_j in $\alpha(x_i)$ ist. Dann ist Φ ein Epimorphismus.

Beweis. Die Abbildung Φ entsteht aus der Einschränkung

$$\text{Aut}(F_n) \rightarrow \text{Aut}(F_n/F'_n) \cong \text{Aut}(\mathbb{Z}^n) \cong \text{GL}(n, \mathbb{Z})$$

und ist daher ein wohldefinierter Homomorphismus. Für die Surjektivität genügt es zu zeigen, dass jede Matrix $A \in \text{GL}(n, \mathbb{Z})$ ein Produkt von $\Phi(\alpha_x)$ und $\Phi(\beta_{xy})$ ist. Linksmultiplikation (bzw. Rechtsmultiplikation) mit $\Phi(\alpha_x)$ bewirkt, dass eine Zeile (bzw. Spalte) von A mit -1 multipliziert wird. Durch $\Phi(\beta_{xy})$ kann man eine Zeile (bzw. Spalte) von A zu einer anderen Zeile (bzw. Spalte) addieren. Wie in Bemerkung 3.5 kann man Zeilen und Spalten von A auch vertauschen. Mit diesen Operationen lässt sich A auf die Smith-Normalform bringen. Wegen $\det A = \pm 1$ sind alle Elementarteiler 1, d. h. A lässt sich zur Einheitsmatrix überführen. \square

4 Gruppen-Erweiterungen

Bemerkung 4.1. Nach dem Satz von Jordan-Hölder sind alle endlichen Gruppen (oder solche die eine Kompositionsreihe besitzen) aus einfachen Gruppen aufgebaut. Die endlichen einfachen Gruppen sind bekanntlich vollständig klassifiziert. Es bleibt zu untersuchen, wie sich eine Gruppe aus Normalteilern und Faktorgruppen zusammensetzt.

Definition 4.2.

- Eine (Gruppen-)Erweiterung von H mit N ist eine kurze exakte Folge von Gruppen

$$1 \rightarrow N \xrightarrow{\nu} G \xrightarrow{\pi} H \rightarrow 1,$$

d. h. $N \cong \nu(N) \trianglelefteq G$ und $G/\nu(N) \cong \pi(G) = H$.⁹

⁹Achtung: Dieser Sprachgebrauch ist in der Literatur nicht einheitlich.

- Wir nennen G eine *zerfallende* Erweiterung, falls ein Homomorphismus $\rho: H \rightarrow G$ mit $\pi \circ \rho = \text{id}_H$ existiert. Gegebenenfalls ist $\rho(H)$ ein Komplement von $\nu(N)$ in G und $G \cong N \rtimes H$. Umgekehrt ist jedes semidirekte Produkt eine zerfallende Erweiterung.
- Zwei Gruppen-Erweiterungen G_1, G_2 von H mit N heißen *äquivalent*, falls ein Homomorphismus $\gamma: G_1 \rightarrow G_2$ mit $\gamma \circ \nu_1 = \nu_2$ und $\pi_2 \circ \gamma = \pi_1$ existiert. Das heißt, das folgende Diagramm kommutiert:

$$\begin{array}{ccccc}
 & & G_1 & & \\
 & \nearrow \nu_1 & \downarrow \gamma & \nwarrow \pi_1 & \\
 N & & & & H \\
 & \searrow \nu_2 & & \nearrow \pi_2 & \\
 & & G_2 & &
 \end{array}$$

Bemerkung 4.3.

- Jede Gruppe G mit Normalteiler N ist eine Erweiterung von $H = G/N$ mit N , indem man für ν die Inklusion und für π den kanonischen Epimorphismus wählt.
- Seien G_1 und G_2 äquivalente Erweiterungen mittels $\gamma: G_1 \rightarrow G_2$. Sei $x \in \text{Ker}(\gamma)$. Wegen $\pi_1(x) = \pi_2(\gamma(x)) = 1$ ist $x \in \nu_1(N)$, sagen wir $x = \nu_1(y)$. Aus $\nu_2(y) = \gamma(\nu_1(y)) = \gamma(x) = 1$ folgt $y = 1 = x$. Daher ist γ injektiv. Für $g \in G_2$ existiert $x \in G_1$ mit $\pi_2(\gamma(x)) = \pi_1(x) = \pi_2(g)$. Also existiert $y \in N$ mit $g^{-1}\gamma(x) = \nu_2(y) = \gamma(\nu_1(y))$. Dies zeigt $g = \gamma(G_1)$ und γ ist surjektiv. Insgesamt gilt $G_1 \cong G_2$. Die Äquivalenz von Gruppen ist daher eine Äquivalenzrelation.
- Isomorphe Erweiterungen müssen allerdings nicht äquivalent sein: Sei

$$G_1 = G_2 = \langle x, y \mid x^4 = y^2 = 1, yxy = x^{-1} \rangle \cong D_8,$$

$N = \langle x^2, y \rangle \cong C_2^2$ und $H = \langle xy \rangle$. Sei ν_1 die Inklusion, $\nu_2(x^2) = y$ und $\nu_2(y) = x^2$. Seien π_1 und π_2 die kanonischen Epimorphismen. Wegen $Z(G_i) = \langle x^2 \rangle$ kann es kein $\gamma \in \text{Aut}(G_i)$ mit $\gamma(x^2) = \gamma(\nu_1(x^2)) = \nu_2(x^2) = y$ geben. Dennoch ist es nützlich Erweiterungen bis auf Äquivalenz bestimmen zu können.

- Seien G_1 und G_2 äquivalente Erweiterungen von H mit N bzgl. $\gamma: G_1 \rightarrow G_2$. Angenommen G_1 zerfällt mit $\rho_1: H \rightarrow G_1$ und $\pi_1 \rho_1 = \text{id}_H$. Für $\rho_2 := \gamma \rho_1: H \rightarrow G_2$ gilt $\pi_2 \rho_2 = \pi_2 \gamma \rho_1 = \pi_1 \rho_1 = \text{id}_H$. Also zerfällt auch G_2 .
- Ohne die im Folgenden beschriebenen Methoden kann man Erweiterungen in GAP mit dem `grpconst`-Paket konstruieren:

```

LoadPackage("grpconst",false);
G:=AlternatingGroup(6);; #das Paket erwartet eine Permutationsgruppe
up:=UpwardsExtensions(G,2)[2]; #Erweiterungen von G mit C2
List(up,IdGroup);
P:=DihedralGroup(IsPermGroup,32);;
up:=CyclicExtensions(P,2);; #ist schneller, aber reduziert nicht bis auf Isomorphie
Size(up)=Size(Set(up,IdGroup)); #false, also Liste redundant
UpwardsExtensionsNoCentre(G,2); #funktioniert nur für G = G' und Z(G) = 1

```

Definition 4.4. Seien H und N Gruppen. Für $x \in N$ sei $c_x \in \text{Inn}(N)$ der innere Automorphismus (d. h. $c_x(y) = xyx^{-1}$). Ein Paar von Abbildungen

$$\alpha: H \rightarrow \text{Aut}(N), \quad x \mapsto \alpha_x, \quad \kappa: H \times H \rightarrow N$$

heißt *Parametersystem* von H mit N , falls für alle $x, y, z \in H$ gilt:

- $\boxed{\alpha_x \alpha_y = c_{\kappa(x, y)} \alpha_{xy}},$
- $\boxed{\kappa(x, y) \kappa(xy, z) = \alpha_x(\kappa(y, z)) \kappa(x, yz)}.$

Ggf. nennt man α *Automorphismensystem* und κ *Faktorensystem*. Ein Parametersystem (oder Faktorensystem) heißt *normalisiert*, falls $\kappa(x, 1) = \kappa(1, x) = 1$ für alle $x \in H$ gilt (ggf. ist $\alpha_1 = \text{id}_N$). Schließlich heißt κ *trivial*, falls $\kappa(x, y) = 1$ für alle $x, y \in G$ (ggf. ist α ein Homomorphismus).

Lemma 4.5. *Jede Erweiterung von H mit N bestimmt ein (normalisiertes) Parametersystem.*

Beweis. Sei $N \xrightarrow{\nu} G \xrightarrow{\pi} H$ eine Erweiterung. Für $x \in H$ wählen wir $\tilde{x} \in G$ mit $\pi(\tilde{x}) = x$ und $\tilde{1} = 1$. Dann ist $\alpha_x: N \rightarrow N, y \mapsto \nu^{-1}(\tilde{x}\nu(y)\tilde{x}^{-1})$ ein Automorphismus (beachte: ν ist injektiv) und $\alpha_1 = \text{id}_N$. Für $x, y \in H$ ist $\pi(\tilde{x}\tilde{y}) = xy = \pi(\tilde{x})\pi(\tilde{y}) = \pi(\tilde{x}\tilde{y})$. Daher existiert $\kappa(x, y) \in N$ mit $\tilde{x}\tilde{y} = \nu(\kappa(x, y))\tilde{x}\tilde{y}$. Dabei gilt $\kappa(x, 1) = \kappa(1, x) = 1$. Für $g \in N$ gilt

$$\begin{aligned} (\alpha_x \alpha_y)(g) &= \alpha_x(\nu^{-1}(\tilde{y}\nu(g)\tilde{y}^{-1})) = \nu^{-1}(\tilde{x}\tilde{y}\nu(g)\tilde{y}^{-1}\tilde{x}^{-1}) = \nu^{-1}(\nu(\kappa(x, y))\tilde{x}\tilde{y}\nu(g)\tilde{x}\tilde{y}^{-1}\nu(\kappa(x, y)^{-1})) \\ &= \kappa(x, y)\nu^{-1}(\tilde{x}\tilde{y}\nu(g)\tilde{x}\tilde{y}^{-1})\kappa(x, y)^{-1} = c_{\kappa(x, y)}\alpha_{xy}(g). \end{aligned}$$

Für $x, y, z \in H$ gilt

$$\begin{aligned} \nu(\kappa(x, y))\nu(\kappa(xy, z))\tilde{x}\tilde{y}\tilde{z} &= \nu(\kappa(x, y))\tilde{x}\tilde{y}\tilde{z} = (\tilde{x}\tilde{y})\tilde{z} = \tilde{x}(\tilde{y}\tilde{z}) = \tilde{x}\nu(\kappa(y, z))\tilde{y}\tilde{z} \\ &= \nu(\alpha_x(\kappa(y, z)))\tilde{x}\tilde{y}\tilde{z} = \nu(\alpha_x(\kappa(y, z)))\nu(\kappa(x, yz))\tilde{x}\tilde{y}\tilde{z}. \end{aligned}$$

Da ν injektiv ist, folgt die Behauptung. □

Beispiel 4.6.

- Ist $G = N \rtimes H$, so kann man $\tilde{x} \in H$ im obigen Beweis wählen. Man erhält dann das triviale Faktorensystem und für $\alpha: H \rightarrow \text{Aut}(N)$ die Konjugationsoperation.
- Ist $x \in H$ mit $x^2 \neq 1$, so kann man $\tilde{x}^{-1} = \tilde{x}^{-1}$ im obigen Beweis wählen. Man erhält dann $\kappa(x, x^{-1}) = 1$.
- Sei $G = \langle x, y \rangle = Q_8$, $N = \langle x \rangle \cong C_4$, ν die Inklusion und $H = \langle z \rangle \cong C_2$. Wir können $\tilde{z} = y$ wählen. Man erhält $\kappa(z, z) = \tilde{z}^2(\tilde{z}^2)^{-1} = y^2 \neq 1$.
- Sei $n \in \mathbb{N}$ und $H = \langle x \rangle \cong C_n \cong \langle a \rangle = N$. Für $i, j \in \mathbb{Z}$ sei $\alpha_{x^i} := \text{id}_N$ und $\kappa(x^i, x^j) := a^{ij}$ (wohldefiniert!). Dann gilt

$$\kappa(x^i, x^j) \kappa(x^i x^j, x^k) = x^{ij+(i+j)k} = x^{jk+i(j+k)} = \kappa(x^j, x^k) \kappa(x^i, x^j x^k).$$

Daher ist (α, κ) ein normalisiertes Parametersystem.

Lemma 4.7. *Jedes normalisierte Parametersystem von H mit N bestimmt eine Erweiterung.*

Beweis. Sei (α, κ) ein normalisiertes Parametersystem von H mit N . Wir betrachten die Menge $G = N \times H$ mit der Verknüpfung

$$(a, x)(b, y) := (a\alpha_x(b)\kappa(x, y), xy).$$

Dann gilt

$$\begin{aligned} ((a, x)(b, y))(c, z) &= (a\alpha_x(b)\kappa(x, y), xy)(c, z) = (a\alpha_x(b)\kappa(x, y)\alpha_{xy}(c)\kappa(xy, z), xyz) \\ &= (a\alpha_x(b)\kappa(x, y)\alpha_{xy}(c)\kappa(x, y)^{-1}\kappa(x, y)\kappa(xy, z), xyz) \\ &= (a\alpha_x(b)\alpha_x(\alpha_y(c))\alpha_x(\kappa(y, z))\kappa(x, yz), xyz) \\ &= (a\alpha_x(b\alpha_y(c)\kappa(y, z))\kappa(x, yz), xyz) \\ &= (a, x)(b\alpha_y(c)\kappa(y, z), yz) = (a, x)((b, y)(c, z)). \end{aligned}$$

Die Verknüpfung ist daher assoziativ. Da κ normalisiert ist, ist $(1, 1)$ ein neutrales Element. Inverse Elemente erhält man durch

$$(\kappa(y^{-1}, y)^{-1}\alpha_{y^{-1}}(b)^{-1}, y^{-1})(b, y) = (\kappa(y^{-1}, y)^{-1}\alpha_{y^{-1}}(b)^{-1}\alpha_{y^{-1}}(b)\kappa(y^{-1}, y), y^{-1}y) = (1, 1).$$

Also ist G eine Gruppe. Offenbar ist $\nu: N \rightarrow G, a \mapsto (a, 1)$ ein Monomorphismus und $\pi: G \rightarrow H, (a, x) \mapsto x$ ein Epimorphismus mit $\nu(N) = N \times 1 = \text{Ker}(\pi)$. \square

Bemerkung 4.8.

- (i) Für das triviale Faktorensystem ergibt sich im obigen Beweis das semidirekte Produkt $N \rtimes H$.
- (ii) Sei (α, κ) ein normalisiertes Parametersystem mit $\alpha_x = \text{id}_N$ für alle $x \in H$ (wir schreiben dafür $\alpha = 1$). Wegen $c_{\kappa(x, y)} = c_{\kappa(x, y)}\alpha_{xy} = \alpha_x\alpha_y = \text{id}_N$ ist $\kappa(H \times H) \leq Z(N)$. Sei G die entsprechende Erweiterung und $K := \langle (1, x) : x \in H \rangle$. Wegen

$$\begin{aligned} (a, x)(1, y)(a, x)^{-1} &= (a\kappa(x, y), xy)(\kappa(x^{-1}, x)^{-1}a^{-1}, x^{-1}) \\ &= (a\kappa(x, y)\kappa(x^{-1}, x)^{-1}a^{-1}\kappa(xy, x^{-1}), xyx^{-1}) = (1, x)(1, y)(1, x)^{-1} \in K \end{aligned}$$

ist $K \trianglelefteq G$ und $N \cap K \leq \kappa(H \times H) \leq Z(G)$. Also ist $G = N * K$ ein Zentralprodukt.

Definition 4.9. Zwei Parametersysteme $(\alpha, \kappa), (\alpha', \kappa')$ heißen *äquivalent*, falls eine Abbildung $\varphi: H \rightarrow N$ mit

- $\alpha'_x = c_{\varphi(x)}\alpha_x,$
- $\kappa'(x, y) = \varphi(x)\alpha_x(\varphi(y))\kappa(x, y)\varphi(xy)^{-1}$

für alle $x, y \in H$ existiert. Ggf. schreiben wir $(\alpha, \kappa) \sim (\alpha', \kappa')$.

Bemerkung 4.10. Die Abbildungen $H \rightarrow N$ bilden eine Gruppe $C^1(H, N)$ bzgl. $(\varphi\psi)(x) := \varphi(x)\psi(x)$ ($x \in H$), die zu $\times_{h \in H} N$ isomorph ist. Wir zeigen, dass ${}^\varphi(\alpha, \kappa) := (\alpha', \kappa')$ wie in Definition 4.9 eine

Operation von $C^1(H, N)$ auf der Menge der Parametersysteme definiert. Zunächst muss gezeigt werden, dass (α', κ') ein Parametersystem ist:

$$\begin{aligned}
\alpha'_x \alpha'_y &= c_{\varphi(x)} \alpha_x c_{\varphi(y)} \alpha_y = c_{\varphi(x)} \alpha_x c_{\varphi(y)} \alpha_x^{-1} \alpha_x \alpha_y = c_{\varphi(x)} c_{\alpha_x(\varphi(y))} c_{\kappa(x,y)} \alpha_{xy} = c_{\kappa'(x,y)} \alpha'_{xy} \\
\kappa'(x, y) \kappa'(xy, z) &= \varphi(x) \alpha_x(\varphi(y)) \kappa(x, y) \alpha_{xy}(\varphi(z)) \kappa(xy, z) \varphi(xyz)^{-1} \\
&= \varphi(x) \alpha_x(\varphi(y)) (c_{\kappa(x,y)} \alpha_{xy}) (\varphi(z)) \kappa(x, y) \kappa(xy, z) \varphi(xyz)^{-1} \\
&= \varphi(x) \alpha_x(\varphi(y)) (\alpha_x \alpha_y) (\varphi(z)) \alpha_x(\kappa(y, z)) \kappa(x, yz) \varphi(xyz)^{-1} \\
&= \varphi(x) \alpha_x(\varphi(y) \alpha_y(\varphi(z)) \kappa(y, z)) \kappa(x, yz) \varphi(xyz)^{-1} \\
&= (c_{\varphi(x)} \alpha_x)(\kappa'(y, z)) \varphi(x) \alpha_x(\varphi(yz)) \kappa(x, yz) \varphi(xyz)^{-1} \\
&= \alpha'_x(\kappa'(y, z)) \kappa'(x, yz).
\end{aligned}$$

Sicher ist ${}^1(\alpha, \kappa) = (\alpha, \kappa)$. Sei $\varphi, \psi \in C^1(H, N)$ mit ${}^\psi(\alpha, \kappa) = (\alpha', \kappa')$. Dann gilt

$$\begin{aligned}
c_{\varphi(x)} \alpha'_x &= c_{\varphi(x)} c_{\psi(x)} \alpha_x = c_{\varphi(x)\psi(x)} \alpha_x = c_{(\varphi\psi)(x)} \alpha_x, \\
\varphi(x) \alpha'_x(\varphi(y)) \kappa'(x, y) \varphi(xy)^{-1} &= \varphi(x) \psi(x) \alpha_x(\varphi(y)) \alpha_x(\psi(y)) \kappa(x, y) \psi(xy)^{-1} \varphi(xy)^{-1} \\
&= (\varphi\psi)(x) \alpha_x((\varphi\psi)(y)) \kappa(x, y) (\varphi\psi)(xy)^{-1}.
\end{aligned}$$

Dies zeigt ${}^\varphi({}^\psi(\alpha, \kappa)) = {}^{\varphi\psi}(\alpha, \kappa)$. Die Äquivalenzklassen von Parametersystemen sind also die Bahnen unter $C^1(H, N)$. Insbesondere ist \sim eine Äquivalenzrelation. Die Anzahl der Äquivalenzklassen könnte man mit Burnside's Lemma bestimmen.

Lemma 4.11. *Jedes Parametersystem ist zu einem normalisierten Parametersystem äquivalent.*

Beweis. Sei (α, κ) ein beliebiges Parametersystem und $\zeta := \kappa(1, 1) \in N$. Wegen $\alpha_1 \alpha_1 = c_\zeta \alpha_1$ ist $\alpha_1 = c_\zeta$. Aus

$$\zeta \kappa(1 \cdot 1, x) = \alpha_1(\kappa(1, x)) \kappa(1, 1x) = \zeta \kappa(1, x) \zeta^{-1} \kappa(1, x),$$

folgt $\kappa(1, x) = \zeta$ für alle $x \in H$. Mit $\kappa(x, 1) \kappa(x1, 1) = \alpha_x(\zeta) \kappa(x, 1 \cdot 1)$ ist $\kappa(x, 1) = \alpha_x(\zeta)$.

Definiere nun $\varphi(1) := \zeta^{-1}$ und $\varphi(y) := 1$ für $y \in H \setminus \{1\}$. Dann gilt

$$\begin{aligned}
\varphi(x) \alpha_x(\varphi(1)) \kappa(x, 1) \varphi(x)^{-1} &= \varphi(x) \alpha_x(\zeta)^{-1} \alpha_x(\zeta) \varphi(x)^{-1} = 1, \\
\varphi(1) \alpha_1(\varphi(x)) \kappa(1, x) \varphi(x)^{-1} &= \zeta^{-1} \zeta \varphi(x) \zeta^{-1} \zeta \varphi(x)^{-1} = 1
\end{aligned}$$

für alle $x \in H$. Auf diese Weise erhält man ein äquivalentes normalisiertes Parametersystem. \square

Lemma 4.12. *Äquivalente Erweiterungen definieren äquivalente Parametersysteme.*

Beweis. Seien $N \xrightarrow{\nu_1} G_1 \xrightarrow{\pi_1} H$ und $N \xrightarrow{\nu_2} G_2 \xrightarrow{\pi_2} H$ äquivalente Erweiterungen mittels $\gamma: G_1 \rightarrow G_2$. Für $x \in H$ sei $\tilde{x} \in G_1$ und $\bar{x} \in G_2$ mit $\pi_1(\tilde{x}) = x = \pi_2(\bar{x})$. Wie im Beweis von Lemma 4.5 erhält man Parametersysteme (α, κ) und (α', κ') mit

$$\begin{aligned}
\alpha_x(g) &= \nu_1^{-1}(\tilde{x} \nu_1(g) \tilde{x}^{-1}), & \kappa(x, y) &= \nu_1^{-1}(\tilde{x} \tilde{y} \tilde{x} \tilde{y}^{-1}), \\
\alpha'_x(g) &= \nu_2^{-1}(\bar{x} \nu_2(g) \bar{x}^{-1}), & \kappa'(x, y) &= \nu_2^{-1}(\bar{x} \bar{y} \bar{x} \bar{y}^{-1})
\end{aligned}$$

für $x, y \in H$ und $g \in N$. Wegen $\pi_2(\gamma(\tilde{x})) = \pi_1(\tilde{x}) = x = \pi_2(\bar{x})$ können wir

$$\varphi(x) := \nu_2^{-1}(\bar{x} \gamma(\tilde{x})^{-1}) \in N$$

für $x \in H$ definieren. Wegen $\gamma\nu_1 = \nu_2$ ist $\varphi(x) = \nu_1^{-1}(\gamma^{-1}(\bar{x})\tilde{x}^{-1})$. Es folgt

$$\begin{aligned} (c_{\varphi(x)}\alpha_x)(g) &= \nu_1^{-1}(\gamma^{-1}(\bar{x})\tilde{x}^{-1})\nu_1^{-1}(\tilde{x}\nu_1(g)\tilde{x}^{-1})\nu_1^{-1}(\tilde{x}\gamma^{-1}(\bar{x})^{-1}) = \nu_1^{-1}(\gamma^{-1}(\bar{x})\nu_1(g)\gamma^{-1}(\bar{x})^{-1}) \\ &= \nu_1^{-1}(\gamma^{-1}(\bar{x}\nu_2(g)\bar{x}^{-1})) = \nu_2^{-1}(\bar{x}\nu_2(g)\bar{x}^{-1}) = \alpha'_x(g) \end{aligned}$$

und

$$\begin{aligned} \varphi(x)\alpha_x(\varphi(y))\kappa(x, y)\varphi(xy)^{-1} &= \nu_1^{-1}(\gamma^{-1}(\bar{x})\tilde{x}^{-1})\nu_1^{-1}(\tilde{x}\nu_1(\varphi(y))\tilde{x}^{-1})\nu_1^{-1}(\tilde{x}\tilde{y}\tilde{x}\tilde{y}^{-1})\nu_1^{-1}(\tilde{x}\tilde{y}\gamma^{-1}(\bar{xy})^{-1}) \\ &= \nu_1^{-1}(\gamma^{-1}(\bar{x})\nu_1(\varphi(y))\tilde{y}\gamma^{-1}(\bar{xy})^{-1}) \\ &= \nu_1^{-1}(\gamma^{-1}(\bar{x})\gamma^{-1}(\bar{y})\gamma^{-1}(\bar{xy})^{-1}) = \nu_2^{-1}(\bar{xy}\bar{xy}^{-1}) = \kappa'(x, y). \end{aligned}$$

Daher sind (α, κ) und (α', κ') äquivalent. \square

Lemma 4.13. *Äquivalente (normalisierte) Parametersysteme definieren äquivalente Erweiterungen.*

Beweis. Seien (α, κ) und (α', κ') äquivalente Parametersysteme mittels $\varphi: H \rightarrow N$. Nach Lemma 4.11 können wir annehmen, dass beide Parametersysteme normalisiert sind. Dann gilt

$$1 = \kappa'(1, x) = \varphi(1)\alpha_1(\varphi(x))\kappa(1, x)\varphi(x)^{-1} = \varphi(1).$$

Wir konstruieren (G_1, \cdot) und $(G_2, *)$ wie im Beweis von Lemma 4.7. Da G_1 und G_2 als Mengen gleich sind, können wir $\gamma: G_1 \rightarrow G_2$, $(a, x) \mapsto (a\varphi(x)^{-1}, x)$ definieren. Für $(a, x), (b, y) \in G_1$ gilt

$$\begin{aligned} \gamma(a, x) * \gamma(b, y) &= (a\varphi(x)^{-1}, x) * (b\varphi(y)^{-1}, y) = (a\varphi(x)^{-1}\alpha'_x(b\varphi(y)^{-1})\kappa'(x, y), xy) \\ &= (a\alpha_x(b\varphi(y)^{-1})\alpha_x(\varphi(y))\kappa(x, y)\varphi(xy)^{-1}, xy) = (a\alpha_x(b)\kappa(x, y)\varphi(xy)^{-1}, xy) \\ &= \gamma(a\alpha_x(b)\kappa(x, y), xy) = \gamma((a, x) \cdot (b, y)), \end{aligned}$$

d. h. γ ist ein Homomorphismus. Außerdem gilt

$$\begin{aligned} (\gamma\nu_1)(a) &= \gamma(a, 1) = (a\varphi(1)^{-1}, 1) = (a, 1) = \nu_2(a), \\ (\pi_2\gamma)(a, x) &= \pi_2(a\varphi(x)^{-1}, x) = x = \pi_1(a, x). \end{aligned}$$

Also sind G_1 und G_2 äquivalent. \square

Satz 4.14 (SCHREIER). *Es gibt eine Bijektion zwischen der Menge der Äquivalenzklassen von Erweiterungen von H mit N und der Menge der Äquivalenzklassen von (normalisierten) Parametersystemen von H mit N .*

Beweis. Nach Lemma 4.12 und Lemma 4.13 gibt es wohldefinierte Abbildungen zwischen den Mengen von Äquivalenzklassen. Wir zeigen, dass sie zueinander invers sind.

Die Erweiterung $N \xrightarrow{\nu_1} G_1 \xrightarrow{\pi_1} H$ definiere das normalisierte Parametersystem (α, κ) mit den Elementen $\tilde{x} \in G_1$ wie in Lemma 4.5. Aus (α, κ) konstruieren wir die Erweiterung $N \xrightarrow{\nu_2} G_2 \xrightarrow{\pi_2} H$ wie in Lemma 4.7. Jedes Element in G_1 lässt sich eindeutig in der Form $\nu_1(a)\tilde{x}$ mit $a \in N$ und $x \in H$ schreiben. Wir definieren $\gamma: G_1 \rightarrow G_2$, $\nu_1(a)\tilde{x} \mapsto (a, x)$. Für $\nu_1(a)\tilde{x}, \nu_1(b)\tilde{y} \in G_1$ gilt

$$\begin{aligned} \gamma(\nu_1(a)\tilde{x} \cdot \nu_1(b)\tilde{y}) &= \gamma(\nu_1(a)\tilde{x}\nu_1(b)\tilde{x}^{-1} \cdot \tilde{x}\tilde{y}) = \gamma(\nu_1(a)\nu_1(\alpha_x(b)) \cdot \nu_1(\kappa(x, y))\tilde{xy}) \\ &= (a\alpha_x(b)\kappa(x, y), xy) = (a, x) * (b, y) = \gamma(\nu_1(a)\tilde{x}) * \gamma(\nu_1(b)\tilde{y}), \end{aligned}$$

d. h. γ ist ein Homomorphismus mit

$$\begin{aligned}(\gamma\nu_1)(a) &= \gamma(\nu_1(a)\tilde{1}) = (a, 1) = \nu_2(a), \\(\pi_2\gamma)(\nu_1(a)\tilde{x}) &= \pi_2(a, x) = x = \pi_1(\tilde{x}) = \pi_1(\nu_1(a)\tilde{x}).\end{aligned}$$

Also sind G_1 und G_2 äquivalent.

Umgekehrt sei zuerst (α, κ) normalisiert gegeben. Wir konstruieren die Erweiterung G und daraus das Parametersystem (α', κ') mittels der Elemente $\tilde{x} = (1, x) \in G$ für $x \in H$. Zunächst gilt

$$\kappa(x, x^{-1}) = \kappa(x, x^{-1})\kappa(xx^{-1}, x) = \alpha_x(\kappa(x^{-1}, x))\kappa(x, x^{-1}x) = \alpha_x(\kappa(x^{-1}, x)) \quad (4.1)$$

für $x \in H$. Daraus folgt

$$\begin{aligned}\alpha'_x(g) &= \nu^{-1}(\tilde{x}\nu(g)\tilde{x}^{-1}) = \nu^{-1}((1, x)(g, 1)(1, x)^{-1}) = \nu^{-1}((\alpha_x(g), x)(\kappa(x^{-1}, x)^{-1}, x^{-1})) \\&= \nu^{-1}(\alpha_x(g)\alpha_x(\kappa(x^{-1}, x)^{-1})\kappa(x, x^{-1}), 1) = \alpha_x(g), \\ \kappa'(x, y) &= \nu^{-1}(\tilde{x}\tilde{y}\tilde{x}\tilde{y}^{-1}) = \nu^{-1}((1, x)(1, y)(\kappa((xy)^{-1}, xy)^{-1}, (xy)^{-1})) \\&= \nu^{-1}((\kappa(x, y), xy)(\kappa((xy)^{-1}, xy)^{-1}, (xy)^{-1})) \\&= \nu^{-1}(\kappa(x, y)\alpha_{xy}(\kappa((xy)^{-1}, xy)^{-1})\kappa(xy, (xy)^{-1}), 1) \\&= \nu^{-1}(\kappa(x, y), 1) = \kappa(x, y)\end{aligned}$$

für $x, y \in H$ und $g \in N$. Dies zeigt $(\alpha, \kappa) = (\alpha', \kappa')$. □

Bemerkung 4.15. Nach Bemerkung 4.3 entsprechen die zerfallenden Erweiterungen bis auf Äquivalenz genau den Parametersystemen mit trivialem Faktorensystem.

Satz 4.16. Sei $H = \langle x \rangle \cong C_n$ und $\beta \in \text{Aut}(N)$. Genau dann existiert ein Parametersystem (α, κ) mit $\alpha_x = \beta$, wenn ein $a \in N$ mit $\beta(a) = a$ und $\beta^n = c_a$ existiert.

Beweis. Sei (α, κ) ein Parametersystem mit $\alpha_x = \beta$. Im Fall $n = 1$ gilt die Behauptung mit $a := \kappa(1, 1)$, denn

$$\begin{aligned}\alpha_1\alpha_1 &= c_{\kappa(1,1)}\alpha_1, \\ \kappa(1, 1)\kappa(1, 1) &= \alpha_1(\kappa(1, 1))\kappa(1, 1).\end{aligned}$$

Für $n \geq 2$ dürfen wir zu einem normalisierten Parametersystem übergeben, ohne dass sich α_x ändert (siehe Beweis von Lemma 4.11). Wir konstruieren die entsprechende Erweiterung $G = N \times H$. Für $\tilde{x} := (1, x) \in G$ und $b \in N$ gilt

$$\tilde{x}\nu(b)\tilde{x}^{-1} = (1, x)(b, 1)(1, x)^{-1} = (\alpha_x(b), x)(\kappa(x^{-1}, x)^{-1}, x^{-1}) \stackrel{(4.1)}{=} (\alpha_x(b), 1) = \nu(\beta(b)).$$

Also ist $\beta = \nu^{-1}c_{\tilde{x}}\nu$. Sei $(a, 1) := \tilde{x}^n$. Dann gilt $\beta^n = \nu^{-1}c_{(a,1)}\nu = c_a$ und

$$\beta(a) = \nu^{-1}(\tilde{x}\nu(a)\tilde{x}^{-1}) = \nu^{-1}(\tilde{x}\tilde{x}^n\tilde{x}^{-1}) = \nu^{-1}(a, 1) = a.$$

Sei umgekehrt $\beta^n = c_a$ und $\beta(a) = a$ für ein $a \in N$. Wir definieren $\alpha_{x^i} := \beta^i$ und

$$\kappa(x^i, x^j) := \begin{cases} 1 & \text{falls } i + j < n, \\ a & \text{falls } i + j \geq n \end{cases}$$

für $0 \leq i, j \leq n-1$. Dann gilt

$$\alpha_{x^i} \alpha_{x^j} = \beta^{i+j} = \begin{cases} \alpha_{x^{i+j}} = c_{\kappa(x^i, x^j)} \alpha_{x^i x^j} & \text{falls } i+j < n, \\ c_a \beta^{i+j-n} = c_{\kappa(x^i, x^j)} \alpha_{x^i x^j} & \text{falls } i+j \geq n \end{cases}$$

und

$$\kappa(x^i, x^j) \kappa(x^{i+j}, x^k) = \begin{cases} 1 & \text{falls } i+j+k < n, \\ a & \text{falls } n \leq i+j+k < 2n, \\ a^2 & \text{falls } i+j+k \geq 2n. \end{cases}$$

Wegen $\alpha_{x^i}(a) = \beta^i(a) = a$ gilt $\kappa(x^i, x^j) \kappa(x^{i+j}, x^k) = \alpha_{x^i}(\kappa(x^j, x^k)) \kappa(x^i, x^{j+k})$ in allen Fällen. Somit ist (α, κ) ein Parametersystem. \square

Beispiel 4.17.

- (i) Ist β in der Situation von Satz 4.16 ein innerer Automorphismus, sagen wir $\beta = c_b$ mit $b \in N$, so gelten die Voraussetzungen mit $a = b^n$. Es gibt also immer eine Erweiterung, sodass β von x induziert wird.
- (ii) Ist N abelsch, so reduzieren sich die Bedingungen zu $\beta^n = 1$. Für nicht-abelsche Gruppen ist das nicht ausreichend (Aufgabe 17).

Bemerkung 4.18. Sei N abelsch. Dann sind die Automorphismensysteme genau die Homomorphismen $\alpha: H \rightarrow \text{Aut}(N)$. Die entsprechenden Faktorensysteme bilden eine Untergruppe $F_\alpha \leq C^2(H, N) := C^1(H \times H, N)$ (bei festem α). Aus $(\alpha, \kappa) \sim (\alpha', \kappa')$ folgt außerdem $\alpha = \alpha'$. Man kann also die Äquivalenzklassen innerhalb F_α untersuchen.

Satz 4.19. Sei N abelsch und $\alpha: H \rightarrow \text{Aut}(N)$ ein Homomorphismus. Dann ist

$$P_\alpha := \{\kappa \in F_\alpha : (\alpha, \kappa) \sim (\alpha, 1)\} \leq F_\alpha.$$

Die Äquivalenzklassen von Parametersystemen mit Automorphismensystem α entsprechen den Elementen von $\overline{F_\alpha} := F_\alpha / P_\alpha$.

Beweis. Für $\kappa, \kappa' \in P_\alpha$ existieren $\varphi, \psi \in C^1(H, N)$ mit $\kappa(x, y) = \varphi(x) \alpha_x(\varphi(y)) \varphi(xy)^{-1}$ und $\kappa'(x, y) = \psi(x) \alpha_x(\psi(y)) \psi(xy)^{-1}$ für $x, y \in H$. Da N abelsch ist, folgt

$$(\kappa \kappa')(x, y) = (\varphi \psi)(x) \alpha_x((\varphi \psi)(y)) (\varphi \psi)(xy)^{-1}$$

und $\kappa \kappa' \in P_\alpha$. Man erhält leicht $P_\alpha \leq F_\alpha$. Da $C^2(H, N) \cong \prod_{x \in H \times H} N$ abelsch ist, gilt $P_\alpha \leq F_\alpha$ und $\overline{F_\alpha}$ ist wohldefiniert. Außerdem ist

$$\begin{aligned} (\alpha, \kappa) \sim (\alpha, \kappa') &\iff \exists \varphi \in C^1(H, N) \forall x, y \in H : \kappa'(x, y) = \varphi(x) \alpha_x(\varphi(y)) \kappa(x, y) \varphi(xy)^{-1} \\ &\iff \exists \varphi \in C^1(H, N) : \kappa^{-1} \kappa' \in P_\alpha \iff \kappa P_\alpha = \kappa' P_\alpha. \end{aligned}$$

Bemerkung 4.20. Erweiterungen lassen sich auf dem Computer besonders effizient für *polyzyklische* Gruppen H berechnen. Dies bedeutet, dass H eine Subnormalreihe mit zyklischen Faktoren besitzt. Für endliche Gruppen ist polyzyklisch äquivalent zu auflösbar. Wir nehmen außerdem an, dass N eine elementarabelsche p -Gruppe ist. Durch den Homomorphismus $\alpha: H \rightarrow \text{Aut}(N)$ wird N dann zu einem $\mathbb{F}_p H$ -Modul.

```

H:=SymmetricGroup(4);; #Permutationsgruppe
H:=Image(IsomorphismPcGroup(H));; #isomorphe polyzyklische Gruppe
IrrM:=IrreducibleModules(H,GF(2),2); #einfache  $\mathbb{F}_2H$ -Moduln der Dimension  $\leq 2$ 
N:=IrrM[2][2];; #ein 2-dimensionaler einfacher  $\mathbb{F}_2H$ -Modul, also  $N \cong C_2^2$ 
ext:=Extensions(H,N); #zwei Erweiterungen der Ordnung 96
List(ext,IdGroup); #Nummer in der small groups library
IdGroup(SplitExtension(H,N)); #zerfallende Erweiterung
Fa:=VectorSpace(GF(2),TwoCocycles(H,N));; #= $F_\alpha$ 
Pa:=Subspace(Fa,TwoCoboundaries(H,N));; #= $P_\alpha$ 
t:=Difference(Fa,Pa)[1];; #nicht-triviales Faktorensystem
G:=Extension(H,N,t);; #das sollte die nicht-zerfallende Erweiterung sein
IdGroup(G);
TwoCohomology(H,N); #mehr Info über  $\overline{F_\alpha}$ 

```

Für nicht-polyzyklische Gruppen kann man das cohomolo-Paket (bisher nur unter Linux) einbinden. Es erwartet als Eingabe eine Permutationsgruppe und eine dazu isomorphe endlich präsentierte Gruppe.

```

LoadPackage("cohomolo",false); #false unterdrückt Banner
H:=GL(5,2);;
gen:=GeneratorsOfGroup(H);;
Hp:=Image(IsomorphismPermGroup(H));;
Hf:=Image(IsomorphismFpGroupByGenerators(H,gen));;
chr:=CHR(Hp,2,Hf,gen); #hier ist  $N = \mathbb{F}_2^5$  und  $\alpha: H \rightarrow \text{Aut}(N)$  der natürliche Isomorphismus
SecondCohomologyDimension(chr); #=1 bedeutet  $\overline{F_\alpha} \cong \mathbb{F}_2$ , d.h. es gibt zwei Erweiterungen
G:=NonsplitExtension(chr); #das ist die DEMPWOLFF-Gruppe
Size(G); #dauert ewig

```

Satz 4.21. Sei N abelsch, $K \leq H$ endlich und $\alpha: H \rightarrow \text{Aut}(N)$ ein Homomorphismus. Sei $\alpha_K: K \rightarrow \text{Aut}(N)$ die Einschränkung von α . Dann ist die Abbildung

$$\overline{F_\alpha} \rightarrow \overline{F_{\alpha_K}}, \quad \kappa P_\alpha \mapsto \kappa_{K \times K} P_{\alpha_K}$$

ein Homomorphismus. Aus $\kappa_{K \times K} \in P_{\alpha_K}$ folgt $\kappa^{|H:K|} \in P_\alpha$. Insbesondere ist $\exp(\overline{F_\alpha})$ ein Teiler von $|H|$.

Beweis. Für $\kappa \in F_\alpha$ ist offensichtlich $\kappa_{K \times K} \in F_{\alpha_K}$ und die Abbildung $F_\alpha \rightarrow F_{\alpha_K}$, $\kappa \mapsto \kappa_{K \times K}$ ist ein Homomorphismus. Aus $\kappa \equiv \kappa' \pmod{P_\alpha}$ folgt $\kappa_{K \times K} \equiv \kappa'_{K \times K} \pmod{F_{\alpha_K}}$. Also ist $\overline{F_\alpha} \rightarrow \overline{F_{\alpha_K}}$ ein wohldefinierter Homomorphismus.

Sei nun $\kappa_{K \times K} \in P_{\alpha_K}$. Sei G eine Erweiterung von H mit N bzgl. (α, κ) . Dann existiert ein Homomorphismus $\rho: K \rightarrow G$ mit $\pi\rho = \text{id}_K$. Sei R ein Repräsentantensystem für H/K mit $1 \in R$. Für $r \in R$ sei $\tilde{r} \in G$ mit $\pi(\tilde{r}) = r$ und $\tilde{1} = 1$. Für $x \in H$ sei $r_x \in R$ mit $r_x^{-1}x \in K$. Wir definieren $\tilde{x} := \tilde{r}_x \rho(r_x^{-1}x)$. Dann gilt $\pi(\tilde{x}) = r_x r_x^{-1}x = x$ und

$$\kappa'(x, y) := \nu^{-1}(\tilde{x} \tilde{y} \tilde{x} y^{-1})$$

definiert ein zu (α, κ) äquivalentes normalisiertes Parametersystem. Für $x, y \in H$ gilt $r_{xy}K = xyK = x r_y K = r_{x r_y} K$ und $r_{xy} = r_{x r_y}$. Es folgt

$$\begin{aligned} \kappa'(x, y) &= \nu^{-1}(\tilde{x} \tilde{r}_y \rho(r_y^{-1}y) \tilde{x} y^{-1}) = \nu^{-1}(\tilde{x} \tilde{r}_y \tilde{x} \tilde{r}_y^{-1} \tilde{x} r_y \rho(r_y^{-1}y) \tilde{x} y^{-1}) \\ &= \kappa'(x, r_y) \nu^{-1}(\tilde{x} \tilde{r}_y \rho(r_y^{-1}y) \tilde{x} y^{-1}) = \kappa'(x, r_y) \nu^{-1}(\tilde{r}_{xy} \rho(r_{xy}^{-1}x r_y) \rho(r_y^{-1}y) \tilde{x} y^{-1}) = \kappa'(x, r_y). \end{aligned}$$

Für $r \in R$ folgt

$$\kappa'(x, y) = \alpha_x(\kappa'(y, r)) \kappa'(x, yr) \kappa'(xy, r)^{-1} = \alpha_x(\kappa'(y, r)) \kappa'(x, r_{yr}) \kappa'(xy, r)^{-1}.$$

Mit r läuft auch r_{yr} durch alle Elemente in R . Sei $\varphi(x) := \prod_{r \in R} \kappa'(x, r)$ für $x \in H$. Dann gilt

$$\kappa'(x, y)^{|H:K|} = \prod_{r \in R} \alpha_x(\kappa'(y, r)) \kappa'(x, r_{yr}) \kappa'(xy, r)^{-1} = \alpha_x(\varphi(y)) \varphi(x) \varphi(xy)^{-1}.$$

Dies zeigt $(\kappa')^{|H:K|} \in P_\alpha$. Wegen $(\alpha, \kappa) \sim (\alpha, \kappa')$ ist auch $\kappa^{|H:K|} \in P_\alpha$ nach Satz 4.19.

Die zweite Aussage folgt, indem man $K = 1$ wählt. □

Bemerkung 4.22. Die folgenden beiden Sätze wurden nachträglich im Gruppentheorie-Skript mit alternativen Beweisen hinzugefügt.

Satz 4.23 (GASCHÜTZ). *Sei G eine endliche Gruppe mit abelschem Normalteiler N . Sei $N \leq H \leq G$ mit $\text{ggT}(|N|, |G : H|) = 1$, sodass N ein Komplement in H besitzt. Dann besitzt N ein Komplement in G .*

Beweis. Bekanntlich ist G eine Erweiterung von G/N mit N . Sei (α, κ) das entsprechende Parametersystem. Nach Voraussetzung zerfällt die Erweiterung von $K := H/N$ mit N . Daher ist $\kappa_{K \times K} \in P_{\alpha_K}$. Aus Satz 4.21 folgt $\kappa^{|G:H|} \in P_\alpha$. Wegen $F_\alpha \leq C^2(G/N, N)$ ist auch $\kappa^{|N|} \in P_\alpha$. Aus $\text{ggT}(|G : H|, |N|) = 1$ ergibt sich $\kappa \in P_\alpha$, d. h. G zerfällt. □

Satz 4.24 (GASCHÜTZ). *Sei G eine endliche Gruppe mit abelschem Normalteiler N . Genau dann besitzt N ein Komplement in G , wenn N ein Komplement in P besitzt für jede Sylowgruppe P/N von G/N .*

Beweis. Ist K ein Komplement von N in G , so ist $K \cap P$ ein Komplement von N in P für $N \leq P \leq G$, denn $N(K \cap P) = NK \cap P = P$ und $N \cap (K \cap P) \leq N \cap K = 1$.

Nehmen wir nun umgekehrt an, dass N ein Komplement in P besitzt für alle Sylowgruppen P/N von G/N . Sei (α, κ) das Parametersystem der Erweiterung G . Nach Satz 4.21 gilt $\kappa^{|G:P|} \in P_\alpha$. Dies zeigt $\kappa^{|G/N|_{p'}} \in P_\alpha$ für alle Primteiler p von $|G/N|$. Da die Zahlen $|G/N|_{p'}$ teilerfremd sind (wobei p über alle Primteiler von $|G|$ läuft), folgt $\kappa \in P_\alpha$, d. h. G zerfällt. □

Definition 4.25. Sei nun N beliebig und (α, κ) ein Parametersystem.

- Die Abbildung $\omega: H \rightarrow \text{Out}(N)$, $x \mapsto \alpha_x \text{Inn}(N)$ ist ein Homomorphismus, den man die *Paarung* von (α, κ) nennt. Sei $\text{Par}(\omega)$ die Menge der Parametersysteme mit Paarung ω . Äquivalente Parametersysteme definieren die gleiche Paarung. Sei $\text{Par}(\omega)$ die entsprechende Menge der Äquivalenzklassen.
- Sei $Z := Z(N)$. Jeder Homomorphismus $\omega: H \rightarrow \text{Out}(N)$, $x \mapsto \omega_x \text{Inn}(N)$ definiert einen wohldefinierten Homomorphismus $\omega_Z: H \rightarrow \text{Aut}(Z)$, $x \mapsto (\omega_x)|_Z$.

Bemerkung 4.26. Nicht zu jedem Homomorphismus $\omega: H \rightarrow \text{Out}(N)$ muss ein entsprechendes Parametersystem existieren (Aufgabe 17).

Satz 4.27. *Sei $\omega: H \rightarrow \text{Out}(N)$ ein Homomorphismus mit $\text{Par}(\omega) \neq \emptyset$. Sei $Z := Z(N)$ und $\beta := \omega_Z$. Dann operiert $\overline{F_\beta}$ regulär auf $\text{Par}(\omega)$. Insbesondere sind $\text{Par}(\omega)$ und $\overline{F_\beta}$ gleichmächtig.*

Beweis. Sei $\lambda \in F_\beta$ und $(\alpha, \kappa) \in \text{Par}(\omega)$. Wegen $\lambda(H \times H) \leq Z$ gilt

$$\begin{aligned}\alpha_x \alpha_y &= c_{\kappa(x,y)} \alpha_{xy} = c_{(\lambda\kappa)(x,y)} \alpha_{xy}, \\ (\lambda\kappa)(x, y)(\lambda\kappa)(xy, z) &= \alpha_x(\kappa(y, z))\beta_x(\lambda(y, z))(\lambda\kappa)(x, yz) = \alpha_x((\lambda\kappa)(y, z))(\lambda\kappa)(x, yz)\end{aligned}$$

für $x, y, z \in H$. Daher ist $(\alpha, \lambda\kappa) \in \text{Par}(\omega)$. Man sieht leicht, dass ${}^\lambda(\alpha, \kappa) := (\alpha, \lambda\kappa)$ eine Operation von F_β auf $\text{Par}(\omega)$ definiert. Sei $(\alpha', \kappa') \sim (\alpha, \kappa)$. Dann existiert $\varphi \in C^1(H, N)$ mit

$$\begin{aligned}\alpha'_x &= c_{\varphi(x)} \alpha_x, \\ (\lambda\kappa')(x, y) &= \varphi(x) \alpha_x(\varphi(y)) (\lambda\kappa)(x, y) \varphi(xy)^{-1}.\end{aligned}$$

Also ist ${}^\lambda(\alpha, \kappa) \sim {}^\lambda(\alpha', \kappa')$ und F_β operiert auf $\overline{\text{Par}(\omega)}$. Sei $\lambda \in P_\beta$, also $\lambda(x, y) = \delta(x) \beta_x(\delta(y)) \delta(xy)^{-1}$ für ein $\delta \in C^1(H, Z)$. Dann ist

$$(\lambda\kappa)(x, y) = \delta(x) \alpha_x(\delta(y)) \kappa(x, y) \delta(xy)^{-1},$$

d. h. ${}^\lambda(\alpha, \kappa) \sim (\alpha, \kappa)$. Somit operiert P_β trivial auf $\overline{\text{Par}(\omega)}$ und man erhält eine wohldefinierte Operation von $\overline{F_\beta}$ auf $\overline{\text{Par}(\omega)}$. Sei $\lambda \in F_\beta$ mit ${}^\lambda(\alpha, \kappa) \sim (\alpha, \kappa)$. Dann existiert $\varphi \in C^1(H, N)$ mit

$$\begin{aligned}\alpha_x &= c_{\varphi(x)} \alpha_x, \\ (\lambda\kappa)(x, y) &= \varphi(x) \alpha_x(\varphi(y)) \kappa(x, y) \varphi(xy)^{-1}\end{aligned}$$

für $x, y \in H$. Es folgt $\varphi(H) \leq Z$ und $\lambda(x, y) = \varphi(x) \beta_x(\varphi(y)) \varphi(xy)^{-1}$. Dies zeigt $\lambda \in P_\beta$. Daher operiert $\overline{F_\beta}$ fixpunktfrei auf $\overline{\text{Par}(\omega)}$. Für die Transitivität seien $(\alpha, \kappa), (\alpha', \kappa') \in \text{Par}(\omega)$. Wegen $\alpha_x \text{Inn}(N) = \omega(x) = \alpha'_x \text{Inn}(N)$ für $x \in H$ existiert $\varphi \in C^1(H, N)$ mit $\alpha_x = c_{\varphi(x)} \alpha'_x$ für $x \in H$. Wir können also (α', κ') durch ein äquivalentes Parametersystem der Form (α, κ') ersetzen. Nun gilt

$$c_{\kappa(x,y)} \alpha_{xy} = \alpha_x \alpha_y = c_{\kappa'(x,y)} \alpha_{xy}$$

und $\lambda := \kappa^{-1} \kappa' : H \times H \rightarrow Z$. Wegen

$$\begin{aligned}\lambda(x, y) \lambda(xy, z) &= \kappa(xy, z)^{-1} \lambda(x, y) \kappa'(xy, z) = \kappa(xy, z)^{-1} \kappa(x, y)^{-1} \kappa'(x, y) \kappa'(xy, z) \\ &= (\alpha_x(\kappa(y, z)) \kappa(x, yz))^{-1} \alpha_x(\kappa'(y, z)) \kappa'(x, yz) \\ &= \kappa(x, yz)^{-1} \alpha_x(\kappa(y, z)^{-1} \kappa'(y, z)) \kappa'(x, yz) = \kappa(x, yz)^{-1} \beta_x(\lambda(y, z)) \kappa'(x, yz) \\ &= \beta_x(\lambda(y, z)) \kappa(x, yz)^{-1} \kappa'(x, yz) = \beta_x(\lambda(y, z)) \lambda(x, yz)\end{aligned}$$

für $x, y \in H$ gilt $\lambda \in F_\beta$ und ${}^\lambda(\alpha, \kappa) = (\alpha, \kappa\lambda) = (\alpha, \kappa')$. Also operiert $\overline{F_\beta}$ regulär auf $\overline{\text{Par}(\omega)}$. \square

Folgerung 4.28. Sei $Z(N) = 1$. Dann gilt:

- (i) Für jeden Homomorphismus $\omega : H \rightarrow \text{Out}(N)$ gilt $|\overline{\text{Par}(\omega)}| = 1$.
- (ii) Besitzt $\text{Inn}(N) \cong N$ ein Komplement in $\text{Aut}(N)$, so zerfällt jede Erweiterung mit N .

Beweis.

- (i) Sei $\omega(x) = \alpha_x \text{Inn}(N)$ für $x \in H$. Wegen $\alpha_{xy} \text{Inn}(N) = \omega(xy) = \omega(x) \omega(y) = \alpha_x \alpha_y \text{Inn}(N)$ existieren $\kappa(x, y) \in N$ mit $\alpha_x \alpha_y = c_{\kappa(x,y)} \alpha_{xy}$ für alle $x, y \in H$. Dabei gilt

$$\begin{aligned}c_{\kappa(x,y)} \kappa(xy, z) \alpha_{xyz} &= c_{\kappa(x,y)} \alpha_{xy} \alpha_z = \alpha_x \alpha_y \alpha_z = \alpha_x c_{\kappa(y,z)} \alpha_{yz} \\ &= c_{\alpha_x(\kappa(y,z))} \alpha_x \alpha_{yz} = c_{\alpha_x(\kappa(y,z)) \kappa(x,yz)} \alpha_{xyz}.\end{aligned}$$

Aus $\text{Inn}(N) \cong N/Z(N) \cong N$ folgt $\kappa(x, y) \kappa(xy, z) = \alpha_x(\kappa(y, z)) \kappa(x, yz)$. Dies zeigt $(\alpha, \kappa) \in \text{Par}(\omega) \neq \emptyset$ und $|\overline{\text{Par}(\omega)}| = 1$ nach Satz 4.27.

- (ii) Nach Voraussetzung existiert ein Homomorphismus $\tau: \text{Out}(N) \rightarrow \text{Aut}(N)$ mit $\tau(\gamma)\text{Inn}(N) = \gamma$ für alle $\gamma \in \text{Out}(N)$. Jeder Homomorphismus $\omega: H \rightarrow \text{Out}(N)$ lässt sich also zu einem Homomorphismus $\alpha := \tau\omega: H \rightarrow \text{Aut}(N)$ liften (d. h. $\omega(x) = \alpha_x \text{Inn}(N)$ für alle $x \in H$). Nach (i) ist die zerfallende Erweiterung bzgl. $(\alpha, 1)$ die einzige Erweiterung mit Paarung ω . \square

Beispiel 4.29. Ist N vollständig, d. h. $Z(N) = 1 = \text{Out}(N)$, so gibt es nur die Erweiterungen $N \times H$. Dies wurde bereits in GT-Aufgabe 24 gezeigt.

Bemerkung 4.30. Die Anzahl der Erweiterungen mit einer nicht-abelschen Gruppe N zu einer Paarung $\omega: K \rightarrow \text{Out}(N)$ lässt sich mit dem `hap`-Paket bestimmen:

```
LoadPackage("hap",false); #lädt weitere Pakete
N:=QuaternionGroup(8);;
H:=AutomorphismGroup(N);;
NH:=SemidirectProduct(H,N);;
omega:=GOuterGroup(NH,Image(Embedding(NH,2))); #definiert Paarung H -> Out(N)
beta:=Center(omega); #zugehöriges Faktorensystem H -> Aut(Z(N))
A:=ActingGroup(beta);; #Urbild von beta
R:=ResolutionFiniteGroup(A,3);; #drei Glieder einer Auflösung
C:=HomToGModule(R,alpha);; #zugehöriger Kettenkomplex
Cohomology(C,2); #Ordnungen der zyklischen Faktoren von F_beta
```

Satz 4.31 (JOHNSON-ZASSENHAUS). Zwei Erweiterungen $N \xrightarrow{\nu_i} G_i \xrightarrow{\pi_i} H$ ($i = 1, 2$) sind genau dann äquivalent, wenn für jede Sylowgruppe P von H die Erweiterungen $\pi_1^{-1}(P)$ und $\pi_2^{-1}(P)$ von P mit N äquivalent sind.

Beweis. Seien G_1 und G_2 äquivalent mittels $\gamma: G_1 \rightarrow G_2$. Für eine Primzahl p und $P \in \text{Syl}_p(H)$ sei $P_i := \pi_i^{-1}(P) \leq G_i$ und $\delta := \gamma_{P_1}$. Dann gilt

$$\delta(P_1) = \gamma(\pi_1^{-1}(P)) = \gamma(\gamma^{-1}(\pi_2^{-1}(P))) = P_2,$$

$\delta\nu_1 = \nu_2$ und $(\pi_2)_{|P_2}\delta = (\pi_1)_{|P_1}$. Also sind P_1 und P_2 äquivalent.

Nehmen wir nun an, dass P_1 und P_2 für alle Sylowgruppen P von H äquivalent sind. Seien (α, κ) und (α', κ') die Parametersysteme von G_1 bzw. G_2 . Dann sind $(\alpha_P, \kappa_{P \times P})$ und $(\alpha'_P, \kappa'_{P \times P})$ äquivalent und es folgt $\alpha_x \text{Inn}(N) = \alpha'_x \text{Inn}(N)$ für alle $x \in P$. Da H von seinen Sylowgruppen erzeugt wird, besitzen (α, κ) und (α', κ') die gleiche Paarung ω . Sei $Z := Z(N)$ und $\beta := \omega_Z$. Nach Satz 4.27 existiert $\lambda \in F_\beta$ mit $(\alpha', \kappa') \sim (\alpha, \lambda\kappa)$. Nach Voraussetzung gilt $\lambda_P \in P_{\beta_P}$ für jede Sylowgruppe P von H , d. h. die Erweiterung von P mit Z zerfällt. Mit Satz 4.24 zerfällt nun auch die Erweiterung von H mit Z , d. h. $\lambda \in P_\beta$. Dies zeigt $(\alpha', \kappa') \sim (\alpha, \lambda\kappa) \sim (\alpha, \kappa)$. \square

Bemerkung 4.32. Satz 4.31 eignete sich nicht, um den Satz 4.24 von Gaschütz für nicht-abelsches N zu beweisen, denn nicht zu jedem Homomorphismus $\omega: H \rightarrow \text{Out}(N)$ existiert eine zerfallende Erweiterung, mit der man vergleichen könnte (Aufgabe 17). Selbst wenn eine solche zerfallende Erweiterung von H mit N existiert, so muss die eingeschränkte Erweiterung von H mit $Z(N)$ nicht unbedingt zerfallen. Zum Beispiel ist $G = D_8 * C_4$ eine zerfallende Erweiterung von $H = C_2$ mit $N = D_8$, aber die eingeschränkte Erweiterung $C_G(N) = C_4$ von H mit $Z(N) \cong C_2$ zerfällt nicht. Ein ähnliches Beispiel zeigt, dass Satz 4.24 für nicht-abelsche Gruppen N im Allgemeinen falsch ist (Aufgabe 15).

5 Zentrale Erweiterungen

Definition 5.1. Ist N abelsch und $\alpha: H \rightarrow \text{Aut}(N)$ trivial, so ist

$$\begin{aligned} Z^2(H, N) &:= F_\alpha = \{\kappa \in C^2(H, N) : \kappa(x, y)\kappa(xy, z) = \kappa(y, z)\kappa(x, yz)\}, \\ B^2(H, N) &:= P_\alpha = \{\kappa \in Z^2(H, N) : \exists \varphi \in C^1(H, N) : \kappa(x, y) = \varphi(x)\varphi(y)\varphi(xy)^{-1}\}, \\ H^2(H, N) &:= \overline{F_\alpha} = F_\alpha/P_\alpha. \end{aligned}$$

Die Elemente von $Z^2(H, N)$ nennt man (2-)Kozyklen. Für $\varphi \in C^1(H, N)$ sei $\partial\varphi \in B^2(H, N)$ mit $\partial\varphi(x, y) := \varphi(x)\varphi(y)\varphi(xy)^{-1}$ für $x, y \in H$. Man nennt $H^2(H, N)$ die zweite Kohomologiegruppe von H mit Werten in N . Ist G eine entsprechende Erweiterung, so gilt $\nu(N) \leq Z(G)$ (vgl. Bemerkung 4.8). Man spricht daher von *zentralen* Erweiterungen.

Bemerkung 5.2.

- (i) Im Folgenden sei A stets eine abelsche Gruppe.
- (ii) Sei H abelsch und G die zentrale Erweiterung auf $A \times H$ mittels $\kappa \in Z^2(H, A)$, d. h.

$$(a, x)(b, y) = (ab\kappa(x, y), xy)$$

für alle $(a, x), (b, y) \in G$. Genau dann ist G abelsch, wenn κ symmetrisch ist, d. h. $\kappa(x, y) = \kappa(y, x)$ für alle $x, y \in H$. Da H abelsch ist, sind die Kozyklen in $B^2(H, A)$ symmetrisch.

Definition 5.3. Für abelsche Gruppen H sei

$$Z_s^2(H, A) := \{\kappa \in Z^2(H, A) : \forall x, y \in H : \kappa(x, y) = \kappa(y, x)\}$$

und $H_s^2(H, A) := Z_s^2(H, A)/B^2(H, A)$.

Satz 5.4. Für $n \in \mathbb{N}$ gilt $H^2(C_n, A) = H_s^2(C_n, A) \cong A/\langle a^n : a \in A \rangle$.

Beweis. Sei G eine zentrale Erweiterung von $H = \langle x \rangle \cong C_n$ mit A . Wegen $A \leq Z(G)$ ist $G/Z(G)$ zyklisch und G abelsch. Dies zeigt $H^2(H, A) = H_s^2(H, A)$. Für $a \in A$ haben wir im Beweis von Satz 4.16 einen Kozyklus $\kappa_a \in Z^2(H, A)$ mit

$$\kappa_a(x^i, x^j) = \begin{cases} 1 & \text{falls } i + j < n, \\ a & \text{falls } i + j \geq n \end{cases}$$

konstruiert. Die Abbildung $F: A \rightarrow H^2(H, A)$, $a \mapsto \kappa_a$ ist offenbar ein Homomorphismus. Sei $\varphi: H \rightarrow A$, $x^i \mapsto a^i$ für $i = 0, \dots, n-1$. Dann gilt

$$\partial\varphi(x^i, x^j) = \begin{cases} 1 & \text{falls } i + j < n, \\ a^n & \text{falls } i + j \geq n. \end{cases}$$

Dies zeigt $a^n \in \text{Ker}(F)$. Für $a \in \text{Ker}(F)$ existiert ein $\varphi \in C^1(H, A)$ mit $\kappa_a = \partial\varphi$. Es gilt

$$\begin{aligned} \varphi(1) &= \partial\varphi(1, 1) = \kappa_a(1, 1) = 1, \\ \varphi(x)^2 &= \kappa_a(x, x)\varphi(x^2) = \varphi(x^2), \\ \varphi(x)^3 &= \kappa_a(x^2, x)\varphi(x^3) = \varphi(x^3), \\ &\vdots \\ \varphi(x)^n &= \kappa_a(x^{n-1}, x)\varphi(1) = a. \end{aligned}$$

Daher ist $a \in \langle b^n : b \in A \rangle$ und $\text{Ker}(F) = \langle a^n : a \in A \rangle$.

Für die Surjektivität von F sei $A \rightarrow G \xrightarrow{\pi} H$ eine Erweiterung von H mit A . Sei $\tilde{x} \in G$ mit $\pi(\tilde{x}) = x$. Für $i = 0, \dots, n-1$ können wir $\tilde{x}^i := \tilde{x}^i$ als Urbild von x^i wählen. Für den Kozyklus κ gilt dann

$$\kappa(x^i, x^j) = \begin{cases} \tilde{x}^i \tilde{x}^j \widetilde{x^{i+j}}^{-1} = 1 & \text{falls } i+j < n, \\ \tilde{x}^i \tilde{x}^j \widetilde{x^{i+j-n}}^{-1} = \tilde{x}^n & \text{falls } i+j \geq n. \end{cases}$$

Mit $a := \tilde{x}^n \in A$ gilt also $\kappa = \kappa_a$. Daher ist F surjektiv. \square

Satz 5.5. Für alle abelschen Gruppen G und H gilt $H_s^2(G \times H, A) \cong H_s^2(G, A) \times H_s^2(H, A)$.

Beweis. Wir orientieren uns am Beweis der Künneth-Formel aus der Gruppentheorie. Wir fassen G und H als Untergruppen von $G \times H$ auf. Für $\kappa \in Z_s^2(G \times H, A)$ sei $\kappa_G \in Z_s^2(G, A)$ die Einschränkung von κ auf $G \times G$ und analog $\kappa_H \in Z_s^2(H, A)$. Dann ist

$$F: Z^2(G \times H, A) \rightarrow Z^2(G, A) \times Z^2(H, A), \quad \kappa \mapsto (\kappa_G, \kappa_H)$$

ein Homomorphismus. Für $\varphi \in C^1(G \times H, A)$ ist sicher $(\partial\varphi)_G = \partial\varphi_G \in B^2(G, A)$ und $(\partial\varphi)_H \in B^2(H, A)$. Somit induziert F einen Homomorphismus $\bar{F}: H_s^2(G \times H, A) \rightarrow H_s^2(G, A) \times H_s^2(H, A)$.

Für die Surjektivität von \bar{F} seien $\kappa_1 \in Z_s^2(G, A)$ und $\kappa_2 \in Z_s^2(H, A)$ normalisiert. Für $x_i \in G$ und $y_i \in H$ sei $\kappa(x_1 y_1, x_2 y_2) := \kappa_1(x_1, x_2) \kappa_2(y_1, y_2)$. Dann ist

$$\begin{aligned} \kappa(x_1 y_1, x_2 y_2) \kappa(x_1 x_2 y_1 y_2, x_3 y_3) &= \kappa_1(x_1, x_2) \kappa_2(y_1, y_2) \kappa_1(x_1 x_2, x_3) \kappa_2(y_1 y_2, y_3) \\ &= \kappa_1(x_2, x_3) \kappa_1(x_1, x_2 x_3) \kappa_2(y_2, y_3) \kappa_2(y_1, y_2 y_3) \\ &= \kappa(x_2 y_2, x_3 y_3) \kappa(x_1 y_1, x_2 y_2 x_3 y_3). \end{aligned}$$

Dies zeigt $\kappa \in Z_s^2(G \times H, A)$ mit $\kappa_G = \kappa_1$ und $\kappa_H = \kappa_2$. Also ist \bar{F} surjektiv.

Für die Injektivität sei $F(\kappa) = (\partial\varphi_1, \partial\varphi_2)$ mit $\varphi_1 \in C^1(G, A)$ und $\varphi_2 \in C^1(H, A)$. Sei $\varphi \in C^1(G \times H, A)$ mit $\varphi(xy) := \varphi_1(x) \varphi_2(y) \kappa(x, y)^{-1}$ für $x \in G$ und $y \in H$. Dann gilt

$$\begin{aligned} \partial\varphi(x_1 y_1, x_2 y_2) &= \varphi(x_1 y_1) \varphi(x_2 y_2) \varphi(x_1 x_2 y_1 y_2)^{-1} \\ &= \varphi_1(x_1) \varphi_2(y_1) \kappa(x_1, y_1)^{-1} \varphi_1(x_2) \varphi_2(y_2) \kappa(x_2, y_2)^{-1} \varphi_1(x_1 x_2)^{-1} \varphi_2(y_1 y_2)^{-1} \kappa(x_1 x_2, y_1 y_2) \\ &= \kappa(x_1, x_2) \kappa(y_1, y_2) \kappa(x_1, y_1)^{-1} \kappa(x_2, y_2)^{-1} \kappa(x_1 x_2, y_1 y_2) \\ &= \kappa(x_2, y_1) \kappa(x_1, x_2 y_1) \kappa(x_1 x_2, y_1)^{-1} \kappa(y_1, y_2) \kappa(x_1, y_1)^{-1} \kappa(x_2, y_2)^{-1} \kappa(x_1 x_2, y_1 y_2) \\ &= \kappa(x_1 y_1, x_2) \kappa(x_1 x_2 y_1, y_2) \kappa(x_2, y_2)^{-1} = \kappa(x_1 y_1, x_2 y_2) \end{aligned}$$

für $x_i \in G$ und $y_i \in H$. Also ist $\kappa = \partial\varphi \in B^2(G \times H, A)$ und \bar{F} ist ein Isomorphismus. \square

Folgerung 5.6. Für jede endliche abelsche Gruppe A gilt $H_s^2(A, \mathbb{C}^\times) = 1$.

Beweis. Da jede komplexe Zahl eine n -te Wurzel besitzt, gilt $\langle z^n : z \in \mathbb{C}^\times \rangle = \mathbb{C}^\times$. Die Behauptung folgt aus Satz 5.5 und Satz 5.4. \square

Folgerung 5.7. Für endliche abelsche Gruppen $G \cong C_{d_1} \times \dots \times C_{d_k}$ und $A \cong C_{e_1} \times \dots \times C_{e_l}$ gilt

$$H_s^2(G, A) \cong \text{Hom}(G, A) \cong \bigtimes_{\substack{1 \leq i \leq k \\ 1 \leq j \leq l}} C_{\text{ggT}(d_i, e_j)}.$$

Beweis. Für $d \in \mathbb{N}$ gilt $H^2(C_d, A) \cong A/\langle a^d : a \in A \rangle \cong \times_{i=1}^l C_{\text{ggT}(d, e_i)}$ nach Satz 5.4. Aus Satz 5.5 folgt $H_s^2(G, A) \cong \times_{i,j} C_{\text{ggT}(d_i, e_j)}$. Sei $G = \langle x_1 \rangle \times \dots \times \langle x_k \rangle \cong C_{d_1} \times \dots \times C_{d_k}$. Dann ist $f \in \text{Hom}(G, A)$ durch

$$f(x_i) \in \langle a \in A : a^{d_i} = 1 \rangle \cong \times_{j=1}^l C_{\text{ggT}(d_i, e_j)} \quad (i = 1, \dots, k)$$

eindeutig bestimmt und jede Wahl definiert einen Homomorphismus $G \rightarrow A$. Offenbar ist die Abbildung $\text{Hom}(G, A) \rightarrow \times_{i,j} C_{\text{ggT}(d_i, e_j)}$, $f \mapsto (f(x_1), \dots, f(x_k))$ ein Isomorphismus. Daraus folgt die Behauptung. \square

Beispiel 5.8. Nach Folgerung 5.7 gibt es vier Äquivalenzklassen abelscher Erweiterungen von C_4 mit C_4 . Allerdings gibt es nur zwei Isomorphietypen solcher Gruppen: C_4^2 und C_{16} . In Satz 5.19 bestimmen wir die Struktur von $H^2(G, A)$ für jede endliche Gruppe G .

Bemerkung 5.9. Für teilerfremde $d_1, d_2 \in \mathbb{N}$ und $e \in \mathbb{N}$ gilt $\text{ggT}(d_1 d_2, e) = \text{ggT}(d_1, e) \text{ggT}(d_2, e)$. Daher hängt die rechte Seite in Folgerung 5.7 nicht von der Zerlegung von G und A ab. Da der Ausdruck symmetrisch ist, gilt $H_s^2(A, B) \cong H_s^2(B, A)$ und $\text{Hom}(A, B) \cong \text{Hom}(B, A)$ für alle endlichen abelschen Gruppen A und B .

Definition 5.10. Eine Erweiterung G von H mit Z heißt *Schur-Erweiterung*, falls $Z \leq Z(G) \cap G'$ gilt. Der *Schur-Multiplikator* von H ist $M(H) := H^2(H, \mathbb{C}^\times)$.

Beispiel 5.11.

- (i) Sei G eine nicht-abelsche endliche nilpotente Gruppe. Nach GT-Satz 3.14 gilt $G' \cap Z(G) \neq 1$. Daher ist G eine Schur-Erweiterung einer kleineren Gruppe. Insbesondere sind D_8 und Q_8 Schur-Erweiterungen von C_2^2 . Außerdem ist $G/G^{[3]}$ eine Schur-Erweiterung von G/G' .
- (ii) Jede quasieinfache Gruppe ist eine Schur-Erweiterung einer einfachen Gruppe.

Bemerkung 5.12.

- (i) Im Folgenden studieren wir die möglichen Schur-Erweiterungen einer festen Gruppe H , die wir zu diesem Zweck in G umbenennen.
- (ii) Sei \widehat{G} eine Schur-Erweiterung von G mit $1 \neq Z \leq \widehat{G}' \cap Z(\widehat{G})$ und $\widehat{G}/Z \cong G$. Besitzt Z ein Komplement K in \widehat{G} , so wäre $\widehat{G} = Z \times K$ und $Z \not\leq 1 \times K' = \widehat{G}'$. Echte Schur-Erweiterungen sind daher nicht zerfallend.
- (iii) Ist $n := |G| < \infty$, so gilt $\exp(M(G)) \mid n$ nach Satz 4.21. Die Werte von $\kappa \in M(G)$ sind also n -te Einheitswurzeln. Dies zeigt $|M(G)| \leq |Z^2(G, \mathbb{C}^\times)| \leq n^{n^2} < \infty$. Im Folgenden sei G stets endlich und A abelsch.
- (iv) Nach Satz 5.4 ist $M(C_n) = 1$ für alle $n \in \mathbb{N}$.
- (v) Nach GT-Lemma 11.14 gilt $A^* := \text{Hom}(A, \mathbb{C}^\times) \cong A$, falls $|A| < \infty$.

Lemma 5.13. *Die Abbildung*

$$\Phi: H_s^2(G/G', A) \rightarrow H^2(G, A), \quad \kappa B^2(G/G', A) \mapsto \Phi_\kappa B^2(G, A)$$

mit $\Phi_\kappa(x, y) = \kappa(xG', yG')$ für $x, y \in G$ ist ein Monomorphismus.

Beweis. Offenbar ist $Z^2(G/G', A) \rightarrow Z^2(G, A)$, $\kappa \mapsto \Phi_\kappa$ ein Homomorphismus. Für $\varphi \in C^1(G/G', A)$ ist $\Phi_{\partial\varphi} \in B^2(G, A)$. Daher ist Φ auf $H^2(G/G', A)$ wohldefiniert. Sei $\kappa \in Z_s^2(G/G', A)$ und $\varphi \in C^1(G, A)$ mit $\Phi_\kappa = \partial\varphi$. Sei $R \subseteq G$ ein Repräsentantensystem für G/G' . Für $x \in G$ sei $r_x \in R$ mit $xG' = r_xG'$. Sei $\bar{\varphi} \in C^1(G/G', A)$ mit $\bar{\varphi}(xG') := \varphi(r_x)$ für $x \in G$. Dann gilt

$$\kappa(xG', yG') = \kappa(r_xG', r_yG') = \Phi_\kappa(r_x, r_y) = \partial\varphi(r_x, r_y) = \partial\bar{\varphi}(xG', yG')$$

für $x, y \in G$. Daher ist Φ injektiv. \square

Lemma 5.14. *Die Abbildung*

$$\Psi: H^2(G, A) \rightarrow \text{Hom}(A^*, M(G)), \quad \kappa B^2(G, A) \mapsto \Psi_\kappa$$

mit $\Psi_\kappa(\lambda) = (\lambda \circ \kappa)B^2(G, \mathbb{C}^\times)$ ist ein Homomorphismus.

Beweis. Für $\lambda, \mu \in A^*$ ist offenbar $\lambda \circ \kappa \in Z^2(G, \mathbb{C}^\times)$ und $(\lambda\mu) \circ \kappa = (\lambda \circ \kappa)(\mu \circ \kappa)$. Also ist $\Psi_\kappa \in \text{Hom}(A^*, M(G))$. Für $\varphi \in C^1(G, A)$ und $\lambda \in A^*$ gilt

$$\Psi_{\partial\varphi}(\lambda) = (\lambda \circ \partial\varphi)B^2(G, \mathbb{C}^\times) = \partial(\lambda \circ \varphi)B^2(G, \mathbb{C}^\times) = 1.$$

Also ist Ψ wohldefiniert. Wegen $\lambda \circ (\kappa_1\kappa_2) = (\lambda \circ \kappa_1)(\lambda \circ \kappa_2)$ ist Ψ ein Homomorphismus. \square

Satz 5.15 (SCHUR). *Sei \hat{G} eine Schur-Erweiterung von G mit $\hat{G}/Z \cong G$. Dann ist Z zu einer Untergruppe von $M(G)$ isomorph. Insbesondere ist $|\hat{G}| \leq |G||M(G)|$ und G besitzt nur endlich viele Schur-Erweiterungen bis auf Isomorphie.*

Beweis. Für $x \in G$ sei $\hat{x} \in \hat{G}$ mit $\hat{x}Z = x$ und $\hat{1} = 1$. Sei $\kappa \in Z^2(G, Z)$ das dazugehörige normalisierte Faktorensystem von \hat{G} (Lemma 4.5). Es gilt $\kappa(x, y) = \hat{x}\hat{y}\hat{xy}^{-1}$ für $x, y \in G$. Wegen $Z^* \cong Z$ genügt es zu zeigen, dass die Abbildung Ψ_κ aus Lemma 5.14 injektiv ist. Sei also $\lambda \in Z^*$ mit $\lambda \circ \kappa = \partial\varphi$ für ein $\varphi \in C^1(G, \mathbb{C}^\times)$. Dann ist

$$\varphi(1) = \varphi(1)\varphi(1)\varphi(1)^{-1} = \partial\varphi(1) = \lambda(\kappa(1, 1)) = \lambda(1) = 1.$$

Sei $\hat{\lambda}: \hat{G} \rightarrow \mathbb{C}^\times$ mit $\hat{\lambda}(\hat{x}a) := \varphi(x)\lambda(a)$ für $x \in G$ und $a \in Z$. Wegen $\hat{\lambda}(a) = \hat{\lambda}(\hat{1}a) = \lambda(a)$ ist $\hat{\lambda}$ eine Fortsetzung von λ . Für $x, y \in G$ und $a, b \in Z$ gilt

$$\begin{aligned} \hat{\lambda}(\hat{x}a \cdot \hat{y}b) &= \hat{\lambda}(\hat{x}\hat{y}ab) = \hat{\lambda}(\kappa(x, y)\hat{x}\hat{y}ab) = \lambda(\kappa(x, y))\varphi(xy)\lambda(a)\lambda(b) \\ &= \varphi(x)\varphi(y)\varphi(xy)^{-1}\varphi(xy)\lambda(a)\lambda(b) = \varphi(x)\lambda(a)\varphi(y)\lambda(b) = \hat{\lambda}(\hat{x}a)\hat{\lambda}(\hat{y}b). \end{aligned}$$

Also ist $\hat{\lambda}$ ein Homomorphismus mit $\hat{G}/\text{Ker}(\hat{\lambda}) \leq \mathbb{C}^\times$. Es folgt $Z \leq \hat{G}' \leq \text{Ker}(\hat{\lambda})$. Dies zeigt $\lambda = 1$. \square

Definition 5.16. Eine Schur-Erweiterung \hat{G} von G heißt *maximal*, falls $|\hat{G}| = |G||M(G)|$.

Satz 5.17 (SCHUR). *Jede endliche Gruppe G besitzt eine maximale Schur-Erweiterung.*

Beweis. Nach Bemerkung 5.12 ist $M(G) = \langle \overline{\kappa_1} \rangle \oplus \dots \oplus \langle \overline{\kappa_n} \rangle$ endlich. Sei $d_i := |\langle \overline{\kappa_i} \rangle|$ und $A_i \leq \mathbb{C}^\times$ mit $|A_i| = d_i$ für $i = 1, \dots, n$. Sei $\kappa_i \in Z^2(G, \mathbb{C}^\times)$ mit $\kappa_i B^2(G, \mathbb{C}^\times) = \overline{\kappa_i}$. Dann ist $\kappa_i^{d_i} = \partial \gamma_i$ für ein $\gamma_i \in C^1(G, \mathbb{C}^\times)$. Sei $\delta_i(x) \in \mathbb{C}^\times$ mit $\delta_i(x)^{d_i} = \gamma_i(x)^{-1}$ für $x \in G$. Nachdem wir κ_i durch $\kappa_i \partial \delta_i$ ersetzt haben, gilt $\kappa_i^{d_i} = 1$ für $i = 1, \dots, n$. Insbesondere ist $\kappa_i \in Z^2(G, A_i)$ für $i = 1, \dots, n$. Nach Lemma 4.11 dürfen wir auch $\kappa_i(x, 1) = \kappa_i(1, x) = 1$ für $x \in G$ annehmen. Sei $A := A_1 \times \dots \times A_n \cong M(G)$ und $\kappa \in C^2(G, A)$ mit $\kappa(x, y) = (\kappa_1(x, y), \dots, \kappa_n(x, y))$ für $x, y \in G$. Offenbar ist dann $\kappa \in Z^2(G, A)$ mit $\kappa(1, x) = \kappa(x, 1) = 1$ für $x \in G$.

Sei $\widehat{G} = A \times G$ die zentrale Erweiterung von A mit G bzgl. κ . Durch $a \mapsto (a, 1)$ fassen A als Untergruppe von \widehat{G} auf. Wir wählen Urbilder $\widehat{x} \in \widehat{G}$ von $x \in G$, sodass $\kappa(x, y) = \widehat{xy} \widehat{xy}^{-1}$ für alle $x, y \in G$ gilt. Sei $\pi_i: A \rightarrow A_i \leq \mathbb{C}^\times$ die i -te Projektion. Mit der Abbildung Ψ_κ aus Lemma 5.14 gilt dann

$$\Psi_\kappa(\pi_i) = (\pi_i \circ \kappa) B^2(G, \mathbb{C}^\times) = \overline{\kappa_i}$$

für $i = 1, \dots, n$. Wegen $M(G) = \langle \overline{\kappa_1}, \dots, \overline{\kappa_n} \rangle$ ist Ψ_κ surjektiv. Nach Bemerkung 5.12 ist $A^* \cong A \cong M(G)$. Daher ist Ψ_κ auch injektiv. Nach dem Hauptsatz über endliche abelsche Gruppen (angewendet auf \widehat{G}/\widehat{G}') existieren Normalteiler $N_1, \dots, N_s \trianglelefteq \widehat{G}$ mit $\widehat{G}' = N_1 \cap \dots \cap N_s$, sodass \widehat{G}/N_i zyklisch ist für $i = 1, \dots, s$.

Nehmen wir $A \not\leq \widehat{G}'$ an. Dann existiert ein i mit $A \not\leq N_i$. Indem man \widehat{G}/N_i in \mathbb{C}^\times einbettet, erhält man einen Homomorphismus $\lambda: \widehat{G} \rightarrow \widehat{G}/N_i \rightarrow \mathbb{C}^\times$ mit $\lambda(A) \neq 1$. Die Einschränkung λ_A ist also ein nicht-triviales Element in A^* . Für $x \in G$ setzen wir $\varphi(x) := \lambda(\widehat{x})$. Dann gilt

$$\Psi_\kappa(\lambda_A)(x, y) = \lambda(\kappa(x, y)) = \lambda(\widehat{xy} \widehat{xy}^{-1}) = \varphi(x) \varphi(y) \varphi(xy)^{-1} = \partial \varphi(x, y)$$

für $x, y \in G$. Dies liefert $\Psi_\kappa(\lambda_A) = 1$ im Widerspruch zur Injektivität von Ψ_κ . Also ist $A \leq \widehat{G}'$ und \widehat{G} ist eine Schur-Erweiterung von G . \square

Bemerkung 5.18. In GAP gibt es mehrere Möglichkeiten den Schur-Multiplikator und eine maximale Schur-Erweiterung zu bestimmen:

```
G:=AlternatingGroup(7);;
AbelianInvariantsMultiplier(G); #Ordnungen der zyklischen Faktoren von M(G)
S:=SchurCover(G); #maximale Schur-Erweiterung
S:=Image(IsomorphismPermGroup(S));; #effizientere Darstellung als Permutationsgruppe
NrMovedPoints(S); #Grad der Permutationsgruppe
S:=Image(SmallerDegreePermutationRepresentation(S));; #noch effizientere Darstellung
NrMovedPoints(S);
StructureDescription(S); #= C6.A7

epi:=EpimorphismSchurCover(G, [3]); #Epimorphismus G-hat -> G mit Kern O3(M(G))
S:=Source(epi); #nicht maximale Schur-Erweiterung G-hat
M:=Kernel(epi); #O3(M(G))

P:=SmallGroup(256, 111);;
SchurCovers(P); #alle maximalen Schur-Erweiterungen, nur für p-Gruppen

LoadPackage("cohomolo", false);
G:=PSL(3, 4);;
for p in PrimeDivisors(Size(G)) do
  chr:=CHR(G, p);;
  Print(SchurMultiplier(chr)); #= Op(M(G)) schneller als AbelianInvariantsMultiplier
od; #insgesamt folgt M(G) = O2(M(G))oplus O3(M(G))cong C12 x C4

LoadPackage("hap", false); #lädt weitere Pakete
GroupHomology(G, 2); #M(G)cong H2(G, Z)
```

Der Befehl **SchurExtension** berechnet hingegen die unendliche zentrale Erweiterung $F/[F, N]$ aus Satz 5.24.

Satz 5.19 (Universeller Koeffizientensatz¹⁰). *Für jede endliche abelsche Gruppe A ist*

$$1 \longrightarrow H_s^2(G/G', A) \xrightarrow{\Phi} H^2(G, A) \xrightarrow{\Psi} \text{Hom}(A^*, M(G)) \longrightarrow 1.$$

eine exakte zerfallende Folge. Insbesondere gilt

$$H^2(G, A) \cong \text{Hom}(G/G' \times M(G), A).$$

Beweis. Die Abbildungen Φ und Ψ wurden in Lemma 5.13 und Lemma 5.14 definiert. Da Φ injektiv ist, ist die Folge am ersten Glied exakt. Für $\kappa \in Z_s^2(G/G', A)$ ist $\lambda \circ \kappa \in Z_s^2(G/G', \mathbb{C}^\times) = 1$ nach Folgerung 5.6. Dies zeigt $\Psi_{\Phi\kappa} = 1$ und $\Phi(H_s^2(G/G', A)) \leq \text{Ker}(\Psi)$. Sei umgekehrt $\kappa \in Z^2(G, A)$ mit $\Psi_\kappa = 1$. Sei $\widehat{G} := A \times G$ die Erweiterung bzgl. κ . Durch $a \mapsto (a, 1)$ fassen wir A als Untergruppe von \widehat{G} auf. Für $\lambda \in A^*$ existiert ein $\varphi \in C^1(G, \mathbb{C}^\times)$ mit $\lambda \circ \kappa = \partial\varphi$. Wir definieren $\widehat{\lambda}: \widehat{G} \rightarrow \mathbb{C}^\times$, $(a, x) \mapsto \lambda(a)\varphi(x)$. Für $(a, x), (b, y) \in \widehat{G}$ gilt dann

$$\widehat{\lambda}((a, x)(b, y)) = \widehat{\lambda}(ab\kappa(x, y), xy) = \lambda(ab)\partial\varphi(x, y)\varphi(xy) = \lambda(a)\varphi(x)\lambda(b)\varphi(y) = \widehat{\lambda}(a, x)\widehat{\lambda}(b, y).$$

Dies zeigt $\widehat{\lambda} \in \widehat{G}^*$ und $\widehat{G}' \cap A \leq \text{Ker}(\widehat{\lambda})$. Bekanntlich existiert für jedes $a \in A \setminus \{1\}$ ein $\lambda \in A^*$ mit $\lambda(a) \neq 1$. Daraus folgt $\widehat{G}' \cap A = 1$. Also ist \widehat{G}/\widehat{G}' eine Erweiterung von

$$\widehat{G}/\widehat{G}'A \cong (\widehat{G}/A)/(\widehat{G}'A/A) \cong G/G'$$

mit $A\widehat{G}'/\widehat{G}' \cong A/(A \cap \widehat{G}') \cong A$. Sei $\pi: \widehat{G} \rightarrow G$, $(a, x) \mapsto x$ die Projektion und $\bar{\pi}: \widehat{G}/\widehat{G}' \rightarrow G/G'$, $x\widehat{G}' \mapsto \pi(x)G'$. Wegen $\widehat{G}' \cong \widehat{G}'A/A \cong G'$ ist die Einschränkung von π auf \widehat{G}' injektiv. Für $s \in G'$ sei $\widehat{s} := \pi^{-1}(s) \in \widehat{G}'$. Sei $R \subseteq G$ ein Repräsentantensystem für G/G' . Für $x \in G$ sei $r_x \in R$ mit $xG' = r_xG'$. Für $r \in R$ sei $\widehat{r} \in \widehat{G}$ ein beliebiges Urbild unter π . Für jedes $x \in G$ existiert genau ein $s_x \in G'$ mit $x = r_x s_x$. Nun ist $\widehat{x} := \widehat{r}_x \widehat{s}_x$ ein Urbild von x unter π . Daher ist κ äquivalent zu $\kappa' \in Z^2(G, A)$ mit $\kappa'(x, y) = \widehat{x}\widehat{y}\widehat{xy}^{-1}$. Offenbar ist $\widehat{x}\widehat{G}'$ ein Urbild von xG' unter $\bar{\pi}$, das nicht von der Wahl des Repräsentanten der Nebenklasse xG' abhängt. Somit existiert ein Kozyklus $\bar{\kappa} \in Z^2(G/G', A)$ mit

$$\bar{\kappa}(xG', yG') = \widehat{x}\widehat{y}\widehat{xy}^{-1}\widehat{G}' = \kappa'(x, y)\widehat{G}'.$$

Dies zeigt $\kappa B^2(G, A) = \kappa' B^2(G, A) = \Phi_{\bar{\kappa}}$, indem man A mit $A\widehat{G}'/\widehat{G}'$ identifiziert. Da \widehat{G}/\widehat{G}' abelsch ist, gilt $\bar{\kappa} \in Z_s^2(G/G', A)$ und $\Phi(H_s^2(G/G', A)) = \text{Ker}(\Psi)$. Also ist die Folge auch am zweiten Glied exakt.

Wir konstruieren jetzt einen Homomorphismus $\Gamma: \text{Hom}(A^*, M(G)) \rightarrow H^2(G, A)$ mit $\Psi \circ \Gamma = \text{id}$. Daraus erhält man sowohl die Surjektivität von Ψ (Exaktheit am dritten Glied) als auch das Zerfallen der Folge. Sei $Z := M(G)$ und $\kappa \in Z^2(G, Z)$ der Kozyklus einer maximalen Schur-Erweiterung. Im Beweis von Satz 5.17 haben wir gesehen, dass die Abbildung $Z^* \rightarrow Z$, $\lambda \mapsto (\lambda \circ \kappa)B^2(G, \mathbb{C}^\times)$ ein Isomorphismus ist. Sei $f \in \text{Hom}(A^*, Z)$. Für $\mu \in A^*$ existiert genau ein $\lambda_\mu \in Z^*$ mit $f(\mu) = (\lambda_\mu \circ \kappa)B^2(G, \mathbb{C}^\times)$. Für $x, y \in G$ definieren wir $\alpha_f(x, y): A^* \rightarrow \mathbb{C}^\times$, $\mu \mapsto \lambda_\mu(\kappa(x, y))$. Aus

$$(\lambda_{\mu_1\mu_2} \circ \kappa)B^2(G, \mathbb{C}^\times) = f(\mu_1\mu_2) = f(\mu_1)f(\mu_2) = (\lambda_{\mu_1} \circ \kappa)(\lambda_{\mu_2} \circ \kappa)B^2(G, \mathbb{C}^\times) = (\lambda_{\mu_1}\lambda_{\mu_2} \circ \kappa)B^2(G, \mathbb{C}^\times)$$

¹⁰Die Bezeichnung beschreibt den Sachverhalt, dass man den Wertebereich A der Kozyklen durch den *universellen* Wertebereich \mathbb{C}^\times ersetzen kann.

folgt $\lambda_{\mu_1\mu_2} = \lambda_{\mu_1}\lambda_{\mu_2}$. Dies zeigt $\alpha_f(x, y) \in (A^*)^*$. Wegen $|A| < \infty$ ist $A \rightarrow (A^*)^*$, $a \mapsto (\mu \mapsto \mu(a))$ ein Isomorphismus (GT-Aufgabe 76). Daher existiert genau ein $\Gamma_f(x, y) \in A$ mit $\alpha_f(x, y)(\mu) = \mu(\Gamma_f(x, y))$ für alle $\mu \in A^*$. Für $x, y, z \in G$ und $\mu \in A^*$ gilt

$$\begin{aligned}\mu(\Gamma_f(x, y)\Gamma_f(xy, z)) &= \alpha_f(x, y)(\mu)\alpha_f(xy, z)(\mu) = \lambda_\mu(\kappa(x, y)\kappa(xy, z)) \\ &= \lambda_\mu(\kappa(y, z)\kappa(x, yz)) = \mu(\Gamma_f(y, z)\Gamma_f(x, yz)).\end{aligned}$$

Dies zeigt $\Gamma_f \in Z^2(G, A)$. Für $f' \in \text{Hom}(A^*, Z)$ und $\mu \in A^*$ sei $\lambda'_\mu \in Z^*$ mit $f'(\mu) = (\lambda'_\mu \circ \kappa)B^2(G, \mathbb{C}^\times)$. Dann gilt $(f'f)(\mu) = (\lambda_\mu\lambda'_\mu \circ \kappa)B^2(G, \mathbb{C}^\times)$ und

$$\mu(\Gamma_{ff'}(x, y)) = \alpha_{ff'}(x, y)(\mu) = (\lambda_\mu\lambda'_\mu)(\kappa(x, y)) = \alpha_f(x, y)(\mu)\alpha_{f'}(x, y)(\mu) = \mu(\Gamma_f(x, y)\Gamma_{f'}(x, y)).$$

Also ist Γ ein Homomorphismus. Aus

$$\Psi_{\Gamma_f}(\mu)(x, y) = (\mu \circ \Gamma_f)(x, y) = \alpha_f(x, y)(\mu) = \lambda_\mu(\kappa(x, y)) = f(\mu)(x, y).$$

folgt $\Psi \circ \Gamma = \text{id}$.

Für die zweite Behauptung benutzen wir Bemerkung 5.9 und $A^* \cong A$:

$$H^2(G, A) \cong H_s^2(G/G', A) \times \text{Hom}(A^*, Z) \cong \text{Hom}(G/G', A) \times \text{Hom}(Z, A) \cong \text{Hom}(G/G' \times Z, A). \quad \square$$

Satz 5.20. *Sei $G/G' \cong C_{d_1} \times \cdots \times C_{d_k}$ und $M(G) \cong C_{e_1} \times \cdots \times C_{e_l}$. Dann besitzt G höchstens*

$$\prod_{\substack{1 \leq i \leq k \\ 1 \leq j \leq l}} \text{ggT}(d_i, e_j)$$

maximale Schur-Erweiterungen bis auf Isomorphie.

Beweis. Sei $\widehat{G} := Z \times G$ eine maximale Schur-Erweiterung von G bzgl. $\kappa \in Z^2(G, Z)$ mit $Z \cong M(G)$. Wie im Beweis von Satz 5.17 ist $\Psi_\kappa: Z^* \rightarrow M(G)$ ein Isomorphismus. Wir zeigen, dass der Isomorphietyp von \widehat{G} nicht von Ψ_κ abhängt. Sei dafür $f \in \text{Aut}(Z)$ und $\kappa' \in Z^2(G, Z)$ mit $\kappa'(x, y) = f(\kappa(x, y))$ für alle $x, y \in G$. Sei $\widehat{H} := Z \times G$ die Erweiterung von G mit Z bzgl. κ' . Dann ist

$$F: \widehat{G} \rightarrow \widehat{H}, \quad (a, x) \mapsto (f(a), x)$$

ein Isomorphismus, denn

$$\begin{aligned}F((a, x)(b, y)) &= F(ab\kappa(x, y), xy) = (f(ab\kappa(x, y)), xy) \\ &= (f(a)f(b)\kappa'(x, y), xy) = (f(a), x)(f(b), y) = F(a, x)F(b, y)\end{aligned}$$

für $(a, x), (b, y) \in \widehat{G}$. Sei $f^* \in \text{Aut}(Z^*)$, $\lambda \mapsto \lambda \circ f$ die zu f duale Abbildung. Dann gilt $\Psi_{\kappa'} = \Psi_\kappa \circ f^*$. Auf diese Weise lässt sich jeder Isomorphismus $Z^* \rightarrow M(G)$ realisieren. Für jede weitere maximale Schur-Erweiterung von G bzgl. eines $\alpha \in Z^2(G, Z)$ kann man also $\Psi_\alpha = \Psi_\kappa$ annehmen. Die Anzahl der maximalen Schur-Erweiterungen ist somit beschränkt durch $|\Psi^{-1}(\Psi_\kappa)| = |\text{Ker}(\Psi)| = |H_s^2(G/G', Z)|$ nach Satz 5.19. Folgerung 5.7 liefert die Behauptung. \square

Beispiel 5.21.

- (i) Sei p eine Primzahl und $G \cong C_p^n$ elementarabelsch. Nach GT-Beispiel 11.38 ist $M(G) \cong C_p^{\binom{n}{2}}$. Also besitzt G höchstens $p^{\binom{n}{2}}$ maximale Schur-Erweiterungen bis auf Isomorphie. Dies lässt sich auch

direkt beweisen: Sei \hat{G} eine maximale Schur-Erweiterung und $Z \leq \hat{G}' \cap Z(\hat{G})$ mit $\hat{G}/Z \cong G$. Wegen $Z \leq \Phi(\hat{G})$ lässt sich G mit n Elementen x_1, \dots, x_n erzeugen. Dann ist $\{[x_i, x_j] : 1 \leq i < j \leq n\}$ eine Basis von $Z \cong M(G)$. Für $i = 1, \dots, n$ existieren $0 \leq e_{ijk} < p$ mit

$$x_i^p = \prod_{j < k} [x_j, x_k]^{e_{ijk}}.$$

Wegen $Z \leq Z(\hat{G})$ ist \hat{G} durch die $n \binom{n}{2}$ Parameter e_{ijk} eindeutig bestimmt. Offensichtlich führen viele Parameterwerte zu isomorphen Gruppen (zum Beispiel durch Permutation der x_i). In Bemerkung 12.36 konstruieren wir die maximale Schur-Erweiterung mit $p > 2$ und $e_{ijk} = 0$ für alle i, j, k . Für $n = 2$ sind die beiden nicht-abelschen Gruppen der Ordnung p^3 die einzigen maximalen Schur-Erweiterungen. Für $p^n \in \{2^3, 2^4, 3^3, 5^3\}$ gibt es 10, 989, 16 bzw. 20 maximale Schur-Erweiterungen von G . Im Allgemeinen ist die Anzahl unbekannt.

- (ii) Die minimal nicht-abelsche 2-Gruppe $Q(2, 1)$ aus Aufgabe 6 besitzt genau sieben maximale Schur-Erweiterungen:

```
G:=SmallGroup(16,3);; #=Q(2,1)
ab:=AbelianInvariants(G); #=[2,4]
mG:=AbelianInvariantsMultiplier(G); #=[2,2]
ProductX(ab,mG,{d,e}->Gcd(d,e)); #=16
Size(SchurCovers(G)); #=7
```

Bemerkung 5.22.

- (i) Ist G perfekt (oder allgemeiner $\text{ggT}(|G/G'|, |M(G)|) = 1$), so besitzt G nur eine maximale Schur-Erweiterung \hat{G} bis auf Isomorphie. Man nennt \hat{G} die *universelle* Schur-Erweiterung von G , denn nach Satz 5.24 ist jede Schur-Erweiterung von G ein Quotient von \hat{G} .
- (ii) Für vollständige Gruppen G gilt Gleichheit in Satz 5.20 (ohne Beweis).

Satz 5.23. Sei G eine beliebige Gruppe mit $|G : Z(G)| < \infty$. Dann ist $|G'| < \infty$.

Beweis (Rosenlicht). Sei $Z := Z(G)$ und $n := |G : Z| < \infty$. Sei R ein Repräsentantensystem für G/Z . Für $\Gamma := \{[r, s] : r, s \in R\}$ gilt $|\Gamma| \leq |R|^2 = |G/Z|^2 = n^2$. Für $r, s \in R$ und $z \in Z$ gilt $[rz, s] = [r, s] = [r, sz]$. Jedes Element $g \in G'$ hat also die Form $g = c_1 \dots c_m$ mit $c_1, \dots, c_m \in \Gamma$. Es genügt zu zeigen, dass man dabei $m \leq n^3$ wählen kann (dann folgt $|G'| \leq n^{2n^3} < \infty$). Nehmen wir $m > n^3$ an. Dann existiert ein $\gamma \in \Gamma$ mit $|\{i \in \{1, \dots, m\} : c_i = \gamma\}| > n$. Wegen $c_i c_{i+1} = c_{i+1} (c_{i+1}^{-1} c_i c_{i+1}) = c_{i+1} \delta$ mit $\delta \in \Gamma$ können wir $c_1 = \dots = c_{n+1} = \gamma$ annehmen. Im Widerspruch zur Minimalität von m werden wir zeigen, dass γ^{n+1} ein Produkt von n Kommutatoren ist. Sei dafür $\gamma = [r, s]$ mit $r, s \in R$. Wegen $\gamma^n = \gamma^{|G:Z|} \in Z$ ist

$$\gamma^{n+1} = \gamma \gamma^n = \gamma s \gamma^n s^{-1} = \gamma s \gamma s^{-1} (s \gamma s^{-1})^{n-1} = [r, s] s [r, s] s^{-1} [s r s^{-1}, s]^{n-1} = [r, s^2] [s r s^{-1}, s]^{n-1}. \quad \square$$

Satz 5.24. Sei $G = F/N$ eine endliche Gruppe mit $F = F_n$. Dann gilt:

- (i) $N/[F, N]$ ist eine endlich erzeugte abelsche Gruppe mit freiem Teil vom Rang n und Torsionsteil $(F' \cap N)/[F, N]$.
- (ii) Für $N/[F, N] = (F' \cap N)/[F, N] \oplus K/[F, N]$ ist F/K eine maximale Schur-Erweiterung von G .
- (iii) Für jede Schur-Erweiterung \hat{G} von G existiert ein $L \trianglelefteq F$ mit $N = (F' \cap N)L$ und $\hat{G} \cong F/L$. Insbesondere ist \hat{G} eine Faktorgruppe einer maximalen Schur-Erweiterung.

(iv) $\boxed{M(G) \cong (F' \cap N)/[F, N]}$ (Hopf-Formel).

Beweis.

- (i) Nach Satz 2.11 ist N endlich erzeugt. Mit $N \trianglelefteq F$ ist $[F, N] \trianglelefteq F$ und $[F, N] \leq F' \cap N$. Wegen $N/[F, N] \leq Z(F/[F, N])$ hat $Z(F/[F, N])$ endlichen Index in $F/[F, N]$. Nach Satz 5.23 ist $F'/[F, N]$ endlich. Daher ist auch $(F' \cap N)/[F, N]$ endlich. Wegen $N' \leq [F, N]$ ist $N/[F, N]$ abelsch. Weiter ist

$$(N/[F, N])/((F' \cap N)/[F, N]) \cong N/(F' \cap N) \cong NF'/F' \leq F/F'.$$

Nach Beispiel 1.17 ist F/F' eine freie abelsche Gruppe vom Rang n . Wegen $|F/N| = |G| < \infty$ muss auch NF'/F' eine freie abelsche Gruppe vom Rang n sein. Daher ist $(F' \cap N)/[F, N]$ der Torsionsteil von $N/[F, N]$.

- (ii) Wegen $K/[F, N] \leq N/[F, N] \leq Z(F/[F, N])$ ist $K \trianglelefteq F$. Sei $\widehat{G} := F/K$ und $Z := N/K$. Dann gilt $\widehat{G}/Z \cong F/N \cong G$ und $Z \leq Z(\widehat{G})$ wegen $[F, N] \leq K$. Aus $N/[F, N] \leq F'K/[F, N]$ folgt

$$Z = N/K \leq F'K/K = (F/K)' = \widehat{G}'.$$

Also ist \widehat{G} eine Schur-Erweiterung mit $Z \cong (F' \cap N)/[F, N]$. Aus Satz 5.15 folgt $|M(G)| \geq |(F' \cap N)/[F, N]|$. Für die umgekehrte Ungleichung zeigen wir erst (iii).

- (iii) Seien $\alpha: F \rightarrow G$ und $\beta: \widehat{G} \rightarrow G$ die kanonischen Epimorphismen mit $N = \text{Ker}(\alpha)$ und $Z := \text{Ker}(\beta)$. Da F frei ist, existiert ein Homomorphismus $\rho: F \rightarrow \widehat{G}$ mit $\beta\rho = \alpha$. Es gilt dann $\widehat{G} = \rho(F)Z$ und $Z \leq \widehat{G}' \leq \rho(F)' \leq \rho(F)$, also $\rho(F) = \widehat{G}$. Offenbar ist $L := \text{Ker}(\rho) \leq \text{Ker}(\alpha) = N$. Wegen $\beta\rho(N) = \alpha(N) = 1$ ist $\rho(N) \leq \text{Ker}(\beta) = Z$. Dies zeigt $\rho([F, N]) \leq [\widehat{G}, Z] = 1$ und $[F, N] \leq L$. Aus $\rho(N) = Z \leq \widehat{G}' = \rho(F')$ folgt außerdem $N \leq F'L$ und $(F' \cap N)L = F'L \cap N = N$ nach Dedekind. Nun gilt

$$|Z| = \frac{|\widehat{G}|}{|G|} = |N : L| = |(F' \cap N)L : L| = |F' \cap N : F' \cap L| \leq |(F' \cap N)/[F, N]|.$$

Daher ist die in (ii) konstruierte Schur-Erweiterung tatsächlich maximal.

Nach (i) und dem Hauptsatz über endlich erzeugte abelsche Gruppen gilt

$$L/[F, N] = (L \cap F')/[F, N] \oplus M/[F, N],$$

wobei $(L \cap F')/[F, N]$ der Torsionsteil ist. Wegen $|N : L| = |F' \cap N : F' \cap L|$ ist $M/[F, N]$ der torsionsfreie Teil von $N/[F, N]$. Nach (ii) ist F/M eine maximale Schur-Erweiterung und $\widehat{G} \cong F/L \cong (F/M)/(L/M)$.

- (iv) Folgt aus dem Beweis von (ii). □

Satz 5.25. Sei $G = \langle x_1, \dots, x_n \mid r_1, \dots, r_k \rangle$ endlich. Dann lässt sich $M(G)$ mit $k - n$ Elementen erzeugen. Insbesondere ist $M(G) = 1$ falls $n = k$.

Beweis. Nach Satz 1.21 ist $n \leq k$. Sei F die freie Gruppe bzgl. x_1, \dots, x_n und $N := \langle r_1, \dots, r_k \rangle^F$. Wegen $N/[F, N] \leq Z(F/[F, N])$ ist $N/[F, N] = \langle \bar{r}_1, \dots, \bar{r}_k \rangle$, wobei $\bar{r}_i := r_i[F, N]$. Nach Satz 5.24 hat der freie Teil von $N/[F, N]$ Rang n und der Torsionsteil ist zu $M(G)$ isomorph. Also lässt sich $M(G)$ mit $k - n$ Elementen erzeugen. □

Beispiel 5.26. Nach Satz 5.25 und Aufgabe 2 ist $M(Q_{2^n}) = 1$ für $m \geq 1$ und $n \geq 3$ (vgl. GT-Beispiel 11.38). Für unendliche Gruppen ist Satz 5.25 falsch: Zum Beispiel ist $F_2/F_2^{[3]}$ eine Schur-Erweiterung von $F_2/F_2' \cong \langle x, y \mid [x, y] = 1 \rangle \cong C_\infty^2$.

Satz 5.27. Seien $\widehat{G}_1, \widehat{G}_2$ maximale Schur-Erweiterungen von G mit $\widehat{G}_1/Z_1 \cong G \cong \widehat{G}_2/Z_2$. Dann gilt

- (i) (SCHUR) $\widehat{G}'_1 \cong \widehat{G}'_2$ und $\widehat{G}_1/\widehat{G}'_1 \cong G/G' \cong \widehat{G}_2/\widehat{G}'_2$.
- (ii) (GASCHÜTZ) $\widehat{G}_1/Z(\widehat{G}_1) \cong \widehat{G}_2/Z(\widehat{G}_2)$.
- (iii) (READ) $Z(\widehat{G}_1)/Z_1 \cong Z(\widehat{G}_2)/Z_2$.

Beweis. Sei $G = F/N$, $K_i \trianglelefteq F$ und $\widehat{G}_i \cong F/K_i$ wie in Satz 5.24. Wir zeigen, dass die angegebenen Gruppen nicht von i abhängen.

(i) Es gilt

$$\begin{aligned}\widehat{G}'_i &\cong F'K_i/K_i \cong F'/(F' \cap K_i) = F'/(F' \cap N \cap K_i) = F'/[F, N], \\ \widehat{G}_i/\widehat{G}'_i &\cong (\widehat{G}_i/Z_i)/(\widehat{G}'_i/Z_i) \cong G/G'.\end{aligned}$$

(ii) Für $L/[F, N] := Z(F/[F, N])$ gilt $[F, L] \leq [F, N] \leq K_i$ und $L/K_i \leq Z(F/K_i)$. Sei umgekehrt $xK_i \in Z(F/K_i)$. Dann ist $[x, F] \leq K_i \cap F' = K_i \cap F' \cap N = [F, N]$ und es folgt $x[F, N] \in Z(F/[F, N]) = L/[F, N]$. Dies zeigt

$$\widehat{G}_i/Z(\widehat{G}_i) \cong (F/K_i)/Z(F/K_i) = (F/K_i)/(L/K_i) \cong F/L.$$

(iii) Mit den Bezeichnungen aus (ii) gilt

$$Z(\widehat{G}_i)/Z_i \cong (L/K_i)/(N/K_i) \cong L/N. \quad \square$$

Bemerkung 5.28.

(i) Im Allgemeinen ist $Z(\widehat{G}_1) \not\cong Z(\widehat{G}_2)$ in der Situation von Satz 5.27. Zum Beispiel sind die minimal nicht-abelschen Gruppen

$$\begin{aligned}\widehat{G}_1 &= \langle x, y \mid x^8 = y^2 = 1, \ yxy^{-1} = x^5 \rangle, \\ \widehat{G}_2 &= \langle x, y \mid x^4 = y^2 = [x, y]^2 = [x, x, y] = [y, x, y] = 1 \rangle\end{aligned}$$

der Ordnung 16 aus Aufgabe 4 und Aufgabe 6 maximale Schur-Erweiterungen von $G = C_4 \times C_2$ mit $Z(\widehat{G}_1) = \langle x^2 \rangle \cong C_4$ und $Z(\widehat{G}_2) = \langle x^2, [x, y] \rangle \cong C_2^2$ (aus GT-Satz 11.37 folgt $M(G) \cong C_2$).

(ii) Schur-Multiplikatoren kommen auch in der Darstellungstheorie endlicher Gruppen vor: Sei $N \trianglelefteq G$ und $\Delta: N \rightarrow \text{GL}(d, \mathbb{C})$ eine irreduzible Darstellung von N . Für $g \in G$ ist auch ${}^g\Delta: N \rightarrow \text{GL}(d, \mathbb{C})$, $x \mapsto \Delta(g^{-1}xg)$ eine Darstellung. Nehmen wir an, dass Δ und ${}^g\Delta$ für alle $g \in G$ äquivalent sind, d. h. für $g \in G$ existiert $T_g \in \text{GL}(d, \mathbb{C})$ mit ${}^g\Delta(x) = T_g\Delta(x)T_g^{-1}$ für alle $x \in N$. Sei $g_1, \dots, g_k \in G$ ein Repräsentantensystem für G/N und $T_i := T_{g_i}$. Für $x \in N$ definieren wir

$$\Gamma: G \rightarrow \text{GL}(d, \mathbb{C}), \quad g_ix \mapsto \Delta(x^{-1})T_i.$$

Für $y \in N$ gilt

$$\Gamma(g_ix)\Delta(y)\Gamma(g_ix)^{-1} = \Delta(x^{-1})T_i\Delta(y)T_i^{-1}\Delta(x) = \Delta(x^{-1}g_i^{-1}yg_ix) = {}^{g_ix}\Delta(y).$$

Dies zeigt

$$\Gamma(gh)\Delta(y)\Gamma(gh)^{-1} = {}^{gh}\Delta(y) = {}^g({}^h\Delta)(y) = \Gamma(g)\Gamma(h)\Delta(y)\Gamma(h)^{-1}\Gamma(g)^{-1}$$

für $g, h \in G$ und alle $y \in N$. Aus Schurs Lemma¹¹ folgt $\Gamma(gh) = \kappa(g, h)\Gamma(g)\Gamma(h)$ für ein $\kappa(g, h) \in \mathbb{C}^\times$. Man nennt Γ eine *projektive Darstellung* von G , denn $G \rightarrow \text{PGL}(d, \mathbb{C})$, $g \mapsto \Gamma(g)\mathbb{C}^\times$ ist ein Homomorphismus. Wegen

$$\begin{aligned} \kappa(x, yz)\kappa(y, z)\Gamma(x)\Gamma(y)\Gamma(z) &= \kappa(x, yz)\Gamma(x)\Gamma(yz) = \Gamma(x(yz)) = \Gamma((xy)z) \\ &= \kappa(xy, z)\Gamma(xy)\Gamma(z) = \kappa(xy, z)\kappa(x, y)\Gamma(x)\Gamma(y)\Gamma(z) \end{aligned}$$

ist $\kappa \in Z^2(G, \mathbb{C}^\times)$. Tatsächlich hängt κ nur G/N ab, d. h. $\kappa \in Z^2(G/N, \mathbb{C}^\times)$. Andere Wahlen der T_i liefern äquivalente κ . Im Fall $M(G/N) = 1$ kann man $\kappa = 1$ erreichen. Dann ist Γ eine gewöhnliche Darstellung, die Δ fortsetzt.

- (iii) Wir beschäftigen uns nun mit der Frage, welche Gruppen die Form $G/Z(G)$ haben. Dabei lassen wir wieder unendliche Gruppen G zu.

Definition 5.29. Man nennt G *zentral erweiterbar* (engl. *capable*), falls eine Gruppe H mit $H/Z(H) \cong G$ existiert. Sei $Z^*(G)$ der Durchschnitt aller Normalteiler N , sodass G/N zentral erweiterbar ist. Man nennt $Z^*(G)$ das *Epizentrum* von G .

Bemerkung 5.30.

- (i) Zentral erweiterbare Gruppen sind innere Automorphismengruppen wegen $H/Z(H) \cong \text{Inn}(H)$.
- (ii) Da $G/Z(G)$ zentral erweiterbar ist, gilt $Z^*(G) \leq Z(G)$. Offenbar ist $Z^*(G)$ charakteristisch in G .

Beispiel 5.31. Gruppen mit trivialem Zentrum sind zentral erweiterbar. Wegen $D_{4n}/Z(D_{4n}) \cong D_{2n}$ sind alle Diedergruppen zentral erweiterbar. Nicht-triviale zyklische Gruppen sind nicht zentral erweiterbar.

Lemma 5.32. Für jede Gruppe G ist $G/Z^*(G)$ zentral erweiterbar.

Beweis. Sei $\{N_i : i \in I\}$ die Menge der Normalteiler von G , sodass G/N_i zentral erweiterbar ist. Dann existieren Gruppen $\{H_i : i \in I\}$ und Epimorphismen $\varphi_i : H_i \rightarrow G/N_i$ mit $\text{Ker}(\varphi_i) = Z(H_i)$. Sei $H := \times_{i \in I} H_i$ und

$$L := \{(h_i)_i \in H : \exists g \in G : \forall i \in I : \varphi_i(h_i) = gN_i\} \leq H.$$

Sicher ist $Z(H) = \times Z(H_i) \leq Z(L)$. Da die Projektion von L nach H_i für jedes i surjektiv ist, gilt $Z(H) = Z(L)$. Für jedes $g \in G$ existiert genau ein Tupel $(h_i)_i \in L/Z(L)$ mit $\varphi_i(h_i) = gN_i$ für alle $i \in I$. Man sieht leicht, dass die Abbildung $G \rightarrow L/Z(L)$, $g \mapsto (h_i)_i Z(L)$ ein Epimorphismus mit Kern $Z^*(G) = \bigcap_{i \in I} N_i$ ist. Also ist $G/Z^*(G) \cong L/Z(L)$ zentral erweiterbar. \square

Folgerung 5.33. Genau dann ist G zentral erweiterbar, wenn $Z^*(G) = 1$ gilt.

Lemma 5.34. Für jede Gruppe G ist $Z^*(G)$ der Durchschnitt aller Untergruppen der Form $\pi(Z(H))$, wobei $Z \rightarrow H \xrightarrow{\pi} G$ eine zentrale Erweiterung von G ist.

¹¹siehe Lemma 1.9 in Charaktertheorie-Skript

Beweis. Sei $D \leq G$ der Durchschnitt über $\pi(Z(H))$ wie angegeben. Für jede zentrale Erweiterung $\pi: H \rightarrow G$ gilt $\pi(Z(H)) \trianglelefteq \pi(H) = G$ und

$$G/\pi(Z(H)) \cong (H/\text{Ker}(\pi))/(Z(H)/\text{Ker}(\pi)) \cong H/Z(H).$$

Also ist $G/\pi(Z(H))$ zentral erweiterbar und $Z^*(G) \leq D$.

Sei umgekehrt G/N zentral erweiterbar für ein $N \trianglelefteq G$. Dann existiert ein Epimorphismus $\alpha: H \rightarrow G/N$ mit $\text{Ker}(\alpha) = Z(H)$. Sei

$$L := \{(x, y) \in G \times H : \alpha(y) = xN\} \leq G \times H.$$

Die Projektion $\rho: L \rightarrow G$, $(x, y) \rightarrow x$ ist surjektiv mit $\text{Ker}(\rho) = 1 \times \text{Ker}(\pi) \leq Z(L)$. Also ist ρ eine zentrale Erweiterung von G . Es folgt $D \leq \rho(Z(L))$. Da die Projektion von L nach H surjektiv ist, gilt $Z(L) \leq G \times Z(H)$. Wegen $Z(H) = \text{Ker}(\alpha)$ ist $Z(L) \leq N \times Z(H)$ und $D \leq \rho(Z(L)) \leq N$. Dies zeigt $D \leq Z^*(G)$. \square

Bemerkung 5.35. Wir zeigen, dass man in Lemma 5.34 (für endliche Gruppen) nur eine einzige zentrale Erweiterung betrachten muss.

Satz 5.36 (BEYL-FELGNER-SCHMID). *Sei \widehat{G} eine maximale Schur-Erweiterung einer endlichen Gruppe G und $\gamma: \widehat{G} \rightarrow G$ der entsprechende Epimorphismus. Dann gilt $Z^*(G) = \gamma(Z(\widehat{G}))$.*

Beweis. Da jede Schur-Erweiterung zentral ist, gilt $Z^*(G) \leq \gamma(Z(\widehat{G}))$ nach Lemma 5.34. Sei umgekehrt $\alpha: H \rightarrow G$ eine zentrale Erweiterung. Wir müssen $\gamma(Z(\widehat{G})) \leq \alpha(Z(H))$ zeigen. Sei F eine freie Gruppe und $\pi: F \rightarrow G$ ein Epimorphismus mit Kern N . Dann existiert ein Homomorphismus $\varphi: F \rightarrow H$ mit $\alpha\varphi = \pi$. Wegen $\alpha(\varphi(N)) = \pi(N) = 1$ ist $\varphi(N) \leq \text{Ker}(\alpha) \leq Z(H)$. Es folgt $\varphi([F, N]) \leq [H, Z(H)] = 1$. Da π surjektiv ist, gilt $H = \text{Ker}(\alpha)\varphi(F) = Z(H)\varphi(F)$.

Nach Satz 5.24 können wir $\widehat{G} = F/K$ annehmen, wobei $N/[F, N] = (F' \cap N)/[F, N] \oplus K/[F, N]$. Außerdem sei $\gamma(xK) = \pi(x)$ für alle $x \in F$. Sei $W/K := Z(\widehat{G})$. Dann gilt

$$[\varphi(W), \varphi(F)] = \varphi([W, F]) \leq \varphi(F' \cap K) = \varphi(F' \cap N \cap K) = \varphi([F, N]) = 1.$$

Es folgt $\varphi(W) \leq Z(H)$ und $\gamma(Z(\widehat{G})) = \pi(W) \leq \alpha(Z(H))$. \square

Folgerung 5.37. *Sei G endlich mit $M(G) = 1$. Genau dann ist G zentral erweiterbar, wenn $Z(G) = 1$ gilt.*

Beispiel 5.38. Für $n \geq 3$ ist Q_{2^n} nicht zentral erweiterbar, denn $M(Q_{2^n}) = 1$ (Beispiel 5.26) und $Z(Q_{2^n}) \neq 1$.

Satz 5.39 (BAER). *Sei $A = C_{d_1} \times \dots \times C_{d_k}$ eine endliche abelsche Gruppe mit $1 \neq d_1 \mid d_2 \mid \dots \mid d_k$. Genau dann ist A zentral erweiterbar, wenn $k \geq 2$ und $d_{k-1} = d_k$ gilt.*

Beweis. Für $k = 1$ ist $A \neq 1$ zyklisch und daher nicht zentral erweiterbar. Sei nun $k \geq 2$. Sei $A = \langle a_1 \rangle \times \dots \times \langle a_k \rangle$ mit $|\langle a_i \rangle| = d_i$ für $i = 1, \dots, k$. Nehmen wir zuerst an, dass A zentral erweiterbar ist. Sei $\gamma: H \rightarrow A$ ein Epimorphismus mit $\text{Ker}(\gamma) = Z(H)$. Sei $H_i := \gamma^{-1}(\langle a_i a_k \rangle)$ für $i = 1, \dots, k-1$ und $H_k := \gamma^{-1}(\langle a_k \rangle)$. Da $H_i/Z(H)$ zyklisch ist, ist H_i abelsch für $i = 1, \dots, k$. Wegen $A = \langle a_1 a_k, \dots, a_{k-1} a_k, a_k \rangle$ gilt $H = \langle H_1, \dots, H_k \rangle$ und $\bigcap_{i=1}^k H_i = Z(H)$. Wegen $(a_i a_k)^{d_{k-1}} = a_k^{d_{k-1}}$ für $i = 1, \dots, k-1$ ist $\gamma^{-1}(a_k^{d_{k-1}}) \in Z(H) = \text{Ker}(\gamma)$, d. h. $d_k = |\langle a_k \rangle| = d_{k-1}$.

Sei nun $Z := Z^*(A) \neq 1$. Sei F eine freie Gruppe und $N, L \trianglelefteq F$ mit $F/N \cong A$ und $F/L \cong (F/N)/(L/N) \cong A/Z$. Sei $\hat{A} := F/K$ eine maximale Schur-Erweiterung von A mit $N/[F, N] = (F' \cap N)/[F, N] \oplus K/[F, N]$. Nach Satz 5.36 gilt $Z(\hat{A}) = L/K$ und $[F, L] \leq F' \cap K \leq [F, N]$. Daher ist die Abbildung

$$M(A) = (F' \cap N)/[F, N] \rightarrow (F' \cap L)/[F, L] = M(A/Z), \quad x[F, N] \mapsto x[F, L]$$

injektiv. Insbesondere ist $|M(A)| \leq |M(A/Z)|$. Nach GT-Beispiel-11.38 gilt $|M(A)| = d_1^{k-1} d_2^{k-2} \dots d_{k-1}$. Andererseits existieren $e_i \mid d_i$ mit $M(A/Z) = e_1^{k-1} \dots e_{k-1}$. Aus $|M(G)| \leq |M(A/Z)|$ folgt nun leicht $d_{k-1} < d_k$. \square

Definition 5.40. Gruppen G und H heißen *isoklin*¹², falls es Isomorphismen

$$\varphi: G' \rightarrow H', \quad \psi: G/Z(G) \rightarrow H/Z(H), \quad xZ(G) \mapsto \tilde{x}Z(H)$$

mit $\varphi([x, y]) = [\tilde{x}, \tilde{y}]$ für alle $x, y \in G$ gibt. Ggf. heißt ψ ein *Isoklinismus* und wir schreiben $G \approx H$.

Bemerkung 5.41.

- (i) Die Eigenschaft $\varphi([x, y]) = [\tilde{x}, \tilde{y}]$ hängt nicht von der Wahl der Repräsentanten \tilde{x} ab. Außerdem gilt $\varphi(g)Z(H) = \psi(gZ(G))$ für alle $g \in G'$.
- (ii) Offenbar ist Isoklinismus eine Äquivalenzrelation und isomorphe Gruppen sind isoklin.
- (iii) Die Abbildung $\varphi: G' \rightarrow H'$ ist durch einen Isoklinismus eindeutig bestimmt.
- (iv) Für $G \approx H$ gilt $G' \cong H'$ und

$$G/Z(G)G' \cong (G/Z(G))/(G/Z(G))' \cong (H/Z(H))/(H/Z(H))' \cong H/Z(H)H'.$$

Daher unterscheiden sich $|G|$ und $|H|$ nur durch den sogenannten *Verzweigungsfaktor*

$$Z(G)G'/G' \cong Z(G)/(Z(G) \cap G').$$

Für $x \in G' \cap Z(G)$ gilt $\varphi(x)Z(H) = \psi(xZ(G)) = 1$, d. h. $\varphi(x) \in Z(H)$. Die Einschränkung von φ liefert also einen Isomorphismus $G' \cap Z(G) \cong H' \cap Z(H)$.

- (v) Für $G \approx H$ gilt nach Voraussetzung $\varphi(G') = H'$. Nehmen wir $\varphi(G^{[k]}) = H^{[k]}$ für ein $k \geq 2$ an. Für $y \in G^{[k]}$ gilt $\tilde{y} \in \varphi(y)Z(H) \subseteq H^{[k]}Z(H)$. Für $x \in G$ folgt $\varphi([x, y]) = [\tilde{x}, \tilde{y}] \in H^{[k+1]}$. Dies zeigt $\varphi(G^{[k+1]}) \subseteq H^{[k+1]}$. Aus Symmetriegründen muss Gleichheit gelten. Insbesondere ist $G^{[k]} \cong H^{[k]}$ für alle $k \geq 2$. Außerdem gilt $G/Z_k(G) \cong G/Z_k(H)$ für $k \geq 1$. Insbesondere haben G und H die gleiche Nilpotenzklasse (falls nilpotent) und Auflösbarkeitsstufe (falls auflösbar).
- (vi) Aus $G/Z(G) \cong H/Z(H)$ und $G' \cong H'$ folgt nicht $G \approx H$ (siehe Beispiel 5.48).

Beispiel 5.42.

- (i) Alle abelschen Gruppen sind zueinander isoklin. Für jede abelsche Gruppe A gilt allgemeiner $G \approx G \times A$.

¹²Hall führte den Begriff im englischen Original als *isoclinic* ein und schlug als deutsche Übersetzung *gleich schief* vor.

- (ii) Seien \widehat{G}_1 und \widehat{G}_2 maximale Schur-Erweiterungen von G . Wie im Beweis von Satz 5.27 sei $G = F/N$ und $\widehat{G}_i = F/K_i$ für eine freie Gruppe F . Für $L/[F, N] = Z(F/[F, N])$ ist

$$\psi: \widehat{G}_1/Z(\widehat{G}_1) \cong F/L \cong \widehat{G}_2/Z(\widehat{G}_2), \quad xK_1Z(\widehat{G}_1) \mapsto xK_2Z(\widehat{G}_2)$$

ein kanonischer Isomorphismus. Da auch der Isomorphismus $\widehat{G}'_1 \cong F'/[F, N] \cong \widehat{G}'_2$ kanonisch ist, ist ψ ein Isoklinismus. Umgekehrt ist nicht jede zu \widehat{G}_1 isokline Gruppe (der gleichen Ordnung) eine (maximale) Schur-Erweiterung von G . Zum Beispiel ist Q_8 nach Beispiel 5.26 eine maximale Schur-Erweiterung von sich selbst, aber $Q_8 \approx D_8$.

- (iii) Sei $H \leq G$ mit $G = HZ(G)$. Dann ist $Z(H) = H \cap Z(G)$, $H' = G'$ und die Abbildung $H/Z(H) \rightarrow G/Z(G)$, $hZ(H) \mapsto hZ(G)$ ist ein Isoklinismus. Also gilt $G \approx H$.
- (iv) Sei G endlich. Ist $Z(G) \not\leq \Phi(G)$, so existiert eine maximale Untergruppe $M < G$ mit $G = MZ(G)$. Nach (iii) gilt $G \approx M$. Wiederholt man das Argument mit M , so erhält man schließlich eine Untergruppe $H \leq G$ mit $G \approx H$ und $Z(H) \leq \Phi(H)$.
- (v) Sei $N \trianglelefteq G$ mit $N \cap G' = 1$. Wegen $[G, N] \leq N \cap G' = 1$ ist $N \leq Z(G)$. Offenbar ist $G' \rightarrow G'N/N \cong (G/N)'$, $x \mapsto xN$ ein Isomorphismus. Für $xN \in Z(G/N)$ gilt $[x, G] \leq G' \cap N = 1$ und $x \in Z(G)$. Dies zeigt $Z(G/N) = Z(G)/N$. Daher ist $G/Z(G) \cong (G/N)/Z(G/N)$, $xZ(G) \rightarrow xNZ(G/N)$ ein Isoklinismus. Es folgt $G \approx G/N$.
- (vi) Ist H eine maximale Schur-Erweiterung von $G/Z(G)$, so gilt $H/Z(H) \cong G/Z(G)$ nach Satz 5.36. Im Allgemeinen sind G und H aber nicht isoklin (betrachte $G = A_4$ und $H = \text{SL}(2, 3)$). Der folgende Satz zeigt, dass G dennoch zu einer Schur-Erweiterung von $G/Z(G)$ isoklin ist.

Definition 5.43. Man nennt G eine *Stammgruppe*, falls $Z(G) \leq G'$.

Satz 5.44 (HALL). *Jede Gruppe ist zu einer Stammgruppe isoklin.*

Beweis. Sei $\{g_i : i \in I\}$ ein Erzeugendensystem von G und $A = \bigoplus_{i \in I} \langle a_i \rangle \cong \bigoplus_{i \in I} C_\infty$. Wir betrachten

$$H := \langle (g_i, a_i) : i \in I \rangle \leq G \times A.$$

Wegen $1 \times A \leq Z(G \times A)$ ist $HA = G \times A$ und $G \approx G \times A \approx H$ nach Beispiel 5.42. Wegen

$$[(g_i, a_i), (g_j, a_j)] = ([g_i, g_j], 1)$$

ist $H' = G' \times 1$. In H/H' erzeugen die Nebenklassen von (g_i, a_i) eine freie abelsche Gruppe, d. h. $H/H' \cong A$. Daher ist auch $\overline{Z} := Z(H)/(Z(H) \cap H') \cong Z(H)H'/H'$ eine freie abelsche Gruppe.¹³ Nach der universellen Eigenschaft von freien (abelschen) Gruppen existiert ein Homomorphismus $\alpha: \overline{Z} \rightarrow Z(H)$ mit $Z(H) = \alpha(\overline{Z}) \oplus (Z(H) \cap H')$. Für $K := \alpha(\overline{Z})$ gilt $H \approx H/K$, denn $K \cap H' = 1$ (Beispiel 5.42). Wegen

$$Z(H/K) = Z(H)/K = (Z(H) \cap H')K/K \leq H'K/K = (H/K)'$$

ist H/K eine zu G isokline Stammgruppe. □

Bemerkung 5.45. Die Stammgruppen in einer Äquivalenzklasse isokliner Gruppen sind genau die Vertreter minimaler Ordnung, denn der Verzweigungsfaktor ist trivial.

Definition 5.46. Für $n \in \mathbb{N}$ sei $k_n(G)$ die Anzahl der Konjugationsklassen von G der Länge n .

¹³Siehe Anhang im Algebra-Skript

Satz 5.47. Für endliche Gruppen $G \approx H$ und $n \in \mathbb{N}$ gilt $k_n(G)|Z(H)| = k_n(H)|Z(G)|$.

Beweis. Sei $\psi: G/Z(G) \rightarrow H/Z(H)$, $xZ(G) \mapsto \tilde{x}Z(H)$ ein Isoklinismus. Für $g, x \in G$ gilt

$$g \in C_G(x) \iff [g, x] = 1 \iff \varphi([g, x]) = 1 \iff [\tilde{g}, \tilde{x}] = 1 \iff \tilde{g} \in C_H(\tilde{x}).$$

Dies zeigt

$$|{}^Gx| = |G : C_G(x)| = \frac{|G/Z(G)|}{|C_G(x)/Z(G)|} = \frac{|H/Z(H)|}{|C_H(\tilde{x})/Z(H)|} = |H : C_H(\tilde{x})| = |{}^H\tilde{x}|.$$

Alle Elemente in $xZ(G)$ liegen in Konjugationsklassen der gleichen Länge. Für $n \in \mathbb{N}$ folgt

$$|Z(H)|k_n(G)n = |Z(H)| \left| \bigcup_{\substack{x \in G \\ |{}^Gx|=n}} xZ(G) \right| = |Z(H)| \sum_{\substack{xZ(G) \in G/Z(G) \\ |{}^Gx|=n}} |Z(G)| = |Z(G)| \sum_{\substack{\tilde{x}Z(H) \in H/Z(H) \\ |{}^H\tilde{x}|=n}} |Z(H)| = |Z(G)|k_n(H)n. \quad \square$$

Beispiel 5.48. Der folgende Code liefert nicht-isokline Gruppen G und H der Ordnung 64 mit $G' \cong H'$ und $G/Z(G) \cong H/Z(H)$:

```
G:=SmallGroup(64,128);;
H:=SmallGroup(64,149);;
IdGroup(DerivedSubgroup(G))=IdGroup(DerivedSubgroup(H));
IdGroup(G/Center(G))=IdGroup(H/Center(H));
Number(ConjugacyClasses(G),K->Size(K)=2)=Number(ConjugacyClasses(H),K->Size(K)=2);
```

6 Erweiterungen der alternierenden Gruppen

Bemerkung 6.1. Aus der Gruppentheorie wissen wir, dass die alternierenden Gruppen A_n für $n \geq 5$ einfach sind. Wir bestimmen in diesem Kapitel Erweiterungen von A_n und mit A_n .

Lemma 6.2. Für $n \geq 4$ gilt $C_{S_n}(A_n) = 1$. Insbesondere ist $Z(S_n) = Z(A_n) = 1$.

Beweis. Sei $\sigma \in C_{S_n}(A_n)$ und $\tau := (a, b, c) \in A_n$ ein 3-Zyklus. Aus $\sigma\tau = \tau\sigma$ folgt ${}^\sigma\{a, b, c\} = \{a, b, c\}$. Nun ist $\{a\}$ der Durchschnitt aller 3-elementigen Mengen $\Delta \subseteq \{1, \dots, n\}$, die a enthalten (beachte: $n \geq 4$). Dies zeigt $\sigma(a) = a$ für $a = 1, \dots, n$. \square

Bemerkung 6.3. Zu jedem Homomorphismus $\omega: H \rightarrow \text{Out}(A_n)$ ($n \geq 4$) gibt es nach Folgerung 4.28 also genau eine Erweiterung von A_n mit H zur Paarung ω . Wir müssen daher $\text{Out}(A_n)$ bestimmen.

Lemma 6.4 (GT-Aufgabe 37). Für $n \geq 3$ ist $A_n = \langle (1, 2, 3), \dots, (1, 2, n) \rangle$.

Beweis. Wir argumentieren durch Induktion nach n . Der Fall $n = 3$ ist klar. Sei nun $n \geq 4$. Es genügt zu zeigen, dass $A_n = \langle A_{n-1}, (1, 2, n) \rangle =: H$ gilt. Sei indirekt $\sigma \in A_n \setminus H$. Dann existiert ein $k \neq n$ mit ${}^\sigma k = n$. Wähle $\tau \in A_{n-1}$ mit ${}^\tau 1 = k$. Dann ist $\sigma\tau(1, 2, n) \in A_{n-1}$ und wir erhalten den Widerspruch $\sigma \in H$. \square

Lemma 6.5. Sei Ω eine Menge und $G \leq \text{Sym}(\Omega)$ mit genau einem minimalen Normalteiler. Dann existiert eine Bahn $\Delta \subseteq \Omega$, sodass G treu auf Δ operiert.

Beweis. Seien $\Delta_1, \dots, \Delta_s$ die Bahnen von G . Sei $N \trianglelefteq G$ der einzige minimale Normalteiler und $x \in N \setminus \{1\}$. Dann existiert ein $1 \leq i \leq s$, sodass x nicht-trivial auf Δ_i operiert. Für den Kern K der eingeschränkten Operation $G \rightarrow \text{Sym}(\Delta_i)$ gilt also $K \cap N = 1$. Dies zeigt $K = 1$ und G operiert treu auf Δ_i . \square

Bemerkung 6.6.

- (i) Nach GT-Satz 6.21 und GT-Satz 6.39 gilt die Voraussetzung von Lemma 6.5 für alle symmetrischen und alternierenden Gruppen.
- (ii) Für einen k -Zyklus $(a_1, \dots, a_k) \in S_n$ und eine beliebige Permutation $\sigma \in S_n$ gilt

$$\sigma(a_1, \dots, a_k)\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k)).$$

Dies zeigt, dass alle k -Zyklen in S_n konjugiert sind. Durch Zerlegen in disjunkte Zyklen erhält man, dass zwei beliebige Permutationen $\sigma, \tau \in S_n$ genau dann konjugiert sind, wenn sie den gleichen Zyklentyp haben. Für $\sigma \in A_n$ ist $^{S_n}\sigma \subseteq A_n$ eine Vereinigung von Konjugationsklassen von A_n . Wegen

$$|A_n : C_{A_n}(\sigma)| = |A_n : A_n \cap C_{S_n}(\sigma)| = |A_n C_{S_n}(\sigma) : C_{S_n}(\sigma)|$$

gilt $^{S_n}\sigma = ^{A_n}\sigma$ genau dann, wenn $C_{S_n}(\sigma) \not\subseteq A_n$. Sei $\sigma = \sigma_1 \dots \sigma_l$ mit disjunkten Zyklen σ_i der Länge λ_i (inklusive Einerzyklen). Ist λ_i gerade, so ist $\sigma_i \in C_{S_n}(\sigma) \setminus A_n$. Nehmen wir nun an, dass $\lambda_1, \dots, \lambda_l$ ungerade sind. Angenommen es existieren $i \neq j$ mit $\lambda_i = \lambda_j$. Für $\sigma_i = (a_1, \dots, a_{\lambda_i})$ und $\sigma_j = (b_1, \dots, b_{\lambda_i})$ ist $(a_1, b_1) \dots (a_{\lambda_i}, b_{\lambda_i}) \in C_{S_n}(\sigma) \setminus A_n$.

Im Fall $^{S_n}\sigma \neq ^{A_n}\sigma$ müssen $\lambda_1, \dots, \lambda_l$ also ungerade und paarweise verschieden sein. Man kann zeigen, dass die Umkehrung ebenfalls gilt.

Lemma 6.7. Sei $n \geq 4$ und $A_{n-1} \cong H \leq A_n$. Dann ist $H = \text{Alt}(\{1, \dots, n\} \setminus \{i\})$ für ein $i \in \{1, \dots, n\}$ oder $n = 6$.

Beweis. O. B. d. A. sei $n \geq 5$. Nach Lemma 6.5 operiert H treu auf einer Bahn $\Delta \subseteq \{1, \dots, n\}$. Wegen $|H| = (n-1)!/2$ ist $|\Delta| \geq n-1$. Wir können also annehmen, dass H transitiv auf $\{1, \dots, n\}$ operiert. Insbesondere ist $n \mid |H| \mid (n-1)!$. Daher dürfen wir $n \geq 8$ voraussetzen.

Sei $f: A_{n-1} \rightarrow H$ ein Isomorphismus und sei $\sigma \in A_{n-1}$ ein 3-Zyklus. Offenbar ist A_{n-4} zu einer Untergruppe von $C_{A_{n-1}}(\sigma)$ isomorph. Insbesondere besitzt auch $C_H(f(\sigma))$ eine Untergruppe $C \cong A_{n-4}$. Sei $f(\sigma)$ das disjunkte Produkt von k vielen 3-Zyklen. Offenbar permutiert C die Bahnen von $f(\sigma)$ (einschließlich trivialer Bahnen). Der Kern dieser Operation ist eine 3-Gruppe und damit trivial. Es gibt also einen Monomorphismus $F: C \rightarrow S_{n-2k}$. Wegen $|C| = (n-4)!/2$ folgt $k \leq 2$. Im Fall $k = 2$ ist F transitiv und man erhält den Widerspruch $n = 3k = 6$. Also ist auch $f(\sigma)$ ein 3-Zyklus.

Sei $f((1, 2, 3)) = (\alpha, \beta, \gamma)$ und $f((1, 2, 4)) = (\delta, \epsilon, \varphi)$. Im Fall $\{\alpha, \beta, \gamma\} \cap \{\delta, \epsilon, \varphi\} = \emptyset$ wäre

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

abelsch. Im Fall $|\{\alpha, \beta, \gamma\} \cap \{\delta, \epsilon, \varphi\}| = 1$ würde $\langle f((1, 2, 3)), f((1, 2, 4)) \rangle$ transitiv auf der 5-elementigen Menge $\{\alpha, \beta, \gamma\} \cup \{\delta, \epsilon, \varphi\}$ operieren. Also ist $|\{\alpha, \beta, \gamma\} \cap \{\delta, \epsilon, \varphi\}| = 2$ und $\langle f((1, 2, 3)), f((1, 2, 4)) \rangle$ kann nur vier Ziffern bewegen. Durch Induktion nach k sieht man, dass $\langle f((1, 2, 3)), \dots, f((1, 2, k)) \rangle$ höchstens k Ziffern bewegen kann. Also ist $H = f(A_{n-1}) = \langle f((1, 2, 3)), \dots, f((1, 2, n-1)) \rangle$ (Lemma 6.4) intransitiv. Dies war aber bereits ausgeschlossen. \square

Satz 6.8 (HÖLDER). *Es gilt $\text{Aut}(A_6) \cong S_6 \rtimes C_2$ und $\text{Aut}(A_n) \cong S_n$ für $4 \leq n \neq 6$.*

Beweis. Offenbar operiert S_n durch Konjugation auf A_n mit Kern $C_{S_n}(A_n) = 1$ (Lemma 6.2). Dies liefert einen Monomorphismus $\Psi: S_n \rightarrow \text{Aut}(A_n)$. Sei $H_i := \text{Alt}(\{1, \dots, n\} \setminus \{i\})$ für $i = 1, \dots, n$. Sei zunächst $n \neq 6$. Nach Lemma 6.7 operiert dann $\text{Aut}(A_n)$ auf $\{H_1, \dots, H_n\}$. Dies liefert einen Homomorphismus $\Gamma: \text{Aut}(A_n) \rightarrow S_n$. Sei $f \in \text{Ker}(\Gamma)$ und $\sigma \in A_n$. Dann ist

$$H_{f(\sigma)_i} = f(\sigma)H_i f(\sigma)^{-1} = f(\sigma)f(H_i)f(\sigma)^{-1} = f(\sigma H_i \sigma^{-1}) = f(H_{\sigma_i}) = H_{\sigma_i}$$

und $f(\sigma) = \sigma$. Also ist Γ injektiv. Damit sind Ψ und Γ sogar Isomorphismen. Sei nun $n = 6$.

Schritt 1: $\Psi(S_6) < \text{Aut}(A_6)$.

Offenbar operiert A_5 treu und transitiv auf $\text{Syl}_5(A_5)$ durch Konjugation. Dies liefert einen Monomorphismus $f: A_5 \rightarrow \text{Sym}(\text{Syl}_5(A_5)) \cong S_6$. Im Fall $f(A_5) \not\leq A_6$ wäre $1 \neq f(A_5) \cap A_6 < f(A_5)$ im Widerspruch zur Einfachheit von $f(A_5) \cong A_5$. Also ist $f(A_5) \leq A_6$. Da f transitiv ist, gilt $f(A_5) \neq H_i$ für $i = 1, \dots, 6$. Die Operation von A_6 auf den Nebenklassen $A_6/f(A_5)$ liefert einen Monomorphismus $\varphi: A_6 \rightarrow S_6$. Wie eben ist $\varphi(A_6) = A_6$, d. h. $\varphi \in \text{Aut}(A_6)$. Da $f(A_5)$ der Stabilisator der trivialen Nebenklasse ist, muss $\varphi(f(A_5)) = H_i$ für ein $i \in \{1, \dots, 6\}$ gelten. Insbesondere ist $\varphi \notin \Psi(S_6)$.

Schritt 2: $|\text{Out}(A_6)| = 4$.

Seien $\varphi, \psi \in \text{Aut}(A_6) \setminus \Psi(S_6)$. Offenbar bildet jeder Automorphismus Konjugationsklassen auf Konjugationsklassen ab. Nach Bemerkung 6.6 ist die Menge der 3-Zyklen eine Konjugationsklasse C von A_6 . Gilt $\varphi(C) = C$, so sieht man wie im Beweis von Lemma 6.7, dass φ die Untergruppen H_i permutiert. Dann wäre aber $\varphi \in \Psi(S_6)$. Also muss $\varphi(C) = \psi(C)$ die Konjugationsklasse der Elemente vom Zyklentyp $(3, 3)$ sein, denn dies sind die einzigen weiteren Elemente der Ordnung 3. Es folgt $(\varphi\psi)(C) = C$ und $\varphi\psi \in \Psi(S_6)$. Dies impliziert die Behauptung.

Schritt 3: $\text{Aut}(A_6) \cong S_6 \rtimes C_2$.

Als Untergruppe vom Index 2 ist $\Psi(S_6) < \text{Aut}(A_6)$. Es genügt also ein Element $\varphi \in \text{Aut}(A_6) \setminus \Psi(S_6)$ der Ordnung 2 zu finden. Sei zunächst $\varphi \in \text{Aut}(A_6) \setminus \Psi(S_6)$ beliebig und sei $x := (1, 2, 3, 4, 5) \in A_6$. Dann ist auch $\varphi(x)$ ein 5-Zyklus und daher in S_6 zu x konjugiert (Bemerkung 6.6). Ersetzt man also φ durch ein geeignetes Element aus der Nebenklasse $\varphi\Psi(S_6)$, so kann man $\varphi(x) = x$ annehmen. Also existiert ein $y \in C_{S_6}(x)$ mit $\varphi^2 = \Psi(y)$. Da S_6 genau $6 \cdot 4!$ Zyklen der Länge 5 besitzt, ist $|C_{S_6}(x)| \leq 5$ und damit $y \in C_{S_6}(x) = \langle x \rangle$. Dies zeigt $|\langle \varphi \rangle| \in \{2, 10\}$. Also hat $\varphi^5 \in \text{Aut}(A_6) \setminus \Psi(S_6)$ die Ordnung 2. \square

Satz 6.9. *Für $4 \leq n \neq 6$ zerfällt jede Erweiterung mit A_n .*

Beweis. Nach Satz 6.8 besitzt $\text{Inn}(A_n) \cong A_n$ ein Komplement in $\text{Aut}(A_n) \cong S_n$. Die Behauptung folgt aus Lemma 6.2 und Folgerung 4.28. \square

Bemerkung 6.10. Nach Satz 6.8 ist $\text{Out}(A_6) \cong C_2^2$. Der nächste Satz zeigt, dass Satz 6.9 für $n = 6$ falsch ist.

Satz 6.11. *Die Erweiterung $\text{Aut}(A_6)$ von $\text{Inn}(A_6) \cong A_6$ zerfällt nicht.*

Beweis. Angenommen $A \leq \text{Aut}(A_6)$ ist ein Komplement von $\text{Inn}(A_6)$. Sei $\Psi(S_6) \leq \text{Aut}(A_6)$ wie im Beweis von Satz 6.8. Dann gilt $|\Psi(S_6) \cap A| = 2$. Sei $\sigma \in S_6$ eine Involution mit $\alpha := \Psi(\sigma) \in A$. Wegen $\text{Inn}(A_6) \cap A = 1$ hat σ Zyklentyp (2) oder $(2, 2, 2)$. O. B. d. A. sei $\sigma \in \{(1, 2), (1, 2)(3, 4)(5, 6)\}$. Sei $\beta \in A \setminus \Psi(S_6)$. Wie im Beweis von Satz 6.8 vertauscht β die 3-Zyklen mit den Permutationen vom Zyklentyp $(3, 3)$. Wegen $|A| = 4$ ist A abelsch.

Fall 1: $\sigma = (1, 2)$.

Es gilt

$$\beta((3, 4, 5)) = (\beta\alpha)((3, 4, 5)) = (\alpha\beta)((3, 4, 5)) = (1, 2)\beta((3, 4, 5))(1, 2),$$

aber $(1, 2)$ kann keine Permutation vom Zyklentyp $(3, 3)$ zentralisieren. Widerspruch.

Fall 2: $\sigma = (1, 2)(3, 4)(5, 6)$.

Offenbar wird $(1, 3, 5)(2, 4, 6)$ von σ zentralisiert. Die gleiche Rechnung wie in Fall 1 mit $(1, 3, 5)(2, 4, 6)$ anstelle von $(3, 4, 5)$ zeigt, dass σ einen 3-Zyklus zentralisiert. Dies ist ebenfalls unmöglich. \square

Bemerkung 6.12. Das außergewöhnliche Verhalten von $\text{Aut}(A_6)$ lässt sich durch den (ebenfalls außergewöhnlichen) Isomorphismus $A_6 \cong \text{PSL}(2, 9)$ erklären (Aufgabe 18).

```
G:=AlternatingGroup(6);;
A:=AutomorphismGroup(G);;
sub:=SubgroupsOfIndexTwo(A);;
List(sub, IdGroup);
IdGroup(SymmetricGroup(6));
IdGroup(PGL(2, 9));
IdGroup(MathieuGroup(10));
```

Lemma 6.13. Für $n \in \mathbb{N}$ gilt $|M(S_n)| \leq 2$.

Beweis. Wir benutzen die Präsentation

$$S_n = \langle x_1, \dots, x_{n-1} \mid x_i^2 = (x_i x_{i+1})^3 = [x_i, x_j] = 1 \text{ für } i < j - 1 \rangle$$

aus Satz 2.18. Seien F und N wie in Satz 5.24. Sei $\overline{F} := F/[F, N]$ und $\overline{x_i} := x_i[F, N] \in \overline{F}$ für $i = 1, \dots, n-1$. Seien $a_i := \overline{x_i}^2$, $b_i := (\overline{x_i x_{i+1}})^3$ und $c_{ij} := [\overline{x_i}, \overline{x_j}]$ Elemente in \overline{N} . Wegen $\overline{N} \leq Z(\overline{F})$ sind dies Erzeuger von \overline{N} (man braucht nicht den normalen Abschluss). Da man x_i durch die Transposition $(i, i+1)$ realisieren kann, existieren $g \in F$, $y, z \in N$ mit $\overline{g x_i g^{-1}} = \overline{x_1 y}$ und $\overline{g x_j g^{-1}} = \overline{x_3 y}$ (beachte: $i < j - 1$). Wegen $\overline{N} \leq Z(\overline{F})$ folgt

$$c_{ij} = \overline{g x_i g^{-1}} \overline{g x_j g^{-1}}^{-1} = [\overline{g x_i g^{-1}}, \overline{g x_j g^{-1}}] = [\overline{x_1 y}, \overline{x_3 y}] = [\overline{x_1}, \overline{x_3}] = c_{13}.$$

Außerdem gilt

$$c_{13}^2 a_3 = (c_{13} \overline{x_3})^2 = (\overline{x_1 x_3 x_1^{-1}})^2 = a_3$$

und somit $c_{13}^2 = 1$. Eine ähnliche Rechnung zeigt

$$b_i^2 a_i^{-1} a_{i+1}^{-2} = (b_i (\overline{x_{i+1} x_i x_{i+1}})^{-1})^2 = (\overline{x_i x_{i+1} x_i})^2 = a_i^2 a_{i+1}$$

und es folgt $b_i^2 = (a_i a_{i+1})^3$. Wir setzen $d_1 := a_1$ und $d_{i+1} := b_i (a_i a_{i+1})^{-1}$. Dann gilt $d_{i+1}^2 = a_i a_{i+1}$ und

$$\overline{N} = \langle d_1, \dots, d_{n-1}, c_{13} \rangle$$

mit $c_{13}^2 = 1$. Nach Satz 5.24 hat der freie Teil von \overline{N} Rang $n-1$. Daher müssen d_1, \dots, d_{n-1} unendliche Ordnung haben. Der Torsionsteil ist somit $\langle c_{13} \rangle$. Die Behauptung folgt nun aus Satz 5.24. \square

Lemma 6.14. Für $n \in \mathbb{N} \setminus \{6, 7\}$ gilt $|M(A_n)| \leq 2$ und $|M(A_6)|, |M(A_7)| \leq 6$.

Beweis. Die Fälle $n \leq 7$ können mit GAP oder GT-Folgerung 11.19 behandelt werden. Sei also $n \geq 8$ und

$$A_n \cong \langle x_1, \dots, x_{n-2} \mid x_1^3 = x_2^2 = \dots = x_{n-2}^2 = (x_i x_{i+1})^3 = (x_i x_j)^2 = 1 \text{ für } |j - i| > 1 \rangle$$

wie in Satz 2.19. Wir benutzen die Bezeichnungen aus Lemma 6.13 mit $a_1 := \overline{x_1^3}$, $a_i := \overline{x_i^2}$ ($i \geq 2$), $b_i := (\overline{x_i x_{i+1}})^3$, $c_i := (\overline{x_1 x_i})^2$ ($i \geq 3$) und $c_{ij} := [\overline{x_i}, \overline{x_j}]$ für $2 \leq i < j - 1$. Wie in Lemma 6.13 folgt dann $c := c_{24} = c_{ij}$, $c^2 = 1$ und $b_i^2 = (a_i a_{i+1})^3$ für $i \geq 2$. Für $z_{i+1} := b_i (a_i a_{i+1})^{-1}$ gilt also $\langle b_i, a_i a_{i+1} \rangle = \langle z_{i+1} \rangle$ für $i = 2, \dots, n - 3$. Für $i \geq 3$ ist

$$a_1 = (\overline{x_i^{-1} x_1 x_i})^3 = (a_i^{-1} \overline{x_1^{-1}} c_i)^3 = a_1^{-1} (a_i^{-1} c_i)^3$$

und $\boxed{(c_i a_i^{-1})^3 = a_1^2}$. Wir setzen $z_1 := a_1 (c_3 a_3^{-1})^{-1}$ und erhalten $\langle a_1, c_3 a_3^{-1} \rangle = \langle z_1 \rangle$.

Aus $c_4 = \overline{x_1^{-1}} (\overline{x_1 x_4})^2 \overline{x_1} = (\overline{x_4 x_1})^2$ und $c = a_2 a_4 [\overline{x_2^{-1}}, \overline{x_4^{-1}}] a_2^{-1} a_4^{-1} = [\overline{x_2^{-1}}, \overline{x_4^{-1}}]$ folgt

$$\overline{x_4 x_1 x_2 x_4^{-1}} = c_4 \overline{x_1^{-1} x_4^{-1} x_2 x_4 a_4^{-1}} = c_4 \overline{x_1^{-1} x_2 c a_4^{-1}} = \overline{x_2 (x_1 x_2)^{-1} x_2^{-1} a_2 c_4 c a_4^{-1}}.$$

Die dritte Potenz ergibt

$$b_1 = b_1^{-1} a_2^3 c_4^3 c a_4^{-3}.$$

Wegen $(c_4 a_4^{-1})^3 = a_1^2$ erhält man $b_1^2 = a_1^2 a_2^3 c$. Mit $z_2 := b_1 a_1^{-1} a_2^{-1} c$ gilt $z_2^2 = a_2 c$ und $z_2^3 = a_1^{-1} b_1$.

Für $i \geq 5$ gilt

$$\overline{x_3 x_1 x_i x_3^{-1}} = \overline{c_3 x_1^{-1} x_3^{-1} x_i x_3 a_3^{-1}} = \overline{c_3 x_1^{-1} x_i c_{3i} a_3^{-1}}$$

und $c_i = (c_3 a_3^{-1})^2 (\overline{x_1^{-1} x_i})^2$ nach quadrieren. Wegen $\overline{x_1^{-1} x_i} = a_i \overline{x_i^{-1}} (\overline{x_1 x_i})^{-1} \overline{x_i}$ folgt $(c_i a_i^{-1})^2 = (c_3 a_3^{-1})^2$. Andererseits gilt auch $(c_i a_i^{-1})^3 = a_1^2 = (c_3 a_3^{-1})^3$. Dies zeigt $c_i a_i^{-1} = c_3 a_3^{-1}$ für $i \geq 5$. Die gleiche Rechnung mit Index 4 anstatt 3 liefert $c_4 a_4^{-1} = c_6 a_6^{-1}$. Daher ist $\langle z_1 \rangle = \langle a_1, c_i a_i^{-1} \rangle$ für $i = 3, \dots, n - 2$.

Insgesamt gilt

$$\overline{N} = \langle a_i, b_i, c_i, c \rangle = \langle z_1, \dots, z_{n-2}, c \rangle$$

und es folgt $|M(A_n)| \leq 2$. □

Satz 6.15. *Es gilt*

$$M(S_n) = \begin{cases} 1 & \text{falls } n \leq 3, \\ C_2 & \text{falls } n \geq 4. \end{cases}$$

Beweis. O.B.d.A. sei $n \geq 4$. Nach Lemma 6.13 genügt es eine echte Schur-Erweiterung von S_n zu konstruieren. Sei

$$\widehat{S}_n := \langle x_1, \dots, x_{n-1}, z \mid z^2 = 1, x_i^2 = (x_i x_{i+1})^3 = [x_i, x_j] = z \text{ für } i < j - 1 \rangle.$$

Nach von-Dyck gibt es einen Epimorphismus $\widehat{S}_n \rightarrow S_n$ mit Kern $\langle z \rangle$. Wegen $x_i^2 = [x_i, x_j] = z$ ist $z \in Z(\widehat{S}_n) \cap \widehat{S}_n'$. Allerdings könnte $z = 1$ gelten. Wir definieren Matrizen in $\text{GL}(2^n, \mathbb{C})$ als iterierte Kronecker-Produkte von 2×2 -Matrizen:

$$A := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad B := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad C := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$M_{2k-1} := C^{\otimes(n-k)} \otimes A \otimes 1_2^{\otimes(k-1)}, \quad M_{2k} := C^{\otimes(n-k)} \otimes B \otimes 1_2^{\otimes(k-1)}$$

für $k = 1, \dots, n$. Sei zusätzlich $M_0 := 0_{2^n}$. Wegen $A^2 = B^2 = -C^2 = [A, B] = [A, C] = [B, C] = -1_2$ gilt $M_k^2 = [M_k, M_l] = -I := -1_{2^n}$ für $k \neq l$. Wir setzen nun

$$X_k := \frac{1}{\sqrt{2k}}(\sqrt{k+1}M_k - \sqrt{k-1}M_{k-1})$$

für $k = 1, \dots, n-1$. Es folgt

$$\begin{aligned} X_k^2 &= -\frac{1}{2k}((k+1)I + (k-1)I) = -I \quad (\implies X_k \in \text{GL}(2^n, \mathbb{C})), \\ X_k X_l &= -X_l X_k \quad (k < l-1), \\ X_{k+1} X_k &= \frac{1}{2\sqrt{k^2+k}} \left(\sqrt{(k+2)(k+1)} M_{k+1} M_k - \sqrt{(k+2)(k-1)} M_{k+1} M_{k-1} \right. \\ &\quad \left. + \sqrt{k^2+k} I + \sqrt{k(k-1)} M_k M_{k-1} \right) \\ &= I - X_k X_{k+1}, \\ X_k X_{k+1} X_k &= X_k (I - X_k X_{k+1}) = X_k + X_{k+1} = (I - X_k X_{k+1}) X_{k+1} = X_{k+1} X_k X_{k+1} \\ (X_k X_{k+1})^3 &= X_k X_{k+1} X_k X_{k+1} X_k X_{k+1} = (-I)^3 = -I. \end{aligned}$$

Nach von-Dyck existiert ein Epimorphismus $\Gamma: \widehat{S}_n \rightarrow \langle X_1, \dots, X_{n-1} \rangle$ mit $\Gamma(z) = -I$. Also ist $z \neq 1$ in \widehat{S}_n . \square

Bemerkung 6.16. Nach Satz 5.19 besitzt S_n höchstens $\text{ggT}(|S_n/S'_n|, |M(S_n)|) = 2$ maximale Schur-Erweiterungen. Neben \widehat{S}_n gibt es noch die Schur-Erweiterung

$$\widetilde{S}_n := \langle x_1, \dots, x_{n-1}, z \mid z^2 = 1, x_i^2 = (x_i x_{i+1})^3 = 1, [x_i, x_j] = z \text{ für } i < j-1 \rangle.$$

Man zeigt leicht $\widetilde{S}_4 \cong \text{GL}(2, 3)$. Sei allgemeiner q eine ungerade Primzahlpotenz, $\mathbb{F}_q^\times = \langle \zeta \rangle$ und $x := \begin{pmatrix} 0 & \zeta \\ -1 & 0 \end{pmatrix} \in \text{GL}(2, q)$. Dann induziert x durch Konjugation einen äußeren Automorphismus α von $\text{SL}(2, q)$ der Ordnung 2. Es gilt $\text{SL}(2, 5) \rtimes \langle \alpha \rangle \cong \widetilde{S}_5$. Durch eine ähnliche Konstruktion gelangt man zu $\widetilde{S}_6 \cong \text{SL}(2, 9) \rtimes C_2$ (vgl. Aufgabe 18). Sei nun $\zeta \in \mathbb{F}_{q^2}^\times$ der Ordnung $2(q-1)$ und $x := \text{diag}(\zeta, \zeta^{-1}) \in \text{SL}(2, q^2)$. Dann ist $K(q) := \text{SL}(2, q)\langle x \rangle \leq \text{SL}(2, q^2)$ eine nicht-zerfallende Erweiterung mit $K(3) \cong \widehat{S}_4$ und $K(5) \cong \widehat{S}_5$ (ohne Beweis). Ein äußerer Automorphismus von S_6 liefert einen Isomorphismus $\widehat{S}_6 \cong \widetilde{S}_6$. Für $n \neq 6$ gilt hingegen $\widehat{S}_n \not\cong \widetilde{S}_n$ (Aufgabe 21 und Bemerkung 5.22). Für größere n sind die Schur-Erweiterungen von S_n keine „bekannten“ Gruppen.

```
S1:=SchurCoverOfSymmetricGroup(5,3,1); # $\widehat{S}_5$  als Matrixgruppe über  $\mathbb{F}_3$ 
S2:=SchurCoverOfSymmetricGroup(5,3,-1); # $\widetilde{S}_5$ 
IdGroup(S1); IdGroup(S2);
IsomorphismGroups(SchurCoverOfSymmetricGroup(4,3,-1),GL(2,3));
```

Satz 6.17. Es gilt

$$M(A_n) = \begin{cases} C_6 & \text{falls } n \in \{6, 7\}, \\ C_2 & \text{falls } n = 4, 5, 8, 9, \dots \end{cases}$$

Beweis. Man prüft leicht, dass $\text{SL}(2, 3)$ eine Schur-Erweiterung von A_4 ist (vgl. Aufgabe 15). Daher gilt $M(A_4) \cong C_2$. Sei nun $n \geq 5$, $\widehat{A}_n := \widehat{S}'_n$ und $Z := Z(\widehat{S}_n) \leq Z(\widehat{A}_n)$. Dann ist $\widehat{A}_n/Z \cong (\widehat{S}_n/Z)' \cong S'_n \cong A_n$ und $\widehat{A}'_n Z/Z = (\widehat{A}_n/Z)' \cong A'_n \cong A_n$. Es folgt $|\widehat{S}_n/\widehat{A}'_n| = |\widehat{S}_n/\widehat{A}_n| |\widehat{A}_n/\widehat{A}'_n| \leq 4$ und $Z \leq \widehat{S}'_n \leq \widehat{A}'_n$. Also ist \widehat{A}_n eine Schur-Erweiterung von A_n und $2 \mid |M(A_n)|$ für $n \geq 5$. Für $n \notin \{6, 7\}$ ist \widehat{A}_n die universelle Schur-Erweiterung von A_n nach Bemerkung 5.22.

Es genügt daher Schur-Erweiterungen \widehat{A}_6 und \widehat{A}_7 mit $Z(\widehat{A}_6) \cong Z(\widehat{A}_7) \cong C_3$ zu konstruieren. Wir erzeugen \widehat{A}_6 durch monomiale Matrizen in $\text{GL}(6, 4)$. Sei $\mathbb{F}_4^\times = \langle \zeta \rangle$, $\bar{\zeta} := \zeta^{-1}$ und $(a_1, \dots, a_6; \sigma) := (a_i \delta_{i\sigma(j)})_{ij} \in \text{GL}(6, 4)$ für $a_1, \dots, a_6 \in \mathbb{F}_4$ und $\sigma \in S_6$. Wir definieren

$$\begin{aligned} x_1 &:= (\bar{\zeta}, 1, \zeta, 1, \zeta, \bar{\zeta}; (145)(263)), \\ x_2 &:= (1, 1, 1, 1, \bar{\zeta}, \zeta; (13)(56)), \\ x_3 &:= (1, \zeta, \bar{\zeta}, \zeta, \bar{\zeta}, 1; (23)(45)), \\ x_4 &:= (\bar{\zeta}, 1, \zeta, 1, \zeta, \bar{\zeta}; (15)(36)). \end{aligned}$$

Sei $G := \langle x_1, x_2, x_3, x_4 \rangle$ (man beachte, dass die angegebenen Permutationen eine transitive A_5 erzeugen). Eine Rechnung zeigt

$$x_1^3 = x_2^2 = x_3^2 = x_4^2 = (x_1 x_2)^3 = (x_2 x_3)^3 = (x_3 x_4)^3 = (x_1 x_4)^2 = (x_2 x_4)^2 = 1$$

und $z := (x_1 x_3)^2 = \zeta 1_6 \in Z(G)$. Außerdem ist $z = x_1 x_3 x_1 x_3 = x_1 x_3 x_4 x_1^{-1} x_4 x_3 = [x_1, x_3 x_4] \in G'$. Nach Moore ist G eine Schur-Erweiterung von A_6 mit $Z(G) = \langle z \rangle \cong C_3$. Wir ergänzen nun

$$x_5 := \begin{pmatrix} 1 & \bar{\zeta} & 1 & \bar{\zeta} & 1 & . \\ \zeta & 1 & \zeta & . & \zeta & 1 \\ 1 & \bar{\zeta} & 1 & \bar{\zeta} & . & \bar{\zeta} \\ \zeta & . & \zeta & 1 & \zeta & 1 \\ 1 & \bar{\zeta} & . & \bar{\zeta} & 1 & \bar{\zeta} \\ . & 1 & \zeta & 1 & \zeta & 1 \end{pmatrix}.$$

Eine weitere Rechnung ergibt $x_5^2 = (x_2 x_5)^2 = (x_3 x_5)^2 = (x_4 x_5)^3 = 1$ und $(x_1 x_5)^2 = z$. Daher ist $\langle x_1, \dots, x_5 \rangle$ die gewünschte Schur-Erweiterung \widehat{A}_7 . \square

Bemerkung 6.18.

- (i) Die im Beweis konstruierte Schur-Erweiterung \widehat{A}_6 mit $|Z(\widehat{A}_6)| = 3$ nennt man *VALENTINER-Gruppe*.
- (ii) Angenommen die (universelle) Schur-Erweiterung \widehat{A}_7 ist bereits konstruiert. Dann existiert eine Untergruppe $Z \leq H \leq \widehat{A}_7$ mit $H/Z \cong A_6$. Für $P \in \text{Syl}_3(H)$ ist auch $P \in \text{Syl}_3(\widehat{A}_7)$. Nach Taunt (GT-Satz 7.15) ist P nicht-abelsch und daher $Z = [P, P] \leq H'$. Also ist H eine Schur-Erweiterung von A_6 . Es genügt also \widehat{A}_7 zu konstruieren. Das haben wir mit GAP in Bemerkung 5.18 bereits getan. Die Gruppe lässt sich auch auf andere Weisen konstruieren:

```
PerfectGroup(IsPermGroup, 15120); #einzige perfekte Gruppe dieser Ordnung
LoadPackage("atlasrep", false);
AtlasGroup("6.A7"); #benötigt beim ersten Zugriff Internet
DoubleCoverOfAlternatingGroup(10, 3); #A10 als Matrixgruppe über F3 mit Z(A10) ≅ C2
```

- (iii) Blackburn hat alle Erweiterungen von elementarabelschen Gruppen mit S_n und A_n konstruiert.

7 Symplektische Gruppen

Bemerkung 7.1. Die kompliziertesten einfachen Gruppen sind die Gruppen vom *Lie-Typ*. Dies sind gewisse Matrixgruppen über endlichen Körpern, von denen wir die projektiven speziellen linearen Gruppen $\text{PSL}(n, q)$ bereits in der Gruppentheorie konstruiert haben. In diesem Kapitel werden die

(projektiven) symplektischen Gruppen $\mathrm{PSp}(2n, q)$ eingeführt, die nur in gerader Dimension existieren. Für $n = 1$ gilt $\mathrm{PSp}(2, q) = \mathrm{PSL}(2, q)$. Für $n \geq 2$ erhält man „neue“ einfache Gruppen. Der Beweis benutzt Iwasawas Lemma. Im Unterschied zu $\mathrm{PSL}(n, q)$ versuchen wir diesmal „koordinatenfrei“ zu argumentieren.

Definition 7.2. Sei K ein Körper und V ein endlich-dimensionaler K -Vektorraum. Sei $\beta: V \times V \rightarrow K$, $(v, w) \mapsto [v, w]$ eine Bilinearform mit folgenden Eigenschaften:

- (nicht-ausgeartet) Für alle $v \in V \setminus \{0\}$ existiert ein $w \in V$ mit $[v, w] \neq 0$.
- (alternierend) Für alle $v \in V$ gilt $[v, v] = 0$.

Bzgl. $[\cdot, \cdot]$ nennt man V einen *symplektischen Raum*. Für $v \in V$ und $U \subseteq V$ sei $v^\perp := \{w \in V : [v, w] = 0\} \leq V$ und $U^\perp := \bigcap_{u \in U} u^\perp \leq V$.

Bemerkung 7.3. Aus $[v, v] = 0$ folgt die *Antisymmetrie* $[u, v] = [u + v, u + v] - [v, u] = -[v, u]$ für $u, v \in V$. Für $\mathrm{char} K \neq 2$ sind die Begriffe „alternierend“ und „antisymmetrisch“ äquivalent, denn $[v, v] = -[v, v] = 0$. Für $\mathrm{char} K = 2$ ist Symmetrie und Antisymmetrie identisch.

Satz 7.4. Für $U \leq V$ gilt $\dim V = \dim U + \dim U^\perp$ (aber nicht unbedingt $U \cap U^\perp = 0$).

Beweis. Wir ergänzen eine Basis b_1, \dots, b_k von U zu einer Basis b_1, \dots, b_n von V . Bezüglich dieser Basis identifizieren wir V mit K^n . Für die Gram-Matrix $B = ([b_i, b_j])$ von β gilt dann $[v, w] = vBw^t$ für $v, w \in V$. Da β nicht-ausgeartet ist, ist B invertierbar (alternierend wird für den Beweis nicht benötigt). Die ersten k Zeilen von B bilden eine Matrix A vom Rang $k = \dim U$. Nun ist U^\perp der Lösungsraum des homogenen Gleichungssystems $Ax = 0$. Aus der linearen Algebra folgt $\dim U^\perp = n - k = \dim V - \dim U$. \square

Satz 7.5. Es existiert eine Basis $b_1, \dots, b_n, c_1, \dots, c_n$ von V mit $[b_i, b_j] = 0 = [c_i, c_j]$ und $[b_i, c_j] = \delta_{ij}$ für $i, j = 1, \dots, n$. Insbesondere ist $\dim V = 2n$ gerade (vgl. GT-Aufgabe 67).

Beweis. Induktion nach $\dim V$. Sei $b_1 \in V \setminus \{0\}$. Da β nicht-ausgeartet ist, existiert $c_1 \in V$ mit $[b_1, c_1] \neq 0$. Nach Skalierung gilt $[b_1, c_1] = 1$. Sei nun $U := \langle b_1, c_1 \rangle$. Offenbar ist $U \cap U^\perp = 0$ und Satz 7.4 zeigt $V = U \oplus U^\perp$. Für $u \in U^\perp$ existiert ein $v \in V$ mit $[u, v] \neq 0$. Schreibt man $v = v_1 + v_2$ mit $v_1 \in U$ und $v_2 \in U^\perp$, so folgt $[u, v_2] = [u, v] \neq 0$. Daher ist auch die Einschränkung von β auf U^\perp nicht-ausgeartet und alternierend. Die Behauptung folgt nun mit Induktion. \square

Definition 7.6.

- Man nennt $(v, w) \in V^2$ mit $[v, w] = 1$ ein *hyperbolisches Paar*. Eine Basis wie in Satz 7.5 nennt man *symplektisch*.
- Wir nennen

$$\begin{aligned} \mathrm{Sp}(V) &:= \{f \in \mathrm{GL}(V) : [f(v), f(w)] = [v, w]\} \leq \mathrm{GL}(V), \\ \mathrm{PSp}(V) &:= \mathrm{Sp}(V)/\mathrm{Z}(\mathrm{Sp}(V)). \end{aligned}$$

die (projektive) *symplektische Gruppe* von V .

Bemerkung 7.7.

- (i) Die Gram-Matrix von β bzgl. einer symplektischen Basis ist $B = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}$. Für $v, w \in K^{2n}$ bzgl. dieser Basis gilt $[v, w] = vBw^t$. Dies zeigt

$$\mathrm{Sp}(2n, K) := \{A \in \mathrm{GL}(2n, K) : A^t B A = B\} \cong \mathrm{Sp}(V).$$

Insbesondere hängt der Isomorphietyp von $\mathrm{Sp}(V)$ nicht von β ab. Für endliche Körper setzen wir $\mathrm{Sp}(2n, q) := \mathrm{Sp}(2n, \mathbb{F}_q)$.

- (ii) Für $A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \in \mathrm{Sp}(2n, K)$ gilt

$$\begin{pmatrix} A_1^t & A_3^t \\ A_2^t & A_4^t \end{pmatrix} \begin{pmatrix} A_3 & A_4 \\ -A_1 & -A_2 \end{pmatrix} = A^t B A = B = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix},$$

also $A_1^t A_3 = A_3^t A_1$, $A_2^t A_4 = A_4^t A_2$ und $A_1^t A_4 = 1_n + A_3^t A_2$. Für $n = 1$ sind die ersten beiden Gleichungen trivial und die dritte besagt $\det(A) = 1$. Dies zeigt $\mathrm{Sp}(2, K) = \mathrm{SL}(2, K)$. Für beliebiges n ist $\begin{pmatrix} A_1 & 0 \\ 0 & A_1^{-t} \end{pmatrix} \in \mathrm{Sp}(V)$ für alle $A_1 \in \mathrm{GL}(n, K)$. Daher ist $\mathrm{GL}(n, K)$ zu einer Untergruppe von $\mathrm{Sp}(2n, K)$ isomorph.

- (iii) Wir können die Gram-Matrix von β auch in der Form $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \oplus \dots \oplus \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ anordnen. Dann folgt $\mathrm{Sp}(2k, K) \times \mathrm{Sp}(2(n-k), K) \leq \mathrm{Sp}(2n, K)$ für $0 < k < n$.

Lemma 7.8. *Es gilt $Z(\mathrm{Sp}(V)) = \mathrm{Sp}(V) \cap K^\times \mathrm{id} = \langle -\mathrm{id} \rangle$.*

Beweis. Wegen $-\mathrm{id} \in \mathrm{Sp}(V) \cap K^\times \mathrm{id} \subseteq Z(\mathrm{Sp}(V))$ müssen wir nur $Z(\mathrm{Sp}(2n, K)) \subseteq \langle -1_2 \rangle$ zeigen. Für $n = 1$ ist $Z(\mathrm{Sp}(2, K)) = Z(\mathrm{SL}(2, K)) = \langle -1_2 \rangle$ (im Fall $\mathrm{char} K = 2$ ist $-1_2 = 1_2$). Sei also $n \geq 2$. Wir schreiben $A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \in Z(\mathrm{Sp}(2n, K))$ wie in Bemerkung 7.7. Für $M = \begin{pmatrix} C & 0 \\ 0 & C^{-t} \end{pmatrix} \in \mathrm{Sp}(2n, K)$ mit $C \in \mathrm{GL}(n, K)$ gilt

$$\begin{pmatrix} A_1 C & A_2 C^{-t} \\ A_3 C & A_4 C^{-t} \end{pmatrix} = A M = M A = \begin{pmatrix} C A_1 & C A_2 \\ C^{-t} A_3 & C^{-t} A_4 \end{pmatrix}.$$

Dies zeigt $A_1, A_4 \in Z(\mathrm{GL}(n, K)) = K^\times 1_n$. Für $C = 1_n + E_{ij}$ mit $i \neq j$ folgt $E_{ij} A_2 = -A_2 E_{ji}$ und $A_2 = 0$. Analog ist $A_3 = 0$ und man erhält $A_1^t = A_4^{-1} \in \mathrm{GL}(n, K)$. Sei $\lambda \in K^\times$ mit $A_1 = \lambda 1_n$ und $A_4 = \lambda^{-1} 1_n$. Wegen $B = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix} \in \mathrm{Sp}(2n, K)$ gilt auch

$$\begin{pmatrix} 0 & A_1 \\ -A_4 & 0 \end{pmatrix} = A B = B A = \begin{pmatrix} 0 & A_4 \\ -A_1 & 0 \end{pmatrix}.$$

Also ist $\lambda = \lambda^{-1} = \pm 1$. □

Satz 7.9. *Es gilt*

$$\begin{aligned} |\mathrm{Sp}(2n, q)| &= q^{n^2} \prod_{k=1}^n (q^{2k} - 1), \\ |\mathrm{PSp}(2n, q)| &= \frac{1}{\mathrm{ggT}(q-1, 2)} q^{n^2} \prod_{k=1}^n (q^{2k} - 1). \end{aligned}$$

Beweis. Nach Lemma 7.8 folgt die zweite Gleichung aus der ersten. Jedes $f \in \text{Sp}(V)$ bildet eine symplektische Basis auf eine symplektische Basis ab. Umgekehrt kann man dadurch genau ein $f \in \text{Sp}(V)$ definieren. Daher ist $|\text{Sp}(V)|$ die Anzahl der symplektischen Basen von V . Für $b_1 \in V \setminus \{1\}$ gibt es $q^{2n} - 1$ Möglichkeiten. Der Vektor c_1 definiert genau eine Nebenklasse $c_1 + b_1^\perp$. Also gibt es $|b_1^\perp| = q^{2n-1}$ Möglichkeiten für c_1 . Im Fall $n = 1$ ist daher $|\text{Sp}(2, q)| = q(q^2 - 1)$ wie behauptet. Sei nun $n \geq 2$ und $U := \langle b_1, c_1 \rangle$. Wie in Satz 7.5 ist $V = U \oplus U^\perp$ und $b_2, \dots, b_n, c_2, \dots, c_n$ bilden eine symplektische Basis von U^\perp . Durch Induktion nach n folgt

$$|\text{Sp}(2n, q)| = q^{2n-1}(q^{2n} - 1)|\text{Sp}(2n-2, q)| = q^{2n-1+(n-1)^2} \prod_{k=1}^n (q^{2k} - 1) = q^{n^2} \prod_{k=1}^n (q^{2k} - 1). \quad \square$$

Definition 7.10. Für $\lambda \in K$ und $v \in V$ nennt man die lineare Abbildung

$$t_{\lambda, v}: V \rightarrow V, \quad x \mapsto x + \lambda[x, v]v$$

eine (*symplektische*) *Transvektion*.

Bemerkung 7.11. Für $\lambda, \mu \in K$ und $v, x \in V$ gilt

$$t_{\lambda, v}(t_{\mu, v}(x)) = t_{\lambda, v}(x + \mu[x, v]v) = x + \mu[x, v]v + \lambda[x + \mu[x, v]v, v]v = t_{\lambda+\mu, v}(x).$$

Insbesondere ist $t_{\lambda, v}$ invertierbar mit $t_{\lambda, v}^{-1} = t_{-\lambda, v}$. Wegen

$$[t_{\lambda, v}(x), t_{\lambda, v}(y)] = [x, y] + \lambda[x, v][v, y] + \lambda[y, v][x, v] + \lambda^2[x, v][y, v][v, v] = [x, y]$$

ist $t_{\lambda, v} \in \text{Sp}(V)$. Offenbar ist v^\perp der Fixpunktraum (Eigenraum zum Eigenwert 1) von $t_{\lambda, v}$. Für ein hyperbolisches Paar (v, w) gilt $t_{\lambda, v}(w) = w - \lambda v \in w + v^\perp$. Dies zeigt $\det(t_{\lambda, v}) = 1$. Für $g \in \text{Sp}(V)$ gilt

$$(gt_{\lambda, v}g^{-1})(x) = g(g^{-1}(x) + \lambda[g^{-1}(x), v]v) = x + \lambda[x, g(v)]g(v) = t_{\lambda, g(v)}(x).$$

Für $\mu \in K$ ist

$$t_{\lambda, \mu v}(x) = x + \lambda[x, \mu v]\mu v = x + \lambda\mu^2[x, v]v = t_{\lambda\mu^2, v}(x).$$

Lemma 7.12. Die symplektischen Transvektionen erzeugen $\text{Sp}(V)$. Insbesondere ist $\text{Sp}(V) \leq \text{SL}(V)$.

Beweis. Nach Satz 7.9 genügt es zu zeigen, dass $S := \langle t_{\lambda, v} : \lambda \in K, v \in V \rangle$ transitiv auf der Menge Ω aller symplektischen Basen operiert. Seien $v, w \in V \setminus \{0\}$. Falls $\lambda := [v, w] \neq 0$, so ist

$$t_{\lambda^{-1}, v-w}(v) = v + \lambda^{-1}[v, v-w](v-w) = v - (v-w) = w.$$

Anderenfalls wähle $x \in V \setminus (v^\perp \cup w^\perp)$. Man kann nun $v \mapsto x \mapsto w$ durch zwei Transvektionen realisieren. Also ist S transitiv auf $V \setminus \{0\}$.

Seien nun $u, v, w \in V$ mit $[u, v] = [u, w] = 1$. Dann ist $v - w \in u^\perp$. Im Fall $\lambda := [v, w] \neq 0$ gilt $t_{\lambda^{-1}, v-w}(u, v) = (u, w)$. Anderenfalls setze $x := u + v$. Dann ist $[u, v] = [u, x] = [u, w] = 1$ und $[v, x] \neq 0 \neq [x, w]$. Man kann daher $(u, v) \mapsto (u, x) \mapsto (u, w)$ durch zwei Transvektionen realisieren. Damit ist S transitiv auf der Menge der hyperbolischen Paare.

Seien schließlich $b_1, \dots, b_n, c_1, \dots, c_n$ und $b'_1, \dots, b'_n, c'_1, \dots, c'_n$ symplektische Basen von V . Nach dem bereits Gezeigten können wir $(b'_1, c'_1) = (b_1, c_1)$ annehmen. Dann sind

$$b_2, \dots, b_n, c_2, \dots, c_n \quad \text{und} \quad b'_2, \dots, b'_n, c'_2, \dots, c'_n$$

symplektische Basen von $\langle b_1, c_1 \rangle^\perp$. Nach Induktion existiert ein Produkt von symplektischen Transvektionen auf $\langle b_1, c_1 \rangle^\perp$, dass $(b_2, \dots, b_n, c_2, \dots, c_n)$ auf $(b'_2, \dots, b'_n, c'_2, \dots, c'_n)$ abbildet. Für $x \in \langle b_1, c_1 \rangle^\perp$ werden b_1 und c_1 von $t_{\lambda, x}$ festgehalten. Die Transvektionen auf $\langle b_1, c_1 \rangle^\perp$ lassen sich also nach $V = \langle b_1, c_1 \rangle^\perp \oplus \langle b_1, c_1 \rangle$ fortsetzen, indem man trivial auf $\langle b_1, c_1 \rangle$ operiert. Also kann man $b_1, \dots, b_n, c_1, \dots, c_n$ auf $b'_1, \dots, b'_n, c'_1, \dots, c'_n$ mittels S abbilden. \square

Satz 7.13. *Für jeden endlichen Körper K operiert $\mathrm{PSp}(V)$ treu und primitiv auf der Menge Ω der 1-dimensionalen Unterräume von V .*

Beweis. Für $\mathrm{Sp}(2, K) = \mathrm{SL}(2, K)$ ist die Behauptung bekannt. Sei also $n \geq 2$ und $q := |K|$. Nach GT-Lemma 10.7 operiert $G := \mathrm{Sp}(V) \leq \mathrm{SL}(V)$ auf Ω mit Kern $\mathrm{Sp}(V) \cap K^\times \mathrm{id} = \langle -\mathrm{id} \rangle$. Also operiert $\bar{G} := \mathrm{PSp}(V)$ treu auf Ω . Nach dem Beweis von Satz 7.9 operiert \bar{G} transitiv auf Ω . Sei $U := Ku \in \Omega$ und G_U der Stabilisator von U in G . Sei (u, u') ein hyperbolisches Paar. Wie im Beweis von Lemma 7.12 operiert $G_u \subseteq G_U$ transitiv auf $u' + u^\perp$. Da jeder Vektor in $u' + u^\perp$ einen anderen Unterraum aufspannt, hat G_U eine Bahn der Länge $\geq q^{2n-1}$ auf Ω . Seien $v, w \in u^\perp \setminus U$. Im Fall $[v, w] \neq 0$ kann man wie im Beweis von Lemma 7.12 (u, v) auf (u, w) abbilden. Sei nun $[v, w] = 0$. Wegen

$$(v^\perp)^\perp = \langle v \rangle \neq U = (u^\perp)^\perp \neq (w^\perp)^\perp$$

ist $v^\perp \neq u^\perp \neq w^\perp$. Sei $x \in u^\perp \setminus v^\perp$ und $y \in u^\perp \setminus w^\perp$. Im Fall $u^\perp \subseteq v^\perp \cup w^\perp$ ist $x \in w^\perp, y \in v^\perp$ und man erhält den Widerspruch $x + y \in u^\perp \setminus (v^\perp \cup w^\perp)$. Dies zeigt $u^\perp \not\subseteq v^\perp \cup w^\perp$. Sei also $x \in u^\perp \setminus (v^\perp \cup w^\perp)$. Man kann nun mit zwei Transvektionen $(u, v) \mapsto (u, x) \mapsto (u, w)$ realisieren. Also sind G_u und G_U transitiv auf $u^\perp \setminus U$. Dies liefert eine Bahn der Länge $\frac{q^{2n-1}-q}{q-1} < q^{2n-1}$. Wegen

$$|\Omega \setminus \{U\}| = \frac{q^{2n} - q}{q - 1} = \frac{q^{2n-1} - q}{q - 1} + q^{2n-1}$$

hat G_U zwei Bahnen auf $\Omega \setminus \{U\}$ mit den Längen q^{2n-1} und $\frac{q^{2n-1}-q}{q-1}$.

Angenommen G ist imprimitiv auf Ω mit Block $\Delta \ni U$. Dann muss eine der beiden nicht-trivialen Bahnen von G_U in Δ liegen. Allerdings sind $q^{2n-1} + 1$ und $\frac{q^{2n-1}-q}{q-1} + 1 = \frac{q^{2n-1}-1}{q-1}$ keine Teiler von $|\Omega| = \frac{q^{2n}-1}{q-1} = q^{2n-1} + q^{2n-2} + \dots + 1$. Dieser Widerspruch zeigt, dass G und \bar{G} primitiv operieren. \square

Lemma 7.14. *Für $n \geq 2$ und $(n, q) \neq (2, 2)$ ist $\mathrm{Sp}(2n, q)$ perfekt.*

Beweis. Nach Lemma 7.12 genügt es zu zeigen, dass die Transvektionen Kommutatoren sind. Sei zunächst $q \geq 4$. Sei $v \in V \setminus \{0\}$ und $\lambda \in K^\times$. Wähle $\mu \in K^\times \setminus \{\pm 1\}$ und setze $\alpha := \lambda(1 - \mu^2)^{-1}$. Bekanntlich existiert $g \in \mathrm{Sp}(V)$ mit $g(v) = \mu^2 v$. Nach Bemerkung 7.11 gilt

$$\mathrm{Sp}(V)' \ni [t_{\alpha, v}, g] = t_{\alpha, v} g t_{-\alpha, v} g^{-1} = t_{\alpha, v} t_{-\alpha, g(v)} = t_{\alpha, v} t_{-\alpha \mu^2, v} = t_{\alpha(1-\mu^2), v} = t_{\lambda, v}.$$

Sei nun $q = 3$ und $b_1, \dots, b_n, c_1, \dots, c_n$ eine symplektische Basis von V . Wir definieren $g, h \in \mathrm{Sp}(V)$ durch

$$\begin{aligned} g(b_1) &:= b_1 + b_2, & g(c_1) &:= c_2, & g(b_2) &:= b_1, & g(c_2) &:= c_1 - c_2, \\ h(b_1) &:= b_1 - c_1 + c_2, & h(c_1) &:= c_1, & h(b_2) &:= b_2 + c_1, & h(c_2) &:= c_2 \end{aligned}$$

und $g(b_i) = h(b_i) = b_i$ sowie $g(c_i) = h(c_i) = c_i$ für $i \geq 3$. Es gilt

$$\begin{aligned} [g, h](b_1) &= ghg^{-1}(b_1 + c_1 - c_2) = gh(b_2 + c_2) = g(b_2 + c_1 + c_2) = b_1 + c_1, \\ [g, h](c_1) &= ghg^{-1}(c_1) = gh(c_1 + c_2) = g(c_1 + c_2) = c_1, \\ [g, h](b_2) &= ghg^{-1}(b_2 - c_1) = gh(b_1 - b_2 - c_1 - c_2) = g(b_1 - b_2) = b_2, \\ [g, h](c_2) &= ghg^{-1}(c_2) = gh(c_1) = g(c_1) = c_2, \end{aligned}$$

d. h. $t_{1,c_1} = [g, h] \in \text{Sp}(V)'$ und $t_{-1,c_1} = t_{1,c_1}^{-1} \in \text{Sp}(V)'$. Da c_1 beliebig ist, folgt die Behauptung.

Schließlich sei $q = 2$ und $n \geq 3$. Diesmal definieren wir

$$\begin{aligned} g(b_1) &:= b_1 + b_3, & g(c_1) &:= c_3, & g(b_2) &:= b_1, & g(c_2) &:= c_1 + c_3, \\ g(b_3) &:= b_2, & g(c_3) &:= c_2, & h(b_1) &:= b_1 + c_2, & h(c_1) &:= c_1, \\ h(b_2) &:= b_2 + c_1 + c_2 + c_3, & h(c_2) &:= c_2, & h(b_3) &:= b_3 + c_2 + c_3, & h(c_3) &:= c_3 \end{aligned}$$

und $g(b_i) = h(b_i) = b_i$ sowie $g(c_i) = h(c_i) = c_i$ für $i \geq 4$. Es gilt

$$\begin{aligned} [g, h](b_1) &= ghg^{-1}(b_1 + c_2) = gh(b_2 + c_3) = g(b_2 + c_1 + c_2) = b_1 + c_1, \\ [g, h](c_1) &= ghg^{-1}(c_1) = gh(c_1 + c_2) = g(c_1 + c_2) = c_1, \\ [g, h](b_2) &= ghg^{-1}(b_2 + c_1 + c_2 + c_3) = gh(b_3 + c_2 + c_3) = g(b_3) = b_2, \\ [g, h](c_2) &= ghg^{-1}(c_2) = gh(c_3) = g(c_3) = c_2, \\ [g, h](b_3) &= ghg^{-1}(b_3 + c_2 + c_3) = gh(b_1 + b_2 + c_1 + c_3) = g(b_1 + b_2) = b_3, \\ [g, h](c_3) &= ghg^{-1}(c_3) = gh(c_1) = g(c_1) = c_3, \end{aligned}$$

d. h. $t_{1,c_1} = [g, h] \in \text{Sp}(V)'$. Dies zeigt die Behauptung. \square

Satz 7.15. *Es gilt $\text{Sp}(4, 2) \cong S_6$. Insbesondere ist $\text{Sp}(4, 2) = \text{PSp}(4, 2)$ nicht perfekt.*

Beweis. Sei $V := \{x \in \mathbb{F}_2^6 : \sum_{i=1}^6 x_i = 0\} \leq \mathbb{F}_2^6$ und $U := \langle (1, \dots, 1) \rangle \leq V$. Die symmetrische Gruppe S_6 operiert durch Permutation der Koordinaten treu auf $V/U \cong \mathbb{F}_2^4$. Das „Standardskalarprodukt“

$$[v + U, w + U] := \sum_{i=1}^6 v_i w_i$$

ist eine wohldefinierte alternierende Bilinearform auf V/U . Sei $v + U \neq 0$, o. B. d. A. $v_1 = v_2 = 1$ und $v_3 = 0$. Dann ist $w + U := (0, 1, 1, 0, 0, 0) + U \in V/U$ mit $[v + U, w + U] \neq 0$. Also ist die Bilinearform nicht-ausgeartet. Für $\sigma \in S_6$ gilt schließlich $[\sigma(v) + U, \sigma(v) + U] = [v + U, w + U]$. Dies zeigt $S_6 \leq \text{Sp}(4, 2)$. Nach Satz 7.9 ist andererseits $|\text{Sp}(4, 2)| = 2^4(2^2 - 1)(2^4 - 1) = 720 = |S_6|$. \square

Satz 7.16. *Für $n \geq 2$ und $(n, q) \neq (2, 2)$ ist $\text{PSp}(2n, q)$ einfach.*

Beweis. Nach den vorherigen Sätzen ist $G := \text{PSp}(2n, q)$ perfekt und primitiv auf der Menge der 1-dimensionalen Unterräume von V . Sei $U := \langle u \rangle \leq V$ mit $u \neq 0$ und $A := \{\pm t_{\lambda, u} : \lambda \in K\} \leq G_U$. Offenbar ist A abelsch und normal in G_U . Außerdem ist jede Transvektion in $\text{Sp}(V)$ zu $t_{\lambda, u}$ mit einem $\lambda \in K$ konjugiert. Aus Lemma 7.12 folgt $\langle gAg^{-1} : g \in G \rangle = G$. Nach Iwasawas Lemma aus der Gruppentheorie ist G einfach. \square

Bemerkung 7.17. Eine weitere Familie von einfachen Gruppen vom Lie-Typ lässt sich durch Untergruppen von $\mathrm{Sp}(4, q)$ mit $q = 2^{2n+1}$ und $n \in \mathbb{N}$ konstruieren: Sei e_1, e_2, e_3, e_4 eine symplektische Basis auf $V = \mathbb{F}_q^4$ mit $[e_1, e_3] = 1 = [e_2, e_4]$. Wir definieren eine kommutative Multiplikation auf V durch

$$e_i * e_j := \begin{cases} e_1 & \text{falls } \{i, j\} = \{2, 3\}, \\ e_2 & \text{falls } \{i, j\} = \{1, 2\}, \\ e_3 & \text{falls } \{i, j\} = \{1, 4\}, \\ e_4 & \text{falls } \{i, j\} = \{3, 4\}, \\ 0 & \text{sonst} \end{cases}$$

$$\left(\sum_{i=1}^4 \lambda_i e_i \right) * \left(\sum_{i=1}^4 \mu_i e_i \right) := \sum_{i,j=1}^4 (\lambda_i \mu_j)^{2^n} e_i * e_j$$

für $\lambda_i, \mu_j \in \mathbb{F}_q$. Sei $U := \{(u, v) \in V^2 : [u, v] = 0\}$ und

$$\mathrm{Sz}(q) := \{f \in \mathrm{Sp}(V) : \forall (u, v) \in U : f(u) * f(v) = u * v\} \leq \mathrm{Sp}(V).$$

Man nennt $\mathrm{Sz}(q)$ die *Suzuki-Gruppe* über \mathbb{F}_q . Sie ist einfach mit Ordnung

$$|\mathrm{Sz}(q)| = q^2(q^2 + 1)(q - 1) \equiv -1 \pmod{3}.$$

Die Suzuki-Gruppen sind die einzigen nicht-abelschen einfachen Gruppen, deren Ordnung nicht durch 3 teilbar ist. Wegen $q^2 + 1 \equiv 16^n \cdot 4 + 1 \equiv 0 \pmod{5}$ ist die Ordnung jeder nicht-abelschen einfachen Gruppe durch 3 oder 5 teilbar (sogar durch 12 oder $2^6 \cdot 5$ nach Feit-Thompson). Die Untergruppenstruktur und die Charaktertafel von $\mathrm{Sz}(q)$ ist ähnlich wie bei $\mathrm{PSL}(2, q)$ sehr übersichtlich (die Sylowgruppen zu ungeraden Primzahlen sind zyklisch, vgl. GT-Satz 10.13). Suzuki hat auch eine sporadische Gruppe der Ordnung 448.345.497.600 entdeckt.

8 Unitäre Gruppen

Bemerkung 8.1. Nach den linearen und symplektischen Gruppen behandeln wir in diesem Abschnitt eine dritte Familie von (einfachen) Gruppen vom Lie-Typ.

Definition 8.2. Sei $q \neq 1$ eine Primzahlpotenz, $K = \mathbb{F}_{q^2}$ und V ein endlich-dimensionaler K -Vektorraum. Sei $\mathrm{Gal}(K|\mathbb{F}_q) = \langle \alpha \rangle \cong C_2$ mit $\bar{x} := \alpha(x) = x^q$ für $x \in K$ (vgl. komplexe Konjugation). Sei $V \times V \rightarrow K$, $(v, w) \mapsto [v, w]$ eine nicht-ausgeartete Sesquilinearform, d. h. für $u, v, w \in V$ und $\lambda \in K$ gilt

$$\begin{aligned} \forall u \neq 0 \exists v : [u, v] &\neq 0, \\ [u + \lambda v, w] &= [u, w] + \lambda [v, w], \\ [u, v] &= \overline{[v, u]}. \end{aligned}$$

Bzgl. $[\cdot, \cdot]$ nennt man V einen *unitären Raum*.

Bemerkung 8.3.

- (i) Im Folgenden sei V stets ein unitärer Raum.

(ii) Für $u, v, w \in V$ und $\lambda \in K$ gilt

$$[u, v + \lambda w] = \overline{[v + \lambda w, u]} = \overline{[v, u]} + \overline{\lambda[w, u]} = [u, v] + \overline{\lambda}[u, w].$$

(iii) Für $K^\times = \langle \zeta \rangle$ gilt $\zeta \bar{\zeta} = \zeta^{q+1} \in \mathbb{F}_q$. Daher ist die Norm $N: K \rightarrow \mathbb{F}_q$, $x \mapsto x\bar{x}$ surjektiv. Sei $x \in K$ im Kern der Spur $S: K \rightarrow \mathbb{F}_q$, $y \mapsto y + \bar{y}$. Dann gilt $x = -x^q$ und es folgt $x = 0$ oder $x^{q-1} = -1$. Dies zeigt $|\text{Ker}(S)| \leq q$. Als lineare Abbildung muss S nach dem Homomorphiesatz ebenfalls surjektiv sein. Für $v \in V$ gilt $[v, v] = \overline{[v, v]} \in \mathbb{F}_q$. Im Fall $[v, v] \neq 0$ existiert ein $\lambda \in K$ mit $[\lambda v, \lambda v] = 1$, d. h. v lässt sich normieren. Im Gegensatz zu $K = \mathbb{C}$ gibt es Vektoren $v \neq 0$ mit $[v, v] = 0$ (siehe Lemma 8.10).

(iv) Wie üblich definiert man v^\perp und $S^\perp \leq V$ für $v \in V$ und $S \subseteq V$. Wie in Satz 7.4 zeigt man $\dim U + \dim U^\perp = \dim V$ für alle Unterräume $U \leq V$. Daraus folgen die üblichen Regeln:

$$(U^\perp)^\perp = U, \quad U \subseteq W \iff W^\perp \subseteq U^\perp, \quad (U + W)^\perp = U^\perp \cap W^\perp.$$

Gilt $V = U \oplus U^\perp$, so ist die Einschränkung von $[\cdot, \cdot]$ auf U nicht-*ausgeartet*. Daher ist U ein unitärer Raum. Dies werden wir häufig für Induktion nach $\dim V$ benutzen.

Satz 8.4. Jeder unitäre Raum V besitzt eine Orthonormalbasis b_1, \dots, b_n , d. h. es gilt $[b_i, b_j] = \delta_{ij}$.

Beweis. Sei $v \in V \setminus \{0\}$. Da $[\cdot, \cdot]$ nicht-*ausgeartet* ist, existiert ein $w \in V$ mit $[v, w] \neq 0$. Nach Skalierung können wir $[v, w] + [w, v] \neq 0$ annehmen (für $\text{char } K \neq 2$ kann man $[v, w] = 1$ wählen). Im Fall $[v, v] = 0 = [w, w]$ gilt $[v + w, v + w] \neq 0$. In jedem Fall findet man ein $b_1 \in V$ mit $[b_1, b_1] \neq 0$. Nach Normierung ist $[b_1, b_1] = 1$. Im Fall $n = 1$ sind wir fertig. Sei also $n \geq 2$ und $U := b_1^\perp$. Offenbar gilt $V = \langle b_1 \rangle \oplus U$. Nach Bemerkung 8.3 ist U ein unitärer Raum der Dimension $n - 1$. Durch Induktion nach n können wir annehmen, dass U eine Orthonormalbasis b_2, \dots, b_n besitzt. Offenbar ist nun b_1, \dots, b_n eine Orthonormalbasis von V . \square

Beispiel 8.5. Wie über \mathbb{C} sieht man, dass $V = K^n$ bzgl. des Standardskalarprodukts

$$[v, w] := v_1 \overline{w_1} + \dots + v_n \overline{w_n} \quad (v, w \in V)$$

ein unitärer Raum ist. Die Standardbasis e_1, \dots, e_n ist eine Orthonormalbasis von V . Nach Satz 8.4 können wir uns im Folgenden oft auf diesen speziellen Raum beschränken.

Definition 8.6. Eine lineare Abbildung zwischen unitären Räumen $f: V \rightarrow W$ heißt *Isometrie*, falls $[f(u), f(v)]_W = [u, v]_V$ für alle $u, v \in V$ gilt. Man definiert die Gruppen

$$\text{GU}(V) := \{f \in \text{GL}(V) : \forall v, w \in V : [f(v), f(w)] = [v, w]\} \quad (\text{allgemeine unitäre Gruppe}),$$

$$\text{SU}(V) := \text{GU}(V) \cap \text{SL}(V) \quad (\text{spezielle unitäre Gruppe}),$$

$$\text{PSU}(V) := \text{SU}(V)/\text{Z}(\text{SU}(V)) \quad (\text{projektive spezielle unitäre Gruppe}).$$

Bemerkung 8.7. Da $[\cdot, \cdot]$ nicht-*ausgeartet* ist, ist jede Isometrie injektiv. Sei $f \in \text{GL}(V)$ mit Matrix $A \in \text{GL}(n, K)$ bzgl. der Standardbasis. Für $v, w \in V$ gilt $[f(v), f(w)] = [Av, Aw] = v^t A^t \overline{A} w^t$. Durch Einsetzen der Standardbasis sieht man

$$\forall v, w \in V : [f(v), f(w)] = [v, w] \iff A^t \overline{A} = 1_n.$$

Auf diese Weise erhält man die Matrixgruppen

$$\text{GU}(n, q) := \{A \in \text{GL}(n, q^2) : A^t \overline{A} = 1_n\},$$

$$\text{SU}(n, q) := \text{GU}(n, q) \cap \text{SL}(n, q^2),$$

$$\text{PSU}(n, q) := \text{SU}(n, q)/\text{Z}(\text{SU}(n, q)).$$

Beispiel 8.8. Für jede Permutationsmatrix $P \in \text{GL}(n, q^2)$ gilt $P^t \overline{P} = P^{-1}P = 1_n$, d. h. $P \in \text{GU}(n, q)$. Daher besitzt $\text{GU}(n, q)$ (bzw. $\text{SU}(n, q)$) eine zu S_n (bzw. A_n) isomorphe Untergruppe.

Lemma 8.9. Es gilt $C_{\text{GL}(V)}(\text{SU}(V)) = K^\times \text{id}_V$.

Beweis. O. B. d. A. sei $V = K^n$ mit $n \geq 2$. Sei $K^\times = \langle \zeta \rangle$. Wegen $\zeta^{q-1} \overline{\zeta^{q-1}} = \zeta^{q-1+q^2-q} = \zeta^{q^2-1} = 1$ ist $D := \text{diag}(\zeta^{q-1}, \zeta^{1-q}, 1, \dots, 1) \in \text{SU}(n, q) \setminus \{1_n\}$ (auch für $q = 2$). Es folgt

$$C_{\text{GL}(V)}(\text{SU}(V)) \subseteq C_{\text{GL}(V)}(D) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & A \end{pmatrix} : a, b \in K^\times, A \in \text{GL}(n-2, K) \right\}.$$

Durch Permutation der Koordinaten erhält man, dass $C_{\text{GL}(V)}(\text{SU}(V))$ aus Diagonalmatrizen besteht. Wegen

$$\begin{pmatrix} 0 & \cdots & 0 & (-1)^{n-1} \\ 1 & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{pmatrix} \in \text{SU}(n, q)$$

können nur Skalarmatrizen $\text{SU}(V)$ zentralisieren. Umgekehrt gilt natürlich $K^\times \text{id}_V \leq Z(\text{GL}(V))$. \square

Lemma 8.10. Für $\lambda \in \mathbb{F}_q$ sei $V_\lambda := \{v \in V : [v, v] = \lambda\}$. Dann gilt

$$\begin{aligned} z_n &:= |V_0| = q^{2n-1} + (-1)^n q^{n-1} (q-1), \\ w_n &:= |V_1| = q^{n-1} (q^n - (-1)^n). \end{aligned}$$

Beweis. O. B. d. A. sei $V = K^n$ bzgl. des Standardskalarprodukts.

- (i) Für $n = 1$ ist $V_0 = \{0\}$ und $z_1 = 1 = q - (q-1)$ wie behauptet. Sei $n \geq 1$ und $v = (v', v_n) \in K^{n+1}$ mit $v' \in K^n$ und $[v, v] = 0$. Im Fall $[v', v'] = 0$ ist auch $v_n = 0$. Dafür gibt es z_n Möglichkeiten. Sei nun $[v', v'] \neq 0$ und $K^\times = \langle \zeta \rangle$. Sei $a \in \mathbb{Z}$ mit $-[v', v'] = \zeta^{a(q+1)}$. Aus

$$v_n^{q+1} = v_n \overline{v_n} = [v, v] - [v', v'] = -[v', v']$$

folgt $v_n \in \zeta^a \langle \zeta^{q-1} \rangle$. Es existieren genau $|\langle \zeta^{q-1} \rangle| = q+1$ Elemente mit dieser Eigenschaft. Dies zeigt

$$z_{n+1} = z_n + (q^{2n} - z_n)(q+1) = q^{2n+1} + q^{2n} - qz_n.$$

Die Behauptung folgt mit Induktion.

- (ii) Für $\lambda \neq 0$ ist $V_\lambda \rightarrow V_{\lambda \zeta^{q+1}}, v \mapsto \zeta v$ eine Bijektion. Mit (i) folgt

$$w_n = |V_1| = \frac{q^{2n} - z_n}{q-1} = q^{2n-1} - (-1)^n q^{n-1} = q^{n-1} (q^n - (-1)^n). \quad \square$$

Satz 8.11. Es gilt

$$\begin{aligned} |\text{GU}(n, q)| &= q^{n(n-1)/2} \prod_{k=1}^n (q^k - (-1)^k), \\ |\text{SU}(n, q)| &= q^{n(n-1)/2} \prod_{k=2}^n (q^k - (-1)^k), \\ |\text{PSU}(n, q)| &= \frac{q^{n(n-1)/2}}{\text{ggT}(n, q+1)} \prod_{k=2}^n (q^k - (-1)^k). \end{aligned}$$

Beweis. Genau dann gilt $A \in \text{GU}(n, q)$, wenn die Zeilen von A eine Orthonormalbasis von V bzgl. $[\cdot, \cdot]$ bilden. Für die erste Zeile a_1 von A gibt es nach Lemma 8.10 genau w_n Möglichkeiten. Die zweite Zeile a_2 liegt in $U := a_1^\perp$. Wegen $V = \langle a_1 \rangle \oplus U$ ist U ein unitärer Raum der Dimension $n - 1$. Daher gibt es w_{n-1} Möglichkeiten für a_2 usw. Dies zeigt

$$|\text{GU}(n, q)| = w_1 \dots w_n = \prod_{k=1}^n q^{k-1} (q^k - (-1)^k) = q^{n(n-1)/2} \prod_{k=1}^n (q^k - (-1)^k).$$

Für $A \in \text{GU}(n, q)$ gilt $\det(A)^{q+1} = \det(A) \overline{\det(A)} = \det(A^t \bar{A}) = 1$. Wegen $\text{diag}(\zeta^{q-1}, 1, \dots, 1) \in \text{GU}(n, q)$ ist $\det: \text{GU}(n, q) \rightarrow \langle \zeta^{q-1} \rangle$ surjektiv mit Kern $\text{SU}(n, q)$. Daraus folgt die Formel für $|\text{SU}(n, q)|$. Nach Lemma 8.9 ist

$$\text{Z}(\text{SU}(n, q)) = \text{SU}(n, q) \cap K^\times 1_n = \text{SU}(n, q) \cap \langle \zeta^{q-1} \rangle.$$

Für $\zeta^{a(q-1)} 1_n \in \text{Z}(\text{SU}(n, q))$ mit $0 \leq a \leq q$ gilt $\zeta^{a(q-1)n} = 1$. Also ist $a \equiv 0 \pmod{(q+1)/\text{ggT}(n, q+1)}$ und $|\text{Z}(\text{SU}(n, q))| = \text{ggT}(n, q+1)$. Daraus folgt die Formel für $|\text{PSU}(n, q)|$. \square

Lemma 8.12. *Es gilt $\text{SU}(2, q) \cong \text{SL}(2, q)$ und $\text{PSU}(2, q) \cong \text{PSL}(2, q)$.*

Beweis. Wir konstruieren zunächst eine Basis $\{v, v\} \subseteq V_0$ von $V = K^2$ mit $[u, v] = -[v, u]$. Sei dafür $\mu \in K \setminus \{1\}$ mit $\mu^{q+1} = \mu \bar{\mu} = -1$. Für $2 \nmid q$ setzen wir $u := (1, \mu)$, $v := (\mu, 1)$ und für $2 \mid q$ sei $u := (1, 1)$, $v := (1, \mu)$. In beiden Fällen sind u und v linear unabhängig mit $[u, u] = [v, v] = 0$. Nach Bemerkung 8.3 folgt $[u, v] \neq 0$. Nach Normierung von v erhält man $[u, v] = 1$. Für $2 \mid q$ ist dann $[u, v] = \overline{[v, u]} = [v, u] = -[v, u]$. Für $2 \nmid q$ existiert $\tau \in K$ mit $\tau^{q-1} = -1$, d. h. $\bar{\tau} = -\tau$. Indem wir u durch τu ersetzen, erhalten wir $[u, v] = -[v, u]$ wie gewünscht.

Sei $A \in \text{SU}(2, q)$ und $Au = au + cv$, $Av = bu + dv$ mit $a, b, c, d \in K$. Dann gilt

$$\begin{aligned} a\bar{c} - \bar{a}c &= \frac{[Au, Au]}{[u, v]} = 0 = \frac{[Av, Av]}{[u, v]} = b\bar{d} - \bar{b}d, \\ \bar{a}d - c\bar{b} &= \frac{[Au, Av]}{[u, v]} = 1 = d\bar{a} - b\bar{c}, \\ ad - bc &= \det A = 1. \end{aligned}$$

Es folgt

$$\begin{aligned} \bar{c} + bc\bar{c} &= (1 + bc)\bar{c} = a\bar{d}c = \bar{d}ac = (1 + b\bar{c})c = c + bc\bar{c}, \\ b + b\bar{b}c &= b(1 + \bar{c}b) = ba\bar{d} = a\bar{d}b = (1 + bc)\bar{b} = \bar{b} + b\bar{b}c \end{aligned}$$

und $b, c \in \mathbb{F}_q$. Im Fall $b \neq 0$ ergibt sich $d = \bar{d} \in \mathbb{F}_q$. Anderenfalls ist $a \neq 0$ und $ad = 1 = a\bar{d}$. Wieder gilt $d \in \mathbb{F}_q$. Analog erhält man $a \in \mathbb{F}_q$. Die Basistransformation $\{(1, 0), (0, 1)\} \mapsto \{u, v\}$ liefert also einen Monomorphismus $\varphi: \text{SU}(2, q) \rightarrow \text{SL}(2, q)$. Nach Satz 8.11 ist $|\text{SU}(2, q)| = q(q^2 - 1) = |\text{SL}(2, q)|$. Also ist φ ein Isomorphismus. \square

Beispiel 8.13. Offensichtlich ist $\text{GU}(1, q) \cong C_{q+1}$ und $\text{SU}(1, q) = 1$. Nach Lemma 8.12 gilt $\text{PSU}(2, 2) \cong \text{SU}(2, 2) \cong \text{SL}(2, 2) \cong S_3$ und $\text{PSU}(2, 3) \cong \text{PSL}(2, 3) \cong A_4$. Nach Satz 8.11 gilt

$$|\text{SU}(3, 2)| = 2^3(2^2 - 1)(2^3 + 1) = 8 \cdot 27$$

und $|\text{PSU}(3, 2)| = 72$. Insbesondere ist $\text{PSU}(3, 2)$ auflösbar. Genauer gilt $\text{PSU}(3, 2) \cong M_9 \cong C_3^2 \rtimes Q_8$ (Aufgabe 33). Der folgende GAP-Code zeigt $\text{PSU}(4, 2) \cong \text{PSp}(4, 3)$:

$G := \text{PSU}(4, 2);$
 $H := \text{PSp}(4, 3);$
 $\text{IsomorphismGroups}(G, H);$

Bemerkung 8.14. Wie im Beweis von Lemma 8.12 zeigt man, dass jeder unitäre Raum V der Dimension ≥ 2 ein hyperbolisches Paar (u, v) besitzt, d. h. $u, v \in V_0$ und $[u, v] = 1$ (Definition 7.6).

Satz 8.15 (WITT). *Sei V ein unitärer Raum, $U \leq V$ und $\sigma: U \rightarrow V$ eine Isometrie. Dann existiert ein $\tau \in \text{GU}(V)$ mit $\tau|_U = \sigma$.*

Beweis. Induktion nach $\dim U$. O. B. d. A. sei $U \neq 0$. Sei $W \leq U$ mit $\dim(U/W) = 1$. Nach Induktion existiert ein $\tau \in \text{GU}(V)$ mit $\tau|_W = \sigma|_W$. Indem wir σ durch $\tau|_U^{-1}\sigma$ ersetzen, können wir $\sigma|_W = \text{id}_W$ annehmen. O. B. d. A. sei $\sigma \neq \text{id}_U$. Dann ist $R := (\sigma - \text{id}_U)(U) \leq V$ 1-dimensional. Für $u, v \in U$ gilt

$$[\sigma(u), \sigma(v) - v] = [\sigma(u), \sigma(v)] - [\sigma(u), v] = [u, v] - [\sigma(u), v] = [u - \sigma(u), v]. \quad (8.1)$$

Dies zeigt $W \subseteq R^\perp$.

Fall 1: $U \not\subseteq R^\perp$.

Sei $R^\perp = W \oplus Y$. Aus Dimensionsgründen gilt $V = U + R^\perp = U + W + Y = U \oplus Y$. Für $u \in U$ und $y \in Y$ ist $[\sigma(u) - u, y] = 0$, d. h. $[\sigma(u), y] = [u, y]$. Daraus folgt leicht, dass die Abbildung $V \rightarrow V$, $u + y \mapsto \sigma(u) + y$ eine unitäre Fortsetzung von σ ist.

Fall 2: $U \subseteq R^\perp$.

Aus (8.1) folgt $\sigma(U) \subseteq R^\perp$. Angenommen $\sigma(U) \neq U$. Dann ist $W = \sigma(W) = U \cap \sigma(U)$. Wähle $u \in U \setminus W$ und $v \in \sigma(U) \setminus W$. Für $U_0 := \langle u + v \rangle$ gilt

$$U + \sigma(U) = U \oplus U_0 = \sigma(U) \oplus U_0.$$

Sei $R^\perp = (U + \sigma(U)) \oplus Y$ und $S := U_0 + Y$. Dann gilt $R^\perp = U \oplus S = \sigma(U) \oplus S$. Im Fall $\sigma(U) = U$ kann man ein beliebiges Komplement S von U in R^\perp wählen. In beiden Fällen zeigt (8.1), dass

$$R^\perp \rightarrow R^\perp, \quad u + s \mapsto \sigma(u) + s$$

für $u \in U$ und $s \in S$ eine Isometrie ist. Wir können daher $U = R^\perp = \sigma(U)$ annehmen. Sei $R = \langle x \rangle \subseteq U$. Dann gilt $[x, x] = 0$. Sei $v \in V \setminus R^\perp$. Dann ist $T := \langle x, v \rangle$ ein unitärer Raum. Wir können v durch ein geeignetes Element in T ersetzen, sodass (x, v) ein hyperbolisches Paar ist (Bemerkung 8.14). Wegen $T^\perp \subseteq x^\perp = R^\perp = U$ ist

$$U = \langle x \rangle \oplus T^\perp = \langle \sigma(x) \rangle \oplus \sigma(T^\perp).$$

Es folgt $\dim(\langle v \rangle + \sigma(T^\perp)) = \dim(V) - 1$. Wähle $w \in V$ mit $\langle v \rangle + \sigma(T^\perp) = w^\perp$. Wegen $\langle v \rangle + \langle \sigma(x) \rangle + \sigma(T^\perp) = \langle v \rangle + U = V$ ist $\sigma(x) \notin w^\perp$. Daraus ergibt sich $w \notin U$, denn $U = \sigma(U) = \sigma(x^\perp) = \sigma(x)^\perp$. Da $\langle \sigma(x), w \rangle$ ein unitärer Raum ist, können wir w abändern, sodass $(\sigma(x), w)$ ein hyperbolisches Paar ist. Anschließend gilt weiterhin $\sigma(T^\perp) \subseteq \langle \sigma(x), w \rangle^\perp$.

Wir definieren die lineare Abbildung $\tau: V \rightarrow V$, $u + \lambda v \mapsto \sigma(u) + \lambda w$ für $u \in U$ und $\lambda \in K$. Wegen

$$[x, v] = 1 = [\sigma(x), w], \quad [y, v] = 0 = [\sigma(y), w], \quad [v, v] = 0 = [w, w]$$

für alle $y \in T^\perp$ ist $\tau \in \text{GU}(V)$ eine Fortsetzung von σ . □

Lemma 8.16. *Sei V ein unitärer Raum und $v, w \in V$ linear unabhängig mit $[v, v] = [w, w] = 1$. Genau dann gilt $V = \langle v, w \rangle \oplus \langle v, w \rangle^\perp$, wenn $[v, w][w, v] \neq 1$.*

Beweis. Sei $\lambda := [v, w]$. Seien $a, b \in K$ mit $u := av + bw \in \langle v, w \rangle^\perp$. Dann gilt $0 = [u, v] = a + b\bar{\lambda}$ und $0 = [u, w] = a\lambda + b$. Es folgt $a = -b\bar{\lambda} = a\lambda\bar{\lambda}$. Dies zeigt $u = 0$ oder $\lambda\bar{\lambda} = 1$. Gilt umgekehrt $\lambda\bar{\lambda} = 1$, so ist $v - \lambda w \in \langle v, w \rangle^\perp$. \square

Definition 8.17. Sei $v \in V_0$ und $\lambda \in K$ mit $\lambda + \bar{\lambda} = 0$. Man nennt die lineare Abbildung

$$t_{\lambda,v}: V \rightarrow V, \quad x \mapsto x + \lambda[x, v]v$$

eine (unitäre) *Transvektion*.

Bemerkung 8.18. Für $v, x \in V$ und $\lambda, \mu \in K$ gilt

$$t_{\lambda,v}(t_{\mu,v}(x)) = t_{\lambda,v}(x + \mu[x, v]v) = x + \mu[x, v]v + \lambda[x + \mu[x, v]v, v]v = t_{\lambda+\mu,v}(x).$$

Insbesondere ist $t_{\lambda,v}$ invertierbar mit $t_{\lambda,v}^{-1} = t_{-\lambda,v}$. Für $p := \text{char } K$ ist außerdem $t_{\lambda,v}^p = t_{p\lambda,v} = t_{0,v} = \text{id}_V$. Aus $\lambda + \bar{\lambda} = 0$ folgt

$$[t_{\lambda,v}(x), t_{\lambda,v}(y)] = [x, y] + \lambda[x, v][v, y] + \bar{\lambda}[y, v][x, v] = [x, y]$$

und $t_{\lambda,v} \in \text{GU}(V)$. Wie im Beweis von Satz 8.11 ist $\det(t_{\lambda,v})^{q+1} = 1$. Andererseits ist $\det(t_{\lambda,v})^p = \det(t_{\lambda,v}^p) = \det(\text{id}_V) = 1$. Dies zeigt $t_{\lambda,v} \in \text{SU}(V)$. Für $g \in \text{GU}(V)$ gilt $gt_{\lambda,v}g^{-1} = t_{\lambda,g(v)}$ wie in Bemerkung 7.11. Für $\mu \in K^\times$ ist

$$t_{\lambda,\mu v}(x) = x + \lambda[x, \mu v]\mu v = x + \lambda\mu\bar{\mu}[x, v]v = t_{v,\lambda\mu\bar{\mu}}(x)$$

mit $\lambda\mu\bar{\mu} + \bar{\lambda}\bar{\mu}\mu = 0$.

Lemma 8.19. Sei $n \geq 2$ und $(n, q) \neq (3, 2)$. Dann wird $\text{SU}(n, q)$ von allen Transvektionen erzeugt.

Beweis. Sei $V := K^n$.

Fall 1: $n = 2$.

Nach dem Beweis von Lemma 8.12 existiert eine Basis $\{v, w\}$ von V , sodass $\text{SU}(V)$ aus den Matrizen in $\text{SL}(2, q)$ besteht. Nach GT-Lemma 10.8 wird $\text{SL}(2, q)$ von den Elementarmatrizen der Form $1_2 + \lambda E_{ij}$ mit $\lambda \in \mathbb{F}_q$ und $i \neq j$ erzeugt. Es genügt zu zeigen, dass diese Matrizen unitären Transvektionen entsprechen. O. B. d. A. sei $(i, j) = (1, 2)$. Sei $\mu := [w, v] = -[v, w] \in K$ (siehe Beweis von Lemma 8.12). Es gilt $\mu^{-1} = -\bar{\mu}^{-1} = -\mu^{-q} = -\bar{\mu}^{-1}$ und $\lambda\mu^{-1} + \lambda\bar{\mu}^{-1} = \lambda(\mu^{-1} + \bar{\mu}^{-1}) = 0$. Daher ist $t := t_{\lambda\mu^{-1}, v}$ eine Transvektion mit

$$t(v) = v, \quad t(w) = w + \lambda\mu^{-1}[w, v]v = w + \lambda v.$$

Also entspricht t der Matrix $1_2 + \lambda E_{12}$.

Für die Induktion nach n benötigen wir zusätzlich, dass $\text{SU}(V)$ transitiv auf V_1 operiert. Für $u, v \in V_1$ existiert nach Witt ein $\alpha \in \text{GU}(V)$ mit $\alpha(u) = v$. Sei $d := \det(\alpha)$ und $u^\perp = \langle w \rangle$. Wir definieren $\beta \in \text{GU}(V)$ durch $\beta(u) = u$ und $\beta(w) = d^{-1}w$. Dann ist $\alpha\beta \in \text{SU}(V)$ mit $\alpha\beta(u) = v$.

Fall 2: $n \geq 3$.

Sei e_1, \dots, e_n die Standardbasis von V . Sei $\alpha \in \text{SU}(V)$. Dann ist $v := \alpha(e_1)$ ein normierter Vektor.

Schritt 1: Es existiert ein Produkt τ von Transvektionen mit $\tau(e_1) = v$.

Sind e_1 und v linear abhängig, so existiert nach dem ersten Teil des Beweises ein Produkt τ' von Transvektionen in $\langle e_1, e_2 \rangle$ mit $\tau'(e_1) = v$. Nach Lemma 8.16 lässt sich τ' zu einem Produkt von Transvektionen auf V fortsetzen. Wir können daher annehmen, dass e_1 und v linear unabhängig sind.

Nehmen wir nun an, dass $U := \langle e_1, v \rangle^\perp$ einen Vektor u mit $[u, u] \neq 0$ besitzt. Nach Normierung ist $[u, u] = 1$. Nach Lemma 8.16 existieren Produkte von Transvektionen $\tau' \in \text{SU}(\langle e_1, u \rangle)$ und $\tau'' \in \text{SU}(\langle u, v \rangle)$ mit $\tau'(e_1) = u$ und $\tau''(u) = v$. Wieder kann man τ' und τ'' nach V fortsetzen. Dann hat $\tau = \tau''\tau'$ die gewünschte Eigenschaft.

Wir dürfen daher $[u, u] = 0$ für alle $u \in U$ voraussetzen. Wegen $e_1 \in U^\perp \setminus U$ ist dann $U \subsetneq U^\perp$. Aus $n - 2 = \dim U < \dim U^\perp = 2$ folgt $n = 3$. Nach Voraussetzung ist $q \geq 3$. Gilt $v_i \bar{v}_i = [v, e_i][e_i, v] \neq 1$ für ein $i \in \{1, 2, 3\}$, so kann man wie zuvor e_1 auf e_i und e_i auf v mittels Transvektionen abbilden. Wir können also $v_i \bar{v}_i = 1$ für $i = 1, 2, 3$ annehmen. Wegen $1 = [v, v] = 1 + 1 + 1$ ist nun q gerade. Es existieren $\lambda, \mu \in \mathbb{F}_q^\times$ mit $\lambda^2 + \mu^2 = (\lambda + \mu)^2 = 1$. Für $u := (0, \lambda, \mu) \in V_1$ gilt

$$[u, v][v, u] = (\lambda \bar{v}_2 + \mu \bar{v}_3)(\lambda v_2 + \mu v_3) = \lambda^2 + \mu^2 + \lambda \mu (v_2 \bar{v}_3 + \bar{v}_2 v_3) = 1 + \lambda \mu (v_2 \bar{v}_3 + \bar{v}_2 v_3).$$

Angenommen es gilt $v_2 \bar{v}_3 + \bar{v}_2 v_3 = 0$. Wegen $2 \mid q$ ist $v_2^2 = v_2^2 v_3 \bar{v}_3 = v_2 \bar{v}_2 v_3^2 = v_3^2$ und $v_2 = v_3$. Da wir v auf $w := \alpha(e_2)$ mittels Transvektionen abbilden können, dürfen wir die Bedingungen an v auch auf w übertragen. Es gilt also auch $w_2 = w_3$. Nun wäre aber $[v, w] = v_1 \bar{w}_1 \neq 0$. Dieser Widerspruch zeigt $[u, v][v, u] \neq 1$. Man kann also e_1 auf u und u auf v mittels Transvektionen abbilden.

Schritt 2: α ist ein Produkt von Transvektionen.

Für $\beta := \tau^{-1}\alpha \in \text{SU}(V)$ gilt $\beta(e_1) = e_1$. Daher operiert β auf $U := \langle e_2, \dots, e_n \rangle = e_1^\perp$. Durch Induktion nach n ist β_U ein Produkt von Transvektionen, die man nach V fortsetzen kann. Daher ist auch α ein Produkt von Transvektionen. \square

Beispiel 8.20. Jede Transvektion in $\text{SU}(3, 2)$ hat Ordnung $q = 2$ nach Bemerkung 8.18. Nach Aufgabe 33 erzeugen die Transvektionen in $\text{SU}(3, 2)$ eine echte Untergruppe der Ordnung 54.

Lemma 8.21. Für $n \geq 2$ operiert $\text{PSU}(n, q)$ treu und primitiv auf $\Omega := \{\langle v \rangle : v \in V_0 \setminus \{0\}\}$.

Beweis. Sei $V := K^n$. Offenbar operiert $\text{SU}(V)$ durch ${}^A\langle v \rangle = \langle Av \rangle$ auf Ω . Nach Lemma 8.9 liegt $Z(\text{SU}(V))$ im Kern der Operation. Sei umgekehrt A im Kern. Wie im Beweis von Lemma 8.12 konstruiert man $u, v \in V_0$ mit $[u, v] = -[v, u]$. Sei $Au = \lambda_1 u$ und $Av = \lambda_2 v$. Wegen $u + v \in V_0$ gilt

$$\lambda_1 u + \lambda_2 v = A(u + v) \in \langle u + v \rangle.$$

Dies zeigt $\lambda := \lambda_1 = \lambda_2$. Sei $U := \langle u, v \rangle^\perp$. Wegen $V = U \oplus U^\perp$ ist U ein unitärer Raum. Durch Induktion nach n existiert $\mu \in K$ mit $A|_U = \mu \text{id}_U$. Sei $w \in V_0 \cap U$. Aus $u + w \in V_0$ folgt $\lambda = \mu$ und $A = \lambda 1_n \in Z(\text{SU}(V))$. Also operiert $\text{PSU}(V)$ treu auf Ω .

Sei $v \in V_0 \setminus \{0\}$ mit o. B. d. A. $v_1 v_2 \neq 0$. Bekanntlich existieren $q + 1$ Elemente $\lambda \in K$ mit $\lambda^{q+1} = \lambda \bar{\lambda} = -1$. Insbesondere existiert ein solches λ mit $v_1 + \lambda v_2 \neq 0$. Dann ist $u := (1, \bar{\lambda}, 0, \dots, 0) \in V_0$ und $[v, u] \neq 0$. Durch Skalierung von v erreicht man $[u, v] = -[v, u]$. Nun ist $U := \langle u, v \rangle$ ein unitärer Raum mit $\text{SU}(U) \cong \text{SL}(2, q)$ (Lemma 8.12). Es existiert ein $A \in \text{SU}(U)$ mit $\langle Av \rangle = \langle u \rangle$. Wegen $V = U \oplus U^\perp$ kann man A nach $\text{SU}(V)$ fortsetzen, indem man trivial auf U^\perp operiert. Sei $\mu \neq \lambda$ mit $\mu \bar{\mu} = -1$. Dann ist $w := (1, \bar{\mu}) \in V_0$ mit $[u, w] = 1 + \bar{\lambda} \mu \neq 0$. Also existiert ein $B \in \text{SU}(\langle u, w \rangle)$ mit $\langle Bu \rangle = \langle w \rangle$. Wieder lässt sich B nach V fortsetzen. Dies zeigt, dass $\text{PSU}(V)$ transitiv auf Ω operiert.

Zum Nachweis der Primitivität sei zunächst $n = 2$ und $V = \langle u, v \rangle$ mit $u, v \in V_0$ und $[u, v] = -[v, u]$. Jedes Element in $\Omega \setminus \langle v \rangle$ wird erzeugt von einem Vektor $w := u + \lambda v \in V_0$ mit $\lambda \in K$. Dann gilt

$$0 = [w, w] = \lambda[v, u] + \bar{\lambda}[u, v] = (\lambda - \bar{\lambda})[v, u],$$

d. h. $\lambda = \bar{\lambda} \in \mathbb{F}_q$. Also besteht Ω genau aus den 1-dimensionalen Unterräumen von $\mathbb{F}_q u + \mathbb{F}_q v$. Mittels des Isomorphismus $\mathrm{SU}(V) \cong \mathrm{SL}(2, q)$ operiert $\mathrm{SU}(V)$ sogar 2-transitiv auf Ω (GT-Lemma 10.7). Sei nun $n \geq 3$. Angenommen es existiert ein Block $\Delta \subseteq \Omega$. Seien $\langle u \rangle, \langle v \rangle \in \Delta$ verschieden.

Fall 1: $[u, v] \neq 0$.

Sei auch $w \in V_0$ mit $[u, w] \neq 0$. Nach Skalierung können wir $[u, v] = [u, w]$ annehmen. Dann existiert eine Isometrie $\alpha: \langle u, v \rangle \rightarrow \langle u, w \rangle$ mit $\alpha(u) = u$ und $\alpha(v) = w$. Nach Witt lässt sich α zu $\alpha \in \mathrm{GU}(V)$ fortsetzen. Für $d := \det(\alpha)$ gilt $d^{q+1} = d\bar{d} = 1$, d. h. $d = \zeta^{(q-1)a}$ für ein $a \in \mathbb{Z}$. Wir definieren $U := \langle u, v \rangle$ und $\beta \in \mathrm{GL}(U)$ mit $\beta(u) = \zeta^{-qa}u$ und $\beta(v) = \zeta^a v$. Wegen

$$[\beta(u), \beta(v)] = \zeta^{-qa+qa}[u, v] = [u, v]$$

ist $\beta \in \mathrm{GU}(U)$ mit $\det(\beta) = \zeta^{-qa+a} = d^{-1}$. Wegen $V = U \oplus U^\perp$ können wir β als $\beta + \mathrm{id}_{U^\perp}$ nach $\mathrm{GU}(V)$ fortsetzen. Dann ist $\alpha\beta \in \mathrm{SU}(V)$ mit $\alpha\beta(u) \in \langle u \rangle$ und $\alpha\beta(v) \in \langle w \rangle$. Daher enthält Δ alle $\langle v \rangle$ mit $[u, v] \neq 0$.

Sei nun $\langle w \rangle \in \Omega$ mit $w \in u^\perp$. Da V nicht die Vereinigung zweier echter Unterräume ist, existiert ein $x \in V \setminus (u^\perp \cup w^\perp)$. Nach Skalierung sei $[x, u] = 1$. Da die Spur transitiv ist, existiert ein $\lambda \in K$ mit $\lambda + \bar{\lambda} = -[x, x]$ ($\in \mathbb{F}_q$). Für $x' := x + \lambda u$ gilt

$$[x', x'] = [x, x] + (\lambda + \bar{\lambda})[u, x] = 0,$$

d. h. $x' \in V_0$. Wegen $u \in w^\perp$ gilt $x' \notin u^\perp \cup w^\perp$. Aus $x' \notin u^\perp$ folgt $\langle x' \rangle \in \Delta$. Aus $w \notin (x')^\perp$ ergibt sich $\langle w \rangle \in \Delta$. Dies liefert den Widerspruch $\Delta = \Omega$.

Fall 2: $[u, v] = 0$.

Sei $x \in u^\perp \setminus v^\perp$ mit $[x, v] = 1$. Sei $\lambda \in K$ mit $\lambda + \bar{\lambda} = -[x, x]$. Für $x' := x + \lambda v \in u^\perp \setminus v^\perp$ gilt $[x', x'] = 0$ wie in Fall 1. Nun ist $U := \langle x', v \rangle$ ein unitärer Raum. Es existiert ein $\alpha \in \mathrm{SU}(V)$ mit $\alpha(U) = U$, $\alpha(v) \in \langle x' \rangle$ und $\alpha|_{U^\perp} = \mathrm{id}_{U^\perp}$. Wegen $u \in U^\perp$ ist $\langle u \rangle = \langle \alpha(u) \rangle \in \Delta \cap \alpha(\Delta) = \Delta$. Dies zeigt $\langle x' \rangle = \langle \alpha(v) \rangle \in \Delta$. Aus Fall 1 erhält man den Widerspruch $\Delta = \Omega$. \square

Bemerkung 8.22. Nach Lemma 8.10 gilt $z_3 = q^5 - q^2(q-1) = (q^2-1)(q^3+1) + 1$. Daher ist $G := \mathrm{PSU}(3, q)$ eine primitive Gruppe vom Grad $|\Omega| = \frac{z_3-1}{|K^\times|} = q^3 + 1$.

Lemma 8.23. Für $n \geq 3$ und $(n, q) \neq (3, 2)$ ist $\mathrm{SU}(n, q)$ perfekt.

Beweis. Nach Lemma 8.19 genügt es zu zeigen, dass jede unitäre Transvektion $t := t_{\lambda, u}$ ein Produkt von Kommutatoren ist. Sei $v \in V \setminus u^\perp$, sodass (u, v) ein hyperbolisches Paar ist. Dann ist $U := \langle u, v \rangle$ ein unitärer Raum und $t|_{U^\perp} = \mathrm{id}_{U^\perp}$ wegen $U^\perp \subseteq u^\perp$. Nach Lemma 8.12 ist $t|_U \in \mathrm{SU}(U) \cong \mathrm{SL}(2, q)$.

Sei zunächst $q \geq 4$. Nach GT-Lemma 10.9 ist $\mathrm{SL}(2, q)$ perfekt. Also ist $t|_U$ ein Produkt von Kommutatoren $[x, y] \in \mathrm{SU}(U)$. Wie üblich kann man x und y nach V fortsetzen, indem man trivial auf U^\perp operiert. Daher ist $[x, y]$ die Einschränkung eines Kommutators $c \in \mathrm{SU}(V)$ mit $c|_{U^\perp} = \mathrm{id}_{U^\perp}$. Also ist t ein Produkt von Kommutatoren.

Sei nun $q = 3$. Mit U ist auch U^\perp ein unitärer Raum. Daher existiert ein $w \in U^\perp$ mit $[w, w] = 1$. Sei $W := \langle u, v, w \rangle$. Wie im ersten Teils des Beweises genügt es zu zeigen, dass $t|_W \in \mathrm{SU}(W)$ ein Produkt von Kommutatoren ist. Sei $\mu \in K$ mit $\mu\bar{\mu} = -1$. Bzgl. der Basis $\{u, v, w\}$ ist $d := \mathrm{diag}(\mu, -\mu, -\mu^{-2}) \in \mathrm{SU}(W)$. Es gilt

$$t|_W = \begin{pmatrix} 1 & \lambda & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda/2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} d \begin{pmatrix} 1 & \lambda/2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} d^{-1} = [t_{\lambda/2, u}, d] \in \mathrm{SU}(W)'.$$

Sei schließlich $q = 2$ und $n \geq 4$. Wir wählen ein hyperbolisches Paar (u', v') mit $u', v' \in U^\perp$. O.B.d.A. sei $V = U \oplus \langle u', v' \rangle$.¹⁴ Aus $\lambda + \bar{\lambda} = 0$ folgt $\lambda = \bar{\lambda} \in \mathbb{F}_2$. Im Fall $\lambda = 0$ ist $t = \text{id}_V$ ein Kommutator. Sei also $\lambda = 1$. Sei $K^\times = \langle \zeta \rangle$ und $x, y \in \text{GL}(V)$ mit

$$\begin{aligned} x(u) &:= u, & x(u') &:= u', & x(v) &:= v + \zeta^2 u', & x(v') &:= \zeta u + v', \\ y(u) &:= u, & y(u') &:= \zeta^2 u + u', & y(v) &:= v + \zeta v', & y(v') &:= v' \end{aligned}$$

Wegen $\zeta + \zeta^2 = 1$ ist $x, y \in \text{SU}(V)$ und $x^2 = 1, y^2 = 1$. Für $z := [x, y]$ gilt

$$\begin{aligned} z(u) &= u, \\ z(u') &= xy(\zeta^2 u + u') = \zeta^2 u + \zeta^2 u + u' = u', \\ z(v) &= xyx(v + \zeta v') = xy(v + \zeta^2 u' + \zeta^2 u + \zeta v') = x(v + \zeta v' + \zeta u + \zeta^2 u' + \zeta^2 u + \zeta v') \\ &= x(u + v + \zeta^2 u') = u + v, \\ z(v') &= xy(\zeta u + v') = \zeta u + \zeta u + v' = v'. \end{aligned}$$

Dies zeigt $t = z \in \text{SU}(V)'$. □

Satz 8.24. Für $n \geq 3$ und $(n, q) \neq (3, 2)$ ist $\text{PSU}(n, q)$ einfach.

Beweis. Sei $V = K^n$. Wir identifizieren die Elemente in $\text{SU}(V)$ mit ihren Nebenklassen in $G := \text{PSU}(V)$. Nach Lemma 8.21 ist G eine primitive Permutationsgruppe auf $\Omega = \{\langle v \rangle : v \in V_0 \setminus \{0\}\}$. Nach Lemma 8.23 ist G perfekt. Sei $v \in V_0$ und

$$K_0 := \{\lambda \in K : \lambda + \bar{\lambda} = 0\} \cong \mathbb{F}_q$$

der Kern der Spur. Nach Bemerkung 8.18 ist $A := \{t_{\lambda, v} : \lambda \in K_0\} \leq G$ eine elementarabelsche p -Gruppe, wobei $p := \text{char } K$. Für $g \in G_{\langle v \rangle}$ existiert ein $\mu \in K$ mit $g(v) = \mu v$. Nach Bemerkung 8.18 gilt

$$gt_{\lambda, v}g^{-1} = t_{\lambda, g(v)} = t_{\lambda, \mu v} = t_{\lambda\mu\bar{\mu}, v} \in A.$$

Dies zeigt $A \trianglelefteq G_{\langle v \rangle}$. Sei $w \in V_0 \setminus \{0\}$ beliebig. Da G transitiv auf Ω operiert, existiert ein $g \in G$ mit $g(v) \in \langle w \rangle$. Daher enthält $A^G := \langle gAg^{-1} : g \in G \rangle$ alle unitären Transvektionen. Aus Lemma 8.19 folgt $A^G = G$. Nach Iwasawas Lemma aus der Gruppentheorie ist G einfach. □

Beispiel 8.25. Die kleinste einfache Gruppe, die wir bislang noch nicht kannten, ist $\text{SU}(3, 3) = \text{PSU}(3, 3)$ mit Ordnung $3^3(3^2 - 1)(3^3 + 1) = 2^5 \cdot 3^3 \cdot 7 = 6048$.

Bemerkung 8.26. Wall hat gezeigt, dass eine Matrix $A \in \text{GL}(n, q^2)$ genau dann zu einem Element aus $\text{GU}(n, q)$ konjugiert, wenn A und \bar{A}^{-1} ähnlich sind (also in $\text{GL}(n, q^2)$ konjugiert). Außerdem sind Matrizen aus $\text{GU}(n, q)$ genau dann in $\text{GU}(n, q)$ konjugiert, wenn sie ähnlich sind.

Beispiel 8.27.

- (i) Sei $A \in \text{GL}(n, q)$ eine obere Dreiecksmatrix mit Einsen auf der Hauptdiagonale. Wegen $A^{q^n} - 1_n = (A - 1_n)^{q^n} = 0$ sind alle Eigenwerte von A gleich 1. Nach der Jordanschen Normalform ist die Ähnlichkeitsklasse von A durch $\text{rk}((A - 1_n)^k)$ für $k = 1, \dots, n$ eindeutig bestimmt. Wir zeigen $\text{Ker}((A - 1_n)^k) = \text{Ker}((A^{-1} - 1_n)^k)$ für $k = 1, \dots, n$. Für $k = 1$ gilt

$$x \in \text{Ker}(A - 1_n) \iff Ax = x \iff A^{-1}x = x \iff x \in \text{Ker}(A^{-1} - 1_n).$$

¹⁴Man könnte nun $\text{PSU}(4, 2) \cong \text{PSp}(4, 3)$ und Lemma 7.14 benutzen.

Sei nun die Behauptung für k bereits bewiesen. Für $x \in \text{Ker}((A - 1_n)^{k+1})$ gilt induktiv

$$\begin{aligned}(A - 1_n)^k(A - 1_n)x = 0 &\implies (A^{-1} - 1_n)^k(A - 1_n)x = 0 \implies (A - 1_n)(A^{-1} - 1_n)^kx = 0 \\ &\implies (A^{-1} - 1_n)(A^{-1} - 1_n)^kx = 0 \implies x \in \text{Ker}((A^{-1} - 1_n)^{k+1}).\end{aligned}$$

Also besitzen A und $A^{-1} = \overline{A}^{-1}$ die gleiche Jordansche Normalform. Nach Wall ist A zu einer unitären Matrix ähnlich.

- (ii) Bekanntlich bilden die oberen Dreiecksmatrizen mit Einsen auf der Hauptdiagonale eine p -Sylowgruppe P von $\text{GL}(n, q)$, wobei $p \mid q$. Für eine p -Sylowgruppe Q von $\text{GU}(n, q)$ gilt $|Q| = |P|$ nach Satz 8.11. Obwohl nach (i) jedes Element aus P zu einem Element aus Q konjugiert ist, sind P und Q im Allgemeinen nicht isomorph. Für $(n, q) = (3, 2)$ ist $P \cong D_8$ und $Q \cong Q_8$ nach Aufgabe 33.

Bemerkung 8.28. Zu den sogenannten *klassischen* Gruppen vom Lie-Typ fehlt uns noch nur die Familie der *orthogonalen* Gruppen. Hierfür betrachtet man einen n -dimensionalen \mathbb{F}_q -Vektorraum V mit einer nicht-ausgearteten *quadratischen Form* $\rho: V \rightarrow K$, d. h. es gilt $\rho(\lambda v) = \lambda^2 \rho(v)$ für $\lambda \in \mathbb{F}_q$, $v \in V$ und

$$\beta: V \times V \rightarrow K, \quad (u, v) \mapsto \rho(u + v) - \rho(u) - \rho(v)$$

ist eine (symmetrische) nicht-ausgeartete Bilinearform. Ist q ungerade, so ist ρ durch β eindeutig bestimmt, denn

$$\rho(v) = \frac{1}{2} \left(4\rho(v) - \rho(v) - \rho(v) \right) = \frac{1}{2} \left(\rho(v + v) - \rho(v) - \rho(v) \right) = \frac{1}{2} \beta(v, v).$$

In diesem Fall braucht man ρ nicht und kann wie gewohnt mit β arbeiten. Im Allgemeinen hängt der Isomorphietyp der *allgemeinen orthogonalen Gruppe*

$$\text{GO}(n, q, \rho) := \{ f \in \text{GL}(V) : \forall v \in V : \rho(f(v)) = \rho(v) \}$$

von ρ ab. Der Einfachheit halber nehmen wir an, dass q ungerade ist. Dann gibt es genau zwei nicht-äquivalente Bilinearformen β (Aufgabe 34). Falls n ungerade ist, so hängt der Isomorphietyp von $\text{GO}(n, q, \rho)$ nicht von ρ bzw. β ab. Man kann dann β mit dem gewöhnlichen „euklidischen“ Skalarprodukt identifizieren und

$$\text{GO}(n, q) := \text{GO}(n, q, \rho) \cong \{ A \in \text{GL}(n, q) : A^t A = 1_n \}$$

definieren (für gerades q gilt $\text{GO}(2n + 1, q) \cong \text{Sp}(2n, q)$). Ist n gerade, so definiert man $\text{GO}^+(n, q)$ und $\text{GO}^-(n, q)$ entsprechend der Wahl von β . Im Gegensatz zu den bisherigen Gruppen, sind die abgeleiteten Gruppen PSO , PSO^+ und PSO^- in der Regel nicht einfach, sondern besitzen eine einfache Untergruppe $\text{P}\Omega$ (bzw. $\text{P}\Omega^+$, $\text{P}\Omega^-$) vom Index 2 (Kern der *Spinornorm*). Diese Gruppen liefern erst für $n \geq 7$ „neue“ Familien von einfachen Gruppen, denn

$$\begin{array}{lll} \text{P}\Omega(3, q) \cong \text{PSL}(2, q), & \text{P}\Omega^+(4, q) \cong \text{PSL}(2, q)^2, & \text{P}\Omega^-(4, q) \cong \text{PSL}(2, q^2), \\ \text{P}\Omega(5, q) \cong \text{PSp}(4, q), & \text{P}\Omega^+(6, q) \cong \text{PSL}(4, q), & \text{P}\Omega^-(6, q) \cong \text{PSU}(4, q). \end{array}$$

Die kleinsten Gruppen dieser Art sind $\text{P}\Omega^+(8, 2)$, $\text{P}\Omega^-(8, 2)$ und $\text{P}\Omega(7, 3)$ mit Ordnungen 174.182.400, 197.406.720 und 4.585.351.680.

9 Sporadische Gruppen

Bemerkung 9.1. Nach der Klassifikation der endlichen einfachen Gruppen (CFSG) gibt es neben C_p , A_n und den Gruppen vom Lie-Typ noch 26 *sporadische* Gruppen, die zu keiner der Familien gehören. Wir konstruieren in diesem Kapitel fünf sporadischen Gruppen, die gleichzeitig interessante mehrfach-transitive Gruppen sind. Wir wählen zuerst einen möglichst direkten Weg mit einem „maßgeschneiderten“ Lemma von Witt. Anschließend beschreiben wir einen kombinatorischen Ansatz, mit dem auch andere sporadische Gruppen konstruiert werden können.

Definition 9.2. Eine k -transitive Operation $G \rightarrow \text{Sym}(\Omega)$ heißt *scharf k -transitiv*, wenn für zwei k -Tupel $(\alpha_1, \dots, \alpha_k)$ und $(\beta_1, \dots, \beta_k)$ mit paarweise verschiedenen Elementen *genau* ein $g \in G$ mit ${}^g\alpha_i = \beta_i$ für $i = 1, \dots, k$ existiert.

Bemerkung 9.3. Jede scharf k -transitive Operation ist treu. Die scharf 1-transitiven Operationen sind genau die regulären Operationen. Sei $G \rightarrow \text{Sym}(\Omega)$ transitiv, $\omega \in \Omega$ und $k \geq 2$. Wie in GT-Lemma 6.33 zeigt man, dass G genau dann scharf k -transitiv auf Ω operiert, wenn G_ω scharf $(k-1)$ -transitiv auf $\Omega \setminus \{\omega\}$ operiert. Induktiv erhält man, dass eine k -transitive Operation vom Grad n genau dann scharf k -transitiv ist, wenn $|G| = n(n-1) \dots (n-k+1)$ gilt (vgl. GT-Lemma 6.34).

Beispiel 9.4.

- (i) Die natürliche Operation der S_n auf $\{1, \dots, n\}$ ist scharf n -transitiv und scharf $(n-1)$ -transitiv, falls $n \geq 2$.
- (ii) Die natürliche Operation von A_n ist scharf $(n-2)$ -transitiv, falls $n \geq 2$ (siehe GT-Beispiel 6.32).
- (iii) Sei $n \in \mathbb{N}$, p eine Primzahl und $S \leq \text{GL}(n, p)$ ein Singer-Zyklus (GT-Beispiel 6.23). Dann ist $\mathbb{F}_p^n \rtimes S \leq \text{AGL}(n, p)$ eine scharf 2-transitive Permutationsgruppe auf \mathbb{F}_p^n .
- (iv) Nach GT-Aufgabe 47 operiert $\text{SL}(2, 2^n)$ 3-transitiv auf der Menge Ω aller 1-dimensionalen Unterräume von $\mathbb{F}_{2^n}^2$. Wegen $|\Omega| = 2^n + 1$ und $|\text{SL}(2, 2^n)| = (2^{2n} - 1)2^n = (2^n + 1)2^n(2^n - 1)$ ist diese Operation scharf 3-transitiv.

Lemma 9.5. Sei $\alpha, \beta \in \Omega$, $H \leq G \leq \text{Sym}(\Omega)$ und $a, x \in G$ mit folgenden Eigenschaften:

- $\alpha \neq \beta$, ${}^a\alpha \neq \alpha$ und ${}^x\beta \neq \beta$,
- $x \in H$ und $G = \langle H, a \rangle$,
- $aH_\beta a = H_\beta$,
- H operiert k -transitiv auf $\Omega \setminus \{\alpha\}$ mit $k \geq 2$,
- $a^2 = x^2 = (ax)^3 = 1$.

Dann operiert G $(k+1)$ -transitiv auf Ω und $G_\alpha = H$.

Beweis. Wegen $H \subseteq G_\alpha$ ist G_α k -transitiv auf $\Omega \setminus \{\alpha\}$. Wegen ${}^a\alpha \neq \alpha$ ist G offenbar auch transitiv auf Ω . Aus GT-Lemma 6.33 folgt, dass G $(k+1)$ -transitiv operiert. Es bleibt zu zeigen: $G_\alpha \subseteq H$.

Für $K := H \cup HaH$ ist $K^{-1} := \{g^{-1} : g \in K\} = K$ wegen $a^{-1} = a$. Sei $z \in H \setminus H_\beta$. Wegen $k \geq 2$ operiert H_β transitiv auf $\Omega \setminus \{\alpha, \beta\}$. Also existiert ein $h \in H_\beta$ mit ${}^{hz}\beta = {}^x\beta$. Es folgt $x^{-1}hz \in H_\beta$ und

$z \in H_\beta x H_\beta$. Dies zeigt $H = H_\beta \cup H_\beta x H_\beta$. Die Relationen $a^2 = x^2 = (ax)^3 = 1$ implizieren $axa = xax$. Nach Voraussetzung erhalten wir

$$\begin{aligned} aHa &= aH_\beta a \cup aH_\beta x H_\beta a = H_\beta \cup H_\beta axa H_\beta \\ &= H_\beta \cup H_\beta xax H_\beta \subseteq H \cup HaH = K. \end{aligned}$$

Für $g, g' \in HaH$ ist also $gg' \in HaHaH \subseteq HKH \subseteq K$. Dies zeigt $K \leq G$. Wegen $a \in K$ ist sogar $G = \langle H, a \rangle = K$. Für jedes $g \in G \setminus H \subseteq HaH$ ist also ${}^g\alpha \neq \alpha$. Dies zeigt die Behauptung. \square

Lemma 9.6 (WITT). *Sei H eine 2-transitive Permutationsgruppe auf $\Delta := \{4, \dots, n\} \ni \omega$ und sei $x \in H \setminus H_\omega$ eine Involution. Seien $a, b, c \in N_{S_n}(H_\omega)$ Involutionen mit*

$$a = (1, \omega)(2)(3) \dots, \quad b = (1, 2)(3)(\omega) \dots, \quad c = (2, 3)(1)(\omega) \dots$$

und

$$(ax)^3 = (ba)^3 = (cb)^3 = 1, \quad (xb)^2 = (xc)^2 = (ac)^2 = 1.$$

Dann ist $G := \langle H, a, b, c \rangle$ 5-transitiv auf $\{1, \dots, n\}$ und $G_1 \cap G_2 \cap G_3 = H$.

Beweis. Nach Lemma 9.5 mit $(\alpha, \beta) = (1, \omega)$ ist $K := \langle H, a \rangle$ 3-transitiv auf $\Delta \cup \{1\}$ und $K_1 = H$. Nach GT-Satz 6.35 operiert H primitiv auf Δ . Insbesondere ist $H_\omega < H$ maximal und $H = \langle H_\omega, x \rangle$. Aus $x^2 = (xb)^2 = b^2 = 1$ folgt $xb = bx$. Insbesondere ist $bK_1b = bHb = \langle bH_\omega b, x \rangle = \langle H_\omega, x \rangle = H = K_1$. Eine weitere Anwendung von Lemma 9.5 mit $(b, a, 2, 1)$ anstelle von (a, x, α, β) zeigt, dass $L := \langle K, b \rangle$ 4-transitiv auf $\Delta \cup \{1, 2\}$ operiert mit $L_2 = K$. Aus den Relationen folgt nun wieder $ac = ca$ und $xc = cx$. Also ist

$$cL_2c = cKc = \langle cHc, a \rangle = \langle cH_\omega c, x, a \rangle = \langle H_\omega, x, a \rangle = K = L_2.$$

Eine dritte Anwendung von Lemma 9.5 mit $(c, b, 3, 2)$ anstelle von (a, x, α, β) ergibt schließlich, dass $G = \langle L, c \rangle$ 5-transitiv auf $\{1, \dots, n\}$ operiert mit $G_3 = L$. Damit ist auch $G_1 \cap G_2 \cap G_3 = G_1 \cap L_2 = G_1 \cap K = K_1 = H$. \square

Satz 9.7 (MATHIEU). *Sei*

$$\begin{aligned} a &= (1, 4)(7, 8)(9, 11)(10, 12), & b &= (1, 2)(7, 10)(8, 11)(9, 12), \\ c &= (2, 3)(7, 12)(8, 10)(9, 11), & d &= (4, 5, 6)(7, 8, 9)(10, 11, 12), \\ e &= (4, 7, 10)(5, 8, 11)(6, 9, 12), & f &= (5, 7, 6, 10)(8, 9, 12, 11), \\ g &= (5, 8, 6, 12)(7, 11, 10, 9). \end{aligned}$$

Dann ist $M_{12} := \langle a, b, c, d, e, f, g \rangle \leq S_{12}$ scharf 5-transitiv vom Grad 12 und $M_{11} := \langle a, b, d, e, f, g \rangle$ ist scharf 4-transitiv vom Grad 11.

Beweis. Da d die drei Zyklen von e permutiert, ist $E := \langle d, e \rangle$ elementarabelsch der Ordnung 9. Außerdem operiert E regulär auf $\Delta := \{4, \dots, 12\}$. Offenbar ist $f^2 = g^2$ eine Involution und $fgf^{-1} = g^{-1}$. Für $Q := \langle f, g \rangle$ gilt also $\langle g \rangle \trianglelefteq Q$ und $|Q : \langle g \rangle| = 2$. Also ist $|Q| = 8$ (Q ist eine Quaternionengruppe). Eine Rechnung zeigt

$$\begin{aligned} fdf^{-1} &= e, & gdg^{-1} &= (4, 8, 12)(11, 6, 7)(9, 10, 5) = de, \\ fef^{-1} &= d^{-1}, & geg^{-1} &= (4, 11, 9)(8, 6, 10)(12, 7, 5) = de^{-1}. \end{aligned}$$

Also ist $Q \subseteq N_{S_{12}}(E)$ und $H := EQ \leq S_{12}$. Aus Ordnungsgründen ist $E \cap Q = 1$ und somit $|H| = |E||Q| = 9 \cdot 8$. Da E regulär auf Δ operiert, ist $H_4 = E_4Q = Q$. Man sieht leicht, dass Q transitiv auf $\Delta \setminus \{4\}$ operiert. Also ist H 2-transitiv auf Δ nach GT-Lemma 6.33. Wegen $|H| = 9 \cdot 8$ und $|\Omega| = 9$ ist die Operation sogar scharf 2-transitiv. Wir wollen nun Witts Lemma mit $\omega = 4$ und

$$x := df^2d^{-1} = d(5, 6)(7, 10)(8, 12)(9, 11)d^{-1} = (4, 6)(7, 12)(8, 11)(9, 10) \in H \setminus H_4$$

anwenden. Dafür müssen wir zunächst $a, b, c \in N_{S_{12}}(H_4) = N_{S_{12}}(Q)$ zeigen:

$$\begin{aligned}afa^{-1} &= g, & aga^{-1} &= a^2fa^{-2} = f, \\ bfb^{-1} &= f^{-1}, & bgb^{-1} &= (5, 11, 6, 9)(7, 12, 10, 8) = gf, \\ cfc^{-1} &= g^{-1}, & cgc^{-1} &= c^2f^{-1}c^{-2} = f^{-1}.\end{aligned}$$

Die Relationen aus Lemma 9.6 überprüft man wie folgt:

$$\begin{aligned}ax &= (1, 4, 6)(7, 10, 11)(8, 9, 12), & ba &= (1, 4, 2)(7, 11, 12)(8, 10, 9), \\ cb &= (1, 3, 2)(7, 8, 9)(10, 12, 11), & xb &= (1, 2)(4, 6)(7, 9)(10, 12), \\ xc &= (2, 3)(4, 6)(8, 9)(10, 11), & ac &= (1, 4)(2, 3)(7, 10)(8, 12).\end{aligned}$$

Also ist $G := \langle H, a, b, c \rangle = M_{12}$ 5-transitiv auf $\Omega = \{1, \dots, 12\}$ und $G_1 \cap G_2 \cap G_3 = H$. Da H scharf 2-transitiv auf Ω operiert, ist $G_1 \cap G_2 \cap G_3 \cap G_4 \cap G_5 = H_4 \cap H_5 = 1$. Dies zeigt, dass G sogar scharf 5-transitiv ist. Im Beweis von Lemma 9.6 ergab sich $G_3 = M_{11}$. Nach Bemerkung 9.3 ist M_{11} also scharf 4-transitiv vom Grad 11. \square

Bemerkung 9.8. In der Gruppentheorie haben wir gezeigt, dass die einfache Gruppe $H = \text{PSL}(3, 4)$ der Ordnung

$$|H| = \frac{(4^3 - 1)(4^3 - 4)(4^3 - 4^2)}{(4 - 1) \text{ggT}(3, 4 - 1)} = 2^6 \cdot 3^2 \cdot 5 \cdot 7 = 20.160$$

2-transitiv auf der Menge Δ der 21 1-dimensionalen Unterräume von \mathbb{F}_4^3 operiert (Beweis von GT-Lemma 10.7). Um Vektoren von Permutationen zu unterscheiden, schreiben wir die Elemente von \mathbb{F}_4^3 in der Form $[r, s, t]$ mit $r, s, t \in \mathbb{F}_4$. Sei außerdem $\mathbb{F}_4^\times = \langle \zeta \rangle$ und $[[r, s, t]] = \mathbb{F}_4[r, s, t] \in \Delta$.

Lemma 9.9. *Mit den Bezeichnungen aus Bemerkung 9.8 sind folgende Abbildungen Involutionen in $\text{Sym}(\Delta)$:*

$$\alpha[[r, s, t]] := [[r^2 + st, s^2, t^2]], \quad \beta[[r, s, t]] := [[r^2, s^2, t^2\zeta]], \quad \gamma[[r, s, t]] := [[r^2, s^2, t^2]]$$

für $r, s, t \in \mathbb{F}_4$.

Beweis. Da die Werte von α , β und γ homogene Polynome vom Grad 2 in r, s, t sind, hängen die Bilder von $[[r, s, t]] = \mathbb{F}_4[r, s, t]$ nicht von der Wahl des Repräsentanten $[r, s, t]$ ab (d. h. α , β , γ sind wohldefiniert). Bekanntlich ist $\mathbb{F}_4 \rightarrow \mathbb{F}_4$, $x \mapsto x^2$ der Frobenius-Automorphismus (der Ordnung 2). Daher gilt

$$\begin{aligned}\alpha^2[[r, s, t]] &= \alpha[[r^2 + st, s^2, t^2]] = [[r + s^2t^2 + s^2t^2, s, t]] = [[r, s, t]], \\ \beta^2[[r, s, t]] &= \beta[[r^2, s^2, t^2\zeta]] = [[r, s, t\zeta^2\zeta]] = [[r, s, t]], \\ \gamma^2[[r, s, t]] &= [[r, s, t]].\end{aligned}$$

Folglich sind α , β , γ invertierbar und haben Ordnung 2. \square

Satz 9.10 (MATHIEU). Sei $\text{PSL}(3, 4) \cong H \leq \text{Sym}(\Delta)$ wie in Bemerkung 9.8 und $\Omega = \Delta \dot{\cup} \{1, 2, 3\}$. Mit den Bezeichnungen aus Lemma 9.9 sei $a := (1, [1, 0, 0])\alpha$, $b := (1, 2)\beta$ und $c := (2, 3)\gamma$. Dann gilt:

- (i) $M_{22} := \langle H, a \rangle$ ist 3-transitiv auf $\Delta \cup \{1\}$.
- (ii) $M_{23} := \langle H, a, b \rangle$ ist 4-transitiv auf $\Omega \setminus \{3\}$.
- (iii) $M_{24} := \langle H, a, b, c \rangle$ ist 5-transitiv auf Ω .

Beweis. Wir benutzen Witts Lemma mit $\omega = [1, 0, 0] \in \Delta$ und

$$x := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mathbb{F}_4^\times \in \text{PSL}(3, 4).$$

Nach Lemma 9.9 sind a, b, c, x Involutionen. Offenbar ist ${}^b\omega = {}^c\omega = \omega$. Sei F der Frobenius-Automorphismus auf H (bzw. $\text{SL}(3, 4)$). Für $h \in H$ und $[r, s, t] \in \Delta$ gilt ${}^{hc}[r, s, t] = {}^c[h[r^2, s^2, t^2]] = [F(h)[r, s, t]]$. Dies zeigt $cHc^{-1} = H$ und $c \in N_{24}(H_\omega)$. Sei $y := \text{diag}(1, 1, \zeta) \in \text{GL}(3, 4)$. Dann gilt

$${}^{bhb}[r, s, t] = {}^b[h[r^2, s^2, t^2\zeta]] = [yF(h)y^{-1}[r, s, t]].$$

Wegen $yF(h)y^{-1} \in H$ ist auch $b \in \S_{24}(H_\omega)$. Außerdem gilt ${}^{aha}\omega = {}^{ah}1 = {}^a1 = \omega$. Ein Element $h \in H_\omega$ hat die Form ${}^h[r, s, t] = [r + \sigma s + \tau t, \rho_1 s + \rho_2 t, \rho_3 s + \rho_4 t]$ mit $\rho_1 \rho_4 + \rho_2 \rho_3 = \det(h) = 1$. Eine Rechnung zeigt

$$\begin{aligned} {}^{aha}[r, s, t] &= {}^{ah}[r^2 + st, s^2, t^2] = {}^a[r^2 + st + \sigma s^2 + \tau t^2, \rho_1 s^2 + \rho_2 t^2, \rho_3 s^2 + \rho_4 t^2] \\ &= [[r + s^2 t^2 + \sigma^2 s + \tau^2 t + (\rho_1 s^2 + \rho_2 t^2)(\rho_3 s^2 + \rho_4 t^2), \rho_1^2 s + \rho_2^2 t, \rho_3^2 s + \rho_4^2 t]] \\ &= [[r + (\sigma^2 + \rho_1 \rho_3)s + (\tau^2 + \rho_2 \rho_4)t, \rho_1^2 s + \rho_2^2 t, \rho_3^2 s + \rho_4^2 t]]. \end{aligned}$$

Also entspricht aha der Matrix

$$\begin{pmatrix} 1 & \sigma^2 + \rho_1 \rho_3 & \tau^2 + \rho_2 \rho_4 \\ 0 & \rho_1^2 & \rho_2^2 \\ 0 & \rho_3^2 & \rho_4^2 \end{pmatrix} \in H_\omega,$$

denn $\det(aha) = \rho_1^2 \rho_4^2 + \rho_2^2 \rho_3^2 = \det(h)^2 = 1$. Wieder folgt $c \in N_{S_{24}}(H_\omega)$.

Offenbar gilt $xb = bx$, $xc = cx$ und $ac = ca$. Dies zeigt $(xb)^2 = (xc)^2 = (ac)^2 = 1$. Es verbleibt zu zeigen: $(ax)^3 = (ba)^3 = (cb)^3 = 1$. Dies ergibt aus den folgenden Rechnungen:

$$\begin{aligned} {}^{cbc}[r, s, t] &= {}^c[[r, s, t\zeta]] = [[r^2, s^2, t^2\zeta^2]] = {}^b[[r, s, t\zeta^2]] = {}^{bcb}[r, s, t], \\ {}^{bab}[r, s, t] &= {}^b[[r + s^2 t^2 \zeta, s, t\zeta^2]] = [[r^2 + st\zeta^2, s^2, t^2\zeta^2]] \stackrel{1+\zeta=\zeta^2}{=} {}^a[[r + s^2 t^2, s, t\zeta]] = {}^{aba}[r, s, t], \\ {}^{axa}1 &= {}^a[[0, 1, 0]] = [[0, 1, 0]] = {}^{xax}1, \\ {}^{axa}[[1, 0, 0]] &= [[1, 0, 0]] = {}^{xax}[[1, 0, 0]], \\ {}^{axa}[[0, 1, 0]] &= 1 = {}^{xax}[[1, 0, 0]], \\ {}^{axa}[[r, s, t]] &= {}^a[[s^2, r^2 + st, t^2]] = [[s + r^2 t^2 + st^3, r + s^2 t^2, t]] \\ &= \left\{ \begin{array}{l} [[r^2, s^2 + rt, t^2]] \text{ falls } t \neq 0, \\ [[s, r, 0]] \text{ falls } t = 0 \neq rs \end{array} \right\} = {}^x[[s^2 + rt, r^2, t^2]] = {}^{xax}[[r, s, t]]. \end{aligned}$$

Witts Lemma zeigt nun, dass M_{24} 5-transitiv auf Ω operiert. Aus den Beweis von Witts Lemma erhält man $(M_{24})_3 = M_{23}$ und $M_{22} = (M_{23})_2$. Damit folgen die restlichen Aussagen. \square

Definition 9.11. Man nennt M_{11} , M_{12} , M_{22} , M_{23} und M_{24} die *Mathieugruppen* vom Grad 11, 12, 22, 23 bzw. 24. Aus Bemerkung 9.3 ergibt sich

$$\begin{aligned} |M_{11}| &= 11 \cdot 10 \cdot 9 \cdot 8 = 7.920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11, \\ |M_{12}| &= 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95.040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11, \\ |M_{22}| &= 22|\text{PSL}(3, 4)| = 443.520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11, \\ |M_{23}| &= 23|M_{22}| = 10.200.960 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23, \\ |M_{24}| &= 24|M_{23}| = 244.823.040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23. \end{aligned}$$

Lemma 9.12. Sei $G \leq \text{Sym}(\Omega)$ 3-transitiv vom Grad $d = |\Omega| \geq 5$. Ist G_ω einfach für ein $\omega \in \Omega$, so ist G einfach oder d ist eine 2-Potenz.

Beweis. Der Beweis funktioniert wie bei der Einfachheit der alternierenden Gruppen. Sei $1 \neq N \trianglelefteq G$. Nach GT-Satz 6.20 operiert N transitiv. Das Frattini-Argument liefert $G = G_\omega N$. Wir können indirekt $G_\omega \not\leq N$ annehmen. Aus der Einfachheit von G_ω folgt $N_\omega = G_\omega \cap N = 1$. Also ist N ein regulärer Normalteiler und $|N| = d \geq 5$. Nach GT-Lemma 6.19 operiert G_ω 2-transitiv auf $N \setminus \{1\}$ durch Konjugation. Aus GT-Satz 6.36 folgt $d = |N| = 2^k$ für ein $k \in \mathbb{N}$. \square

Beispiel 9.13. Sei $d = 2^n \geq 8$ und $\Omega := \mathbb{F}_2^n$. Nach linearer Algebra operiert die einfache Gruppe $\text{GL}(n, 2)$ 2-transitiv auf $\Omega \setminus \{0\}$. Daher operiert die nicht-einfache Gruppe $\text{AGL}(n, 2) = \mathbb{F}_2^n \rtimes \text{GL}(n, 2)$ 3-transitiv auf Ω mit Stabilisator $G_0 = \text{GL}(n, 2)$ (GT-Beispiel 6.23).

Satz 9.14. Die Mathieugruppen M_{11} , M_{12} , M_{22} , M_{23} und M_{24} sind einfach.

Beweis (CHAPMAN). Sei zunächst $G = M_{11}$ und $P \in \text{Syl}_{11}(G)$. In S_{11} gibt es $10!$ Elemente der Ordnung 11, die sich auf $9!$ Sylowgruppen verteilen. Also ist $|\text{N}_{S_{11}}(P)| = 11 \cdot 10$ und $|\text{N}_G(P) : P|$ teilt 10. Nach Sylow ist

$$5 \equiv 10 \cdot 9 \cdot 8 = \frac{|G|}{11} = |G : \text{N}_G(P)| |\text{N}_G(P) : P| \equiv |\text{N}_G(P) : P| \pmod{11}$$

und somit $|\text{N}_G(P) : P| = 5$ und $|G : \text{N}_G(P)| = 16 \cdot 9$. Sei nun $1 \neq N \trianglelefteq G$. Dann ist N transitiv und alle 11-Sylowgruppen von G liegen in N . Insbesondere ist $|N : \text{N}_N(P)| = 16 \cdot 9$. Dies zeigt $|G : N| \leq 5$. Nehmen wir $|G : N| = 5$ an. Dann besitzt N genau $16 \cdot 9 \cdot 10$ Elemente der Ordnung 11. Die übrigen $|N|/11$ Elemente müssen dann den Stabilisator N_1 bilden. Insbesondere ist $N_1 = \dots = N_{11}$. Dann kann N aber nicht treu operieren. Also ist $G = N$ und G ist einfach.

Die Einfachheit von M_{12} folgt nun aus Lemma 9.12, da M_{11} ein Stabilisator von M_{12} ist. Da $\text{PSL}(3, 4)$ einfach ist, kann man mit Lemma 9.12 auch die Einfachheit von M_{22} , M_{23} und M_{24} zeigen. \square

Bemerkung 9.15.

- (i) Gelegentlich definiert man die Mathieugruppen M_9 , M_{10} , M_{20} und $M_{21} \cong \text{PSL}(3, 4)$ als geeignete Stabilisatoren der größeren Mathieugruppen. Sie sind jedoch keine sporadisch einfachen Gruppen. Im Beweis von Satz 9.7 haben wir $M_9 \cong C_3^2 \rtimes Q_8$ als scharf 2-transitive Gruppe vom Grad 9 konstruiert. Insbesondere ist M_9 eine Frobeniusgruppe.
- (ii) Man kann (elementar) zeigen, dass S_k , S_{k+1} , A_{k+2} , M_{11} und M_{12} die einzigen scharf k -transitiven Permutationsgruppen mit $k \geq 4$ sind. Mit der CFSG konnte man zeigen, dass S_n , A_n , M_{11} , M_{12} , M_{23} und M_{24} die einzigen 4-transitiven Permutationsgruppen sind.

- (iii) Man kann die Mathieugruppen auch jeweils mit nur zwei Permutationen erzeugen, aber dann ist es schwierig die Struktur (geschweige denn die Ordnung) zu bestimmen. Tatsächlich stieß Mathieus Arbeit von 1861 lange Zeit auf Unverständnis. So behauptete MILLER 1898 M_{24} würde nicht existieren. Nach der CFSG weiß man, dass sich jede endliche einfache Gruppe mit einer Involution und einem weiteren Element mit Primzahlordnung erzeugen lässt.
- (iv) Die nachfolgende Definition lässt sich folgendermaßen motivieren: Wie viele Lotto-Scheine muss man kaufen, wenn man garantiert vier „Richtige“ haben will? Im besten Fall kommt jede 4er Kombination nur auf einem Tippschein vor (ob das möglich ist, sehen wir in Beispiel 9.19).

Definition 9.16. Ein $((t, k, v)$ -Steinersystem ist ein Paar $S = (\Omega, \mathcal{B})$ mit folgenden Eigenschaften:

- Ω ist eine v -elementige Menge von „Punkten“ (engl. vertices).
- \mathcal{B} ist eine Menge von k -elementigen Teilmengen von Ω , die „Blöcke“ genannt werden.¹⁵
- Jede t -elementige Teilmenge von Ω liegt in genau einem Block von \mathcal{B} .

Man nennt

$$\text{Aut}(S) := \{\sigma \in \text{Sym}(\Omega) : \forall B \in \mathcal{B} : \sigma(B) \in \mathcal{B}\} \leq \text{Sym}(\Omega)$$

die *Automorphismengruppe* von S .

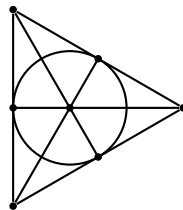
Beispiel 9.17.

- (i) (t, k, v) -Steinersysteme können offensichtlich nur für $t \leq k \leq v$ existieren. Im Fall $t = k$ ist \mathcal{B} die Menge aller k -elementigen Teilmengen von Ω und $\text{Aut}(S) = \text{Sym}(\Omega)$. Im Fall $k = v$ ist $\mathcal{B} = \{\Omega\}$ und $\text{Aut}(S) = \text{Sym}(\Omega)$. Diese Steinersysteme nennt man *trivial*. Wir können also $t < k < v$ annehmen.
- (ii) Im Fall $t = 1$ ist \mathcal{B} eine Partition von Ω und es folgt $k \mid v$. Die Anzahl dieser Steinersysteme ist die Stirling-Zahl der zweiten Art $\left\{ \begin{smallmatrix} v \\ k \end{smallmatrix} \right\}$. Wir sehen in Lemma 9.18, dass es im Allgemeinen starke Einschränkungen an t, k, v gibt.
- (iii) Sei q eine Primzahlpotenz, $n \geq 2$, $\Omega = \mathbb{F}_q^n$ und

$$\mathcal{B} = \{\mathbb{F}_q v + w : v, w \in \Omega, v \neq 0\}$$

die Menge der „Geraden“ auf Ω (man ersetze gedanklich \mathbb{F}_q durch \mathbb{R}). Da je zwei verschiedene Punkte auf genau einer Geraden liegen, ist $S = (\Omega, \mathcal{B})$ ein $(2, q, q^n)$ -Steinersystem. Man nennt S *affine Ebene* über \mathbb{F}_q^n .

- (iv) Sei $n \geq 3$, $\Omega = \{\mathbb{F}_q v : v \in \mathbb{F}_q^n \setminus \{0\}\}$ die Menge der 1-dimensionalen Unterräume von \mathbb{F}_q^n und \mathcal{B} die Menge der 2-dimensionalen Unterräume von \mathbb{F}_q^n (formal: jeder Block besteht aus den 1-dimensionalen Unterräumen eines 2-dimensionalen Raums). Da je zwei linear unabhängige Vektoren einen 2-dimensionalen Unterraum aufspannen, ist $S = (\Omega, \mathcal{B})$ ein $(2, q+1, \frac{q^n-1}{q-1})$ -Steinersystem. Man nennt S *projektive Ebene* über \mathbb{F}_q^n . Für $(q, n) = (2, 3)$ erhält man die *Fano-Ebene*:



¹⁵Dies hat nichts mit den Blöcken einer imprimitiven Operation zu tun.

Lemma 9.18. Sei $S = (\Omega, \mathcal{B})$ ein (t, k, v) -Steinersystem und $0 \leq s \leq t$. Dann gilt:

(i) Die Anzahl der Blöcke, die eine gegebene s -elementige Teilmenge von Ω enthalten, ist

$$\gamma_s := \frac{(v-s)(v-s-1)\dots(v-t+1)}{(k-s)(k-s-1)\dots(k-t+1)}.$$

(ii) $|\mathcal{B}| = \gamma_0 = \frac{v\gamma_1}{k}$.

(iii) (FISHERs Ungleichung) $v \leq |\mathcal{B}|$ und $k \leq \gamma_1$.

Beweis.

(i) Jede s -elementige Teilmenge liegt in genau $\binom{v-s}{t-s}$ t -elementigen Teilmengen von Ω . Jede t -elementige Teilmenge liegt nach Definition in genau einem Block. Jeder Block enthält genau $\binom{k-s}{t-s}$ s -elementige Teilmengen. Dies zeigt

$$\gamma_s = \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} = \frac{(v-s)(v-s-1)\dots(v-t+1)}{(k-s)(k-s-1)\dots(k-t+1)}.$$

(ii) Folgt aus (i).

(iii) Sei $\Omega = \{\omega_1, \dots, \omega_v\}$ und $\mathcal{B} = \{B_1, \dots, B_r\}$. Sei $M := (m_{ij}) \in \mathbb{Z}^{v \times r}$ die Inzidenzmatrix von S , d. h. $m_{ij} = 1$ falls $\omega_i \in B_j$ und $m_{ij} = 0$ sonst. Dann gilt

$$MM^t = \left(\sum_{l=1}^r m_{il}m_{jl} \right)_{ij} = \begin{pmatrix} \gamma_1 & \gamma_2 & \cdots & \gamma_2 \\ \gamma_2 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \gamma_2 \\ \gamma_2 & \cdots & \gamma_2 & \gamma_1 \end{pmatrix} = (\gamma_1 - \gamma_2)1_v + \gamma_2 J,$$

wobei $J = (1) \in \mathbb{Z}^{v \times v}$ die Matrix aus lauter Einsen ist. Nach (i) ist $\gamma_1 = \frac{v-1}{k-1}\gamma_2 > \gamma_2$. Die Eigenwerte von J sind bekanntlich 0 mit Vielfachheit $v-1$ und v mit Vielfachheit 1. Daher sind $\gamma_1 - \gamma_2 > 0$ und $\gamma_1 - \gamma_2 + \gamma_2 v$ die Eigenwerte von MM^t . Insbesondere ist MM^t invertierbar. Dies zeigt

$$v = \text{rk}(MM^t) \leq \text{rk}(M) \leq \min\{r, v\}$$

und es folgt $v \leq r = |\mathcal{B}|$. Aus (ii) ergibt sich $k = \frac{v\gamma_1}{r} \leq \gamma_1$. \square

Beispiel 9.19. Für die optimale Lösung des Lotto-Problems aus Bemerkung 9.15 benötigt man ein $(4, 6, 49)$ -Steinersystem. Wegen $\gamma_3 = \frac{46}{3} \notin \mathbb{N}$ gibt es dies nicht. In jeden Fall benötigt man mindestens

$$\gamma_0 = \frac{49 \cdot 48 \cdot 47 \cdot 46}{6 \cdot 5 \cdot 4 \cdot 3} > 14.125$$

Tipp Scheine.¹⁶

¹⁶Man kann zeigen, dass mindestens 14.749 Tipp-Scheine nötig sind. Ob das tatsächlich ausreicht ist allerdings offen. Siehe https://1jcr.dmgordon.org/show_cover.php?v=49&k=6&t=4.

- (i) Zur (alternativen) Konstruktion der Mathieugruppen startet man mit der affinen Ebene S über \mathbb{F}_3^2 als $(2, 3, 9)$ -Steinersystem. Nun erweitert man S durch Hinzunahme von drei Punkten zu einem $(5, 6, 12)$ -Steinersystem \hat{S} (die Details sind äußerst aufwendig¹⁷). Anschließend definiert man $M_{12} := \text{Aut}(\hat{S})$. Auch die größeren Mathieugruppen lassen sich auf diese Weise gewinnen. Allgemein hat MENDELSON bewiesen, dass jede endliche Gruppe die Automorphismengruppe eines $(2, 3, v)$ -Steinersystems und eines $(3, 4, v)$ -Steinersystems ist.
- (ii) Für M_{22} benutzt man ein $(3, 6, 22)$ -Steinersystem $S = (\Omega, \mathcal{B})$ (es gilt $\text{Aut}(S) \cong M_{22} \rtimes C_2$). Nach Lemma 9.18 ist $|\mathcal{B}| = \frac{22 \cdot 21 \cdot 20}{6 \cdot 5 \cdot 4} = 77$. Sei Γ ein Graph mit Eckenmenge $\Gamma_E := \Omega \cup \mathcal{B} \cup \{\zeta\}$, also $|\Gamma_E| = 22 + 77 + 1 = 100$. Die Ecke ζ sei zu allen $\omega \in \Omega$ benachbart. Zwei Blöcke sind genau dann benachbart in Γ , wenn sie disjunkt sind. Alle anderen Kanten haben die Form $(\omega, B) \in \Omega \times \mathcal{B}$ mit $\omega \in B$. Nach Aufgabe 26 ist Γ ein 22-regulärer Graph. Man nennt ihn *Higman-Sims-Graph*. Es gilt $\text{Aut}(\Gamma) = HS \rtimes C_2$, wobei HS die sporadisch einfache *Higman-Sims-Gruppe* der Ordnung 44.352.000 ist.
- (iii) Die Mathieugruppen lassen sich auch mit Methoden der Codierungstheorie konstruieren. Der (erweiterte binäre) *Golay-Code* ist der von den Zeilen der Matrix

$$\begin{pmatrix} 1 & . & 1 & . & 1 & 1 & 1 & . & . & . & 1 & 1 & . & . & . & . & . & . & . & . \\ . & 1 & . & 1 & . & 1 & 1 & 1 & . & . & . & 1 & 1 & . & . & . & . & . & . & 1 \\ . & . & 1 & . & 1 & . & 1 & 1 & 1 & . & . & . & 1 & 1 & . & . & . & . & . & 1 \\ . & . & . & 1 & . & 1 & . & 1 & 1 & . & . & . & 1 & 1 & . & . & . & . & . & 1 \\ . & . & . & . & 1 & . & 1 & . & 1 & 1 & . & . & . & 1 & 1 & . & . & . & . & 1 \\ . & . & . & . & . & 1 & . & 1 & . & 1 & 1 & . & . & . & 1 & 1 & . & . & . & 1 \\ . & . & . & . & . & . & 1 & . & 1 & . & 1 & 1 & . & . & . & 1 & 1 & . & . & 1 \\ . & . & . & . & . & . & . & 1 & . & 1 & . & 1 & 1 & . & . & . & 1 & 1 & . & 1 \\ . & . & . & . & . & . & . & . & 1 & . & 1 & . & 1 & 1 & . & . & . & 1 & 1 & 1 \end{pmatrix}$$

$$\text{Aut}(C) := \{\sigma \in S_{24} : \forall (c_i) \in C : (c_{\sigma(i)}) \in C\}$$

(iv) Die Automorphismengruppen und Schur-Multiplikatoren sind

G	M_{11}	M_{12}	M_{22}	M_{23}	M_{24}
$\text{Out}(G)$	1	C_2	C_2	1	1
$M(G)$	1	C_2	C_{12}	1	1

```
G:=MathieuGroup(24);;
AllPrimitiveGroups(NrMovedPoints,24,Transitivity,5); #gibt nur eine
PrimitiveIdentification(G); #G=PrimitiveGroup(24,1)
IsSimple(G);
```

75

```
LoadPackage("guava",false); #Paket für Codes
C:=ExtendedBinaryGolayCode();
Display(GeneratorMat(C));
A:=AutomorphismGroup(C);
Transitivity(A); #5-transitiv
c:=Positions(Basis(C)[1],Z(2)^0); #Codewort mit genau acht Einsen
B:=Orbit(A,c,OnSets);; #Blöcke des (5,8,24)-Steinersystems
Size(B); #759 = (24·23·22·21·20)/(8·7·6·5·4)
```

- (v) Die Gruppe M_{23} ist die einzige sporadische Gruppe, für die das *inverse Galois-Problem* noch nicht gelöst ist, d. h. man weiß nicht, ob es einen Zahlkörper $K \subseteq \mathbb{C}$ mit $\text{Gal}(K|\mathbb{Q}) \cong M_{23}$ gibt.
- (vi) Eng verwandt mit dem Golay-Code ist das *Leech-Gitter* $L \leq \mathbb{Z}^{24}$, welches aus den ganzzahligen Linearkombinationen der Zeilen folgender Matrix besteht:

[illegible]

$$\begin{aligned} u &:= (4, 4, 0, \dots, 0), \\ v &:= (4, -4, 0, \dots, 0), \\ w &:= (5, 1, \dots, 1). \end{aligned}$$

Man nennt $Co_2 := C_A(u)$ bzw. $Co_3 := C_A(w)$ die zweite bzw. dritte Conway-Gruppe. Außerdem ist $McL := C_A(u, w)$ die *McLaughlin-Gruppe* und $C_A(v, w) \cong HS$. Alle sind sporadisch einfache Gruppen mit Ordnungen

$$\begin{aligned} |Co_1| &= 2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23 = 4.157.776.806.543.360.000, \\ |Co_2| &= 2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23 = 42.305.421.312.000, \\ |Co_3| &= 2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23 = 495.766.656.000, \\ |McL| &= 2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 = 898.128.000. \end{aligned}$$

- (vii) Erst über 100 Jahre nach Mathieus Arbeit entdeckte JANKO die nächste sporadisch einfache Gruppe J_1 . Sie lässt sich am einfachsten durch eine \mathbb{F}_{11} -Darstellung definieren:

$$J_1 := \left\langle \begin{pmatrix} . & 1 & . & . & . & . & . \\ . & . & 1 & . & . & . & . \\ . & . & . & 1 & . & . & . \\ . & . & . & . & 1 & . & . \\ . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & 1 \\ 1 & . & . & . & . & . & . \end{pmatrix}, \begin{pmatrix} -3 & 2 & -1 & -1 & -3 & -1 & -3 \\ -2 & 1 & 1 & 3 & 1 & 3 & 3 \\ -1 & -1 & -3 & -1 & -3 & -3 & 2 \\ -1 & -3 & -1 & -3 & -3 & 2 & -1 \\ -3 & -1 & -3 & -3 & 2 & -1 & -1 \\ 1 & 3 & 3 & -2 & 1 & 1 & 3 \\ 3 & 3 & -2 & 1 & 1 & 3 & 1 \end{pmatrix} \right\rangle \leq \text{GL}(7, 11).$$

Es gilt $|J_1| = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 = 175.560$. Drei weitere sporadische Gruppen J_2 , J_3 und J_4 sind nach Janko benannt.

- (viii) Präsentationen, Permutations- und Matrixdarstellungen sämtlicher sporadischer Gruppen kann man unter <http://brauer.maths.qmul.ac.uk/Atlas/v3/> nachschlagen oder direkt mit GAP beziehen:

```
LoadPackage("atlasrep");
DisplayAtlasInfo("M24"); #Übersicht Darstellungen, braucht Internet
AtlasGroup("M24", Dimension, 11, Ring, GF(2));
prog:=AtlasProgram("M24", "presentation");;
slp:=StraightLineProgramFromStraightLineDecision(prog.program);;
F:=FreeGroup(2);;
rels:=ResultOfStraightLineProgram(slp, GeneratorsOfGroup(F));;
G:=F/rels;;
PresentationFpGroup(G);

ct:=CharacterTable("M"); #Charaktertafel des Monsters
PrintFactorsInt(Size(ct)); #Primfaktorisierung der Ordnung
NrConjugacyClasses(ct);
SizesConjugacyClasses(ct);
OrdersClassRepresentatives(ct); #Ordnungen der Elemente bis auf Konjugation
```

- (ix) Erst 2014 konnte KEEVASH zeigen, dass es nicht-triviale (t, k, v) -Steinersysteme mit $t \geq 6$ gibt. Tatsächlich sind die Teilbarkeitsbedingungen aus Lemma 9.18 in den „meisten“ Fällen hinreichend für die Existenz eines entsprechenden Steinersystems. Der Beweis ist probabilistisch und nicht konstruktiv.¹⁸ Die Anzahl der $(2, 3, v)$ -Steinersysteme für $v \leq 19$ kann man unter OEIS nachschlagen.

10 Coxetergruppen

Bemerkung 10.1. Die Gruppen, die sich von zwei Involutionen erzeugen lassen, sind bekanntlich genau die Diedergruppen. Wir untersuchen in diesem Abschnitt Gruppen, die sich von endlich vielen Involutionen erzeugen lassen. Diese treten als Symmetriegruppen höher-dimensionaler Räume auf und führen zur Klassifikation der (endlichen) Spiegelungsgruppen.

Definition 10.2. Eine Gruppe der Form

$$G = \langle x_1, \dots, x_n \mid (x_i x_j)^{m_{ij}} = 1, 1 \leq i < j \leq n \rangle$$

mit $2 \leq m_{ij} \leq \infty$ für $i < j$ und $m_{ii} = 1$ für $i = 1, \dots, n$ heißt *Coxetergruppe* vom Rang n .

¹⁸Dazu ein populärwissenschaftlicher Artikel: wired.com

Bemerkung 10.3.

- (i) Im Folgenden sei $G = \langle x_1, \dots, x_n \rangle$ stets eine Coxetergruppe (wir identifizieren die Erzeuger x_1, \dots, x_n der freien Gruppe mit entsprechenden Nebenklassen in G). Die Relationen der Form $(x_i x_j)^\infty = 1$ haben keine Bedeutung und können ignoriert werden. Aus $m_{ii} = 1$ folgt $x_i^2 = 1$ für $i = 1, \dots, n$. Wegen $(x_j x_i)^{m_{ij}} = (x_i x_j)^{-m_{ij}} = 1$ definieren wir $m_{ji} := m_{ij}$ für $i < j$. Nach von-Dyck existiert ein Homomorphismus $f: G \rightarrow \{\pm 1\}$ mit $f(x_i) = -1$ für $i = 1, \dots, n$. Also sind x_1, \dots, x_n Involutionen in G . Die Gleichung $m_{ij} = 2$ besagt, dass x_i und x_j vertauschbar sind.
- (ii) Die Relation $(x_i x_j)^{m_{ij}} = 1$ ist äquivalent zu $x_i x_j x_i \dots = x_j x_i x_j \dots$, wobei auf beiden Seiten genau m_{ij} Faktoren stehen. Sei $(x_i x_j)_n := x_i x_j x_i \dots$ ein alternierendes Produkt von n Faktoren. Verzichtet man in der Definition der Coxetergruppen auf die Bedingung $m_{ii} = 2$, so erhält man *Artingruppen*:

$$\langle x_1, \dots, x_n \mid (x_i x_j)_{m_{ij}} = (x_j x_i)_{m_{ij}}, 1 \leq i, j \leq n \rangle$$

mit $2 \leq m_{ij} \leq \infty$. Die Wahl $m_{ij} = \infty$ für alle i, j ergibt die freie Gruppe F_n . Nach von-Dyck ist jede Coxetergruppe eine Faktorgruppe einer Artingruppe. Im Spezialfall $m_{ij} = 3$ für $|i - j| = 1$ und $m_{ij} = 2$ für $|i - j| > 1$ spricht man von einer *Zopfgruppe*. Im Gegensatz zu S_n (Satz 2.18) gilt $m_{ii} = \infty$ anstatt $m_{ii} = 2$. Man kann die Elemente der Zopfgruppe durch „Zöpfe“ mit n „Strängen“ realisieren. Die Verknüpfung ist das „Verkleben“ der Stränge an deren Enden:

$$\begin{array}{c} x_1 : \begin{array}{c} \text{---} \quad \text{---} \\ \diagup \quad \diagdown \\ \text{---} \quad \text{---} \end{array} \quad x_2 : \begin{array}{c} \text{---} \quad \text{---} \\ \diagdown \quad \diagup \\ \text{---} \quad \text{---} \end{array} \quad x_1^2 : \begin{array}{c} \text{---} \quad \text{---} \\ \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \diagdown \quad \diagup \\ \text{---} \quad \text{---} \end{array} \\ \\ x_1 x_2 x_1 = \begin{array}{c} \text{---} \quad \text{---} \\ \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \diagdown \quad \diagup \\ \text{---} \quad \text{---} \\ \diagup \quad \diagdown \\ \text{---} \quad \text{---} \end{array} = \begin{array}{c} \text{---} \quad \text{---} \\ \diagdown \quad \diagup \\ \text{---} \quad \text{---} \\ \diagup \quad \diagdown \\ \text{---} \quad \text{---} \\ \diagdown \quad \diagup \\ \text{---} \quad \text{---} \end{array} = x_2 x_1 x_2 \end{array}$$

Auf diese Gruppen werden wir allerdings nicht weiter eingehen.

Beispiel 10.4.

- (i) $G = \langle x, y \mid x^2 = y^2 = (xy)^m = 1 \rangle \cong D_{2m}$ ist eine Coxetergruppe.
- (ii) $G = \langle x_1, \dots, x_n \mid x_i^2 = (x_i x_j)^2 = 1, i < j \rangle \cong C_2^n$ ist eine Coxetergruppe.
- (iii) Nach Satz 2.18 sind die symmetrischen Gruppen Coxetergruppen mit $x_i = (i, i + 1)$ für $i = 1, \dots, n - 1$.
- (iv) Im Fall $m_{ij} = \infty$ für alle $i < j$ nennt man G die *universelle* Coxetergruppe vom Rang n . Für $n = 2$ erhält man D_∞ . Jede Coxetergruppe ist eine Faktorgruppe einer universellen Coxetergruppe.
- (v) Eine *Spiegelung* $\sigma \in \text{GL}(\mathbb{R}^d)$ ist eine Abbildung der Form $\sigma_b(v) := v - 2[v, b]b$ für einen normierten Vektor $b \in \mathbb{R}^d$ (hierbei ist $[v, b]$ das Standardskalarprodukt). Eine *Spiegelungsgruppe* ist eine endliche Untergruppe $S \leq \text{GL}(\mathbb{R}^d)$, die von Spiegelungen $\sigma_1, \dots, \sigma_n$ erzeugt wird. Nach von-Dyck ist S eine Faktorgruppe einer Coxetergruppe. Wir werden in Satz 10.41 zeigen, dass S tatsächlich zu einer Coxetergruppe isomorph ist (d. h. alle weiteren Relationen in S folgen aus den Relationen $(\sigma_i \sigma_j)^{m_{ij}} = 1$).
- (vi) Sei S eine endliche, nicht-abelsche einfache Gruppe. Nach Feit-Thompson besitzt S eine Involution s . Offenbar wird S von allen Konjugierten von s erzeugt. Also ist S zu einer Faktorgruppe einer (möglicherweise unendlichen) Coxetergruppe.

Definition 10.5. Jedes $g \in G$ lässt sich in der Form $g = x_{i_1} \dots x_{i_k}$ schreiben. Ist k dabei so klein wie möglich, so nennt man diese Darstellung *reduziert* (im Gegensatz zu freien Gruppen sind reduzierte Darstellungen nicht unbedingt eindeutig). Außerdem sei $l(g) := k$ die *Länge* von g .

Lemma 10.6. Für $g, h \in G$ und $1 \leq i \leq n$ gilt

- (i) $l(gh) \leq l(g) + l(h)$.
- (ii) $l(g^{-1}) = l(g)$.
- (iii) $l(gx_i) = l(g) \pm 1$.

Beweis. Die ersten beiden Aussagen sind trivial. Sie zeigen

$$l(g) - 1 = l(gx_i x_i) - l(x_i) \leq l(gx_i) \leq l(g) + l(x_i) = l(g) + 1.$$

Der Homomorphismus $f: G \rightarrow \{\pm 1\}$ aus Bemerkung 10.3 liefert

$$(-1)^{l(gx_i)} = f(gx_i) = -f(g) = -(-1)^{l(g)}$$

und $l(gx_i) \neq l(g)$. □

Bemerkung 10.7. Der Kern des Homomorphismus $f: G \rightarrow \{\pm 1\}$ ist die Menge der Elemente gerader Länge. Man nennt ihn die *alternierende Untergruppe*. In S_n gilt $\text{sgn}(g) = (-1)^{l(g)}$ für $g \in S_n$.

Definition 10.8. Sei V ein \mathbb{R} -Vektorraum mit Basis b_1, \dots, b_n .

- Wir definieren eine symmetrische Bilinearform auf V durch

$$[b_i, b_j]_G := [b_i, b_j] = -\cos \frac{\pi}{m_{ij}},$$

wobei $-\cos \frac{\pi}{\infty} = -1$ gesetzt wird.

- Für $i = 1, \dots, n$ sei

$$\sigma_i: V \rightarrow V, \quad v \mapsto v - 2[v, b_i]b_i.$$

Satz 10.9. Es existiert genau ein Homomorphismus $\sigma: G \rightarrow \text{GL}(V)$ mit $\sigma(x_i) = \sigma_i$ für $i = 1, \dots, n$. Dabei hat $\sigma_i \sigma_j$ die Ordnung m_{ij} für $1 \leq i, j \leq n$. Mit der Bezeichnung ${}^g v := \sigma(g)(v)$ gilt $[v, w]_G = [{}^g v, {}^g w]_G$.

Beweis. Für $i = 1, \dots, n$ gilt $[b_i, b_i] = 1$. Daher ist $V_i := b_i^\perp := \text{Ker}(v \mapsto [v, b_i]) \leq V$ eine Hyperebene und $V = V_i \oplus \mathbb{R}b_i$. Es gilt $\sigma_i(b_i) = -b_i$ und $\sigma_i(v) = v$ für $v \in V_i$. Also ist σ_i eine „Spiegelung“ an V_i (im Gegensatz zum euklidischen Raum ist $[\cdot, \cdot]_G$ nicht unbedingt positiv definit). Insbesondere hat σ_i Ordnung 2. Sei nun $i < j$ und $W := \langle b_i, b_j \rangle$. Die Definition von σ_i zeigt, dass $\langle \sigma_i, \sigma_j \rangle$ auf W operiert.

Sei zunächst $m_{ij} = \infty$. Dann gilt

$$(\sigma_i \sigma_j)^k(b_i) = (\sigma_i \sigma_j)^{k-1}(\sigma_i(b_i + 2b_j)) = (\sigma_i \sigma_j)^{k-1}(3b_i + 2b_j) = \dots = (2k+1)b_i + 2kb_j$$

für $k \geq 1$. Insbesondere hat $\sigma_i \sigma_j$ unendliche Ordnung.

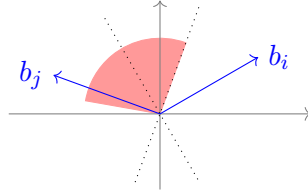
Jetzt sei $m_{ij} < \infty$ und $\varphi := \pi/m_{ij}$. Für $v = \lambda b_i + \mu b_j \in W$ gilt

$$[v, v] = \lambda^2 - 2\lambda\mu \cos \varphi + \mu^2 = (\lambda - \mu \cos \varphi)^2 + \mu^2 \sin^2(\varphi) > 0.$$

Also ist $[\cdot, \cdot]_G$ auf W positiv definit und stimmt daher bis auf Basiswahl mit dem Standardskalarprodukt überein. Außerdem ist

$$[b_i, b_j] = -\cos \varphi = \cos(\pi - \varphi),$$

d. h. der „Winkel“ zwischen b_i und b_j beträgt $\pi - \varphi$. Daher ist $(\sigma_i \sigma_j)|_W$ eine „Drehung“ um 2φ (da die Abbildung linear ist, genügt es die Bilder der beiden linear unabhängigen Spiegelachsen zu betrachten):



Insbesondere hat $(\sigma_i \sigma_j)|_W$ Ordnung m_{ij} . Da $[\cdot, \cdot]_G$ auf W positiv definit ist, gilt $V = W \oplus W^\perp = W \oplus (V_i \cap V_j)$. Da $\sigma_i \sigma_j$ trivial auf $V_i \cap V_j$ operiert, hat $\sigma_i \sigma_j$ auch auf V Ordnung m_{ij} . Nach von-Dyck ist σ nun ein Homomorphismus. Für die letzte Aussage berechnen wir

$$\begin{aligned} [\sigma_i(v), \sigma_i(w)] &= [v - 2[v, b_i]b_i, w - 2[w, b_i]b_i] \\ &= [v, w] - 2[v, b_i][b_i, w] - 2[w, b_i][v, b_i] + 4[v, b_i][w, b_i] = [v, w]. \end{aligned} \quad \square$$

Definition 10.10.

- Man nennt

$$\Phi := \{^g b_i : 1 \leq i \leq n, g \in G\} \subseteq V$$

das *Wurzelsystem* von G und seine Elemente heißen *Wurzeln*.

- Eine Wurzel v lässt sich eindeutig in der Form $v = \sum_{i=1}^n v_i b_i$ schreiben. Man nennt v *positiv* (bzw. *negativ*), falls $v_1, \dots, v_n \geq 0$ (bzw. $v_1, \dots, v_n \leq 0$). Ggf. schreibt man $v > 0$ (bzw. $v < 0$; der Fall $v = 0$ ist ausgeschlossen). Die Menge der positiven Wurzeln sei Π .
- Für $v \in \Phi$ sei

$$\sigma_v : V \rightarrow V, \quad w \mapsto w - 2[w, v]v.$$

Bemerkung 10.11.

- Nach Satz 10.9 sind alle Wurzeln von G normiert bzgl. $[\cdot, \cdot]_G$. Insbesondere ist $\sigma_v(v) = -v$, d. h. σ_v ist die Spiegelung an der Hyperebene v^\perp .
- Wegen $\sigma_i(b_i) = -b_i$ ist $-\Phi = \Phi$ und $\sigma_v = \sigma_{-v}$. Sei $g \in G$ und $1 \leq i \leq n$ mit $v = g(b_i)$. Dann gilt

$$gx_i g^{-1} w = g(g^{-1} w - 2[g^{-1} w, b_i]b_i) = w - 2[w, ^g b_i]^g b_i = w - 2[w, v]v.$$

Dies zeigt $\sigma(gx_i g^{-1}) = \sigma_v$. Wir werden auch $x_v := gx_i g^{-1}$ als Spiegelung bezeichnen.

Beispiel 10.12.

- Sei $G = \langle x, y \rangle \cong D_{2m}$, $\varphi = \pi - \frac{\pi}{m}$, $b_1 = (1, 0)$ und $b_2 = (\cos \varphi, \sin \varphi)$. Dann ist $[\cdot, \cdot]_G$ das Standardskalarprodukt auf \mathbb{R}^2 bzgl. b_1, b_2 und $\sigma : G \rightarrow \text{GL}(\mathbb{R}^2)$ ist die bekannte Darstellung als Symmetriegruppe des regelmäßigen m -Ecks. Die Wurzeln entsprechen den $2m$ Spiegelachsen. Die positiven Wurzeln liegen geometrisch „zwischen“ b_1 und b_2 . Insbesondere ist $\Phi = \Pi \cup (-\Pi)$.

- (ii) Sei $G = \langle x_1, \dots, x_{n-1} \rangle \cong S_n$. Sei e_1, \dots, e_n die Standardbasis von \mathbb{R}^n und $b_i := \frac{1}{\sqrt{2}}(e_i - e_{i+1})$ für $i = 1, \dots, n-1$. Man rechnet leicht nach, dass $[\cdot, \cdot]_G$ das Standardskalarprodukt auf $V := \langle b_1, \dots, b_{n-1} \rangle$ bzgl. b_1, \dots, b_{n-1} ist. Der Homomorphismus $\sigma: G \rightarrow \text{GL}(V)$ entsteht durch die Permutationsoperation von S_n auf den n Koordinaten, denn

$$\begin{aligned} {}^{x_i}b_i &= \sigma_i(b_i) = -b_i = \frac{1}{\sqrt{2}}(e_{i+1} - e_i) = \frac{1}{\sqrt{2}}(e_{x_i(i)} - e_{x_i(i+1)}), \\ {}^{x_i}b_{i+1} &= b_{i+1} - 2[b_{i+1}, b_i]b_i = b_{i+1} + b_i = \frac{1}{\sqrt{2}}(e_i - e_{i+2}) = \frac{1}{\sqrt{2}}(e_{x_i(i+1)} - e_{x_i(i+2)}), \\ {}^{x_i}b_j &= b_j = \frac{1}{\sqrt{2}}(e_{x_i(j)} - e_{x_i(j+1)}) \quad (|j-i| > 1). \end{aligned}$$

Offenbar ist $\Phi = \{e_i - e_j : i \neq j\}$ und $\Pi = \{e_i - e_j : i < j\}$, denn $e_i - e_j = b_i + b_{i+1} + \dots + b_{j-1}$. Insbesondere gilt $|\Phi| = n(n-1)$ und $|\Pi| = n(n-1)/2$.

Lemma 10.13. Für $g \in G$ und $1 \leq i \leq n$ gilt ${}^g b_i > 0$ falls $l(gx_i) > l(g)$ und ${}^g b_i < 0$ falls $l(gx_i) < l(g)$. Insbesondere ist jede Wurzel positiv oder negativ, d. h. $\Phi = \Pi \cup (-\Pi)$.

Beweis. Wegen $g = gx_i x_i$ und ${}^{gx_i} b_i = -{}^g b_i$ genügt es den Fall $l(gx_i) > l(g)$ zu betrachten. Wir beweisen die erste Aussage durch Induktion nach $l(g)$. Im Fall $l(g) = 0$ ist $g = 1$, $l(x_i) = 1$ und $b_i > 0$. Sei nun $g \neq 1$ und $1 \leq j \leq n$ mit $l(gx_j) = l(g) - 1$ (der letzte Faktor einer reduzierten Darstellung von g). Nach Voraussetzung ist $x_j \neq x_i$. Wir betrachten die Diedergruppe $H := \langle x_i, x_j \rangle \leq G$. Sei $l_H: H \rightarrow \mathbb{N}_0$ die Längenfunktion bzgl. der Erzeuger x_i, x_j von H .¹⁹ Sei

$$A := \{y \in gH : l(y) + l_H(y^{-1}g) = l(g)\}.$$

Wegen $g \in A$ ist $A \neq \emptyset$. Wähle $y \in A$ mit $l(y)$ minimal. Wegen $l(gx_j) + l_H(x_j) = l(g) - 1 + 1 = l(g)$ ist $gx_j \in A$. Die Wahl von y zeigt $l(y) \leq l(gx_j) < l(g)$.

Nehmen wir $l(yx_i) = l(y) - 1$ an. Dann gilt

$$l(g) \leq l(yx_i) + l_H(x_i y^{-1}g) \leq l(y) - 1 + l_H(y^{-1}g) + 1 = l(y) + l_H(y^{-1}g) = l(g)$$

und $l(g) = l(yx_i) + l_H(x_i y^{-1}g)$. Dies zeigt $yx_i \in A$ im Widerspruch zu $l(yx_i) < l(y)$. Also gilt $l(yx_i) > l(y)$ und völlig analog $l(yx_j) > l(y)$. Induktion zeigt ${}^y b_i, {}^y b_j > 0$. Sei $h := y^{-1}g \in H$. Wegen $g = yh$ genügt es zu zeigen, dass ${}^h b_i$ eine nicht-negative Linearkombination von b_i und b_j ist.

Angenommen es gilt $l_H(hx_i) < l_H(h)$. Dann wäre

$$l(gx_i) = l(yhx_i) \leq l(y) + l_H(hx_i) < l(y) + l_H(h) = l(g).$$

Also muss jede reduzierte Darstellung von h bzgl. x_i, x_j in x_j enden. Im Fall $m_{ij} = \infty$ ist ${}^{x_j} b_i = b_i + 2b_j$, ${}^{x_i x_j} b_i = {}^{x_i}(b_i + 2b_j) = 3b_i + 2b_j$ usw. (vgl. Beweis von Satz 10.9). Wir können also $m := m_{ij} < \infty$ annehmen. Dann bilden b_i und b_j den Winkel $\pi - \frac{\pi}{m}$ und $x_i x_j$ ist eine „Drehung“ um $\frac{2\pi}{m}$. Ist $l_H(h) = m$, so gilt $h = (x_i x_j)^{m/2}$ falls m gerade und $h = x_j (x_i x_j)^{(m-1)/2}$ falls m ungerade. In beiden Fällen gäbe es eine reduzierte Darstellung, die mit x_i endet (nämlich $h = (x_j x_i)^{m/2}$ bzw. $x_i (x_j x_i)^{(m-1)/2}$). Also ist $l_H(h) < m$ und $h \in \{(x_i x_j)^k, x_j (x_i x_j)^k\}$ mit $k < m/2$. Im Fall $k = (m-1)/2$ ist $h = (x_i x_j)^k$ und ${}^h b_i = b_j$. In allen anderen Fällen ist $(x_i x_j)^k$ eine Drehung um weniger als $\frac{(m-1)\pi}{m}$, d. h. $(x_i x_j)^k b_i$ liegt echt „zwischen“ b_i und b_j . Eine weitere Anwendung von x_j ändert daran nichts. Also ist ${}^h b_i$ eine nicht-negative Linearkombination von b_i und b_j . \square

¹⁹Nach Lemma 10.17 ist l_H die Einschränkung von l auf H . Das wird hier aber nicht benutzt.

Satz 10.14. Der Homomorphismus $\sigma: G \rightarrow \text{GL}(V)$ aus Satz 10.9 ist injektiv.

Beweis. Sei $g \in \text{Ker}(\sigma) \setminus \{1\}$. Dann existiert $1 \leq i \leq n$ mit $l(gx_i) < l(g)$. Lemma 10.13 liefert den Widerspruch $b_i = {}^g b_i < 0$. \square

Definition 10.15. Für $I \subseteq \{1, \dots, n\}$ nennt man $G_I := \langle x_i : i \in I \rangle \leq G$ eine *parabolische* Untergruppe von G .

Satz 10.16. Für $I \subseteq \{1, \dots, n\}$ ist

$$G_I \cong \langle \{y_i : i \in I\} \mid \{(y_i y_j)^{m_{ij}} : i, j \in I\} \rangle,$$

d. h. G_I ist selbst eine Coxetergruppe.

Beweis. Wendet man die Konstruktion von σ auf die Coxetergruppe auf der rechten Seite an, so erhält man genau $\sigma(G_I) \cong G_I$. \square

Lemma 10.17. Sei $g = x_{i_1} \dots x_{i_k} \in G_I$ reduziert in G . Dann gilt $i_1, \dots, i_k \in I$. Insbesondere ist $\{x_1, \dots, x_n\} \cap G_I = \{x_i : i \in I\}$.

Beweis. Induktion nach k . O.B.d.A. sei $k \geq 1$. Nach Lemma 10.13 gilt ${}^g b_{i_k} < 0$. Sei außerdem $g = x_{j_1} \dots x_{j_l}$ mit $j_1, \dots, j_l \in I$. Nach Definition der σ_i gilt

$${}^g b_{i_k} = b_{i_k} + \sum_{a=1}^l \lambda_a b_{j_a}$$

mit $\lambda_a \in \mathbb{R}$. Wegen ${}^g b_{i_k} < 0$ muss $i_k = j_s \in I$ für ein $1 \leq s \leq l$ gelten. Insbesondere ist $h := x_{i_1} \dots x_{i_{k-1}} = g x_{i_k} \in G_I$ reduziert. Die Behauptung folgt nun durch Induktion. \square

Folgerung 10.18. Sind $g = x_{i_1} \dots x_{i_k} = x_{j_1} \dots x_{j_k}$ zwei reduzierte Darstellungen von $g \in G$, so gilt $\{i_1, \dots, i_k\} = \{j_1, \dots, j_k\}$.

Beispiel 10.19. In der Situation von Folgerung 10.18 müssen $\{i_1, \dots, i_k\}$ und $\{j_1, \dots, j_k\}$ nicht als Multimengen übereinstimmen. In S_3 sind beispielsweise $x_1 x_2 x_1 = (1, 3) = x_2 x_1 x_2$ reduzierte Darstellungen.

Satz 10.20. Wir betrachten S_n als Coxetergruppe in den Erzeugern $x_i := (i, i+1)$. Für $\sigma \in S_n$ existieren eindeutig bestimmte Zahlen $l \geq 0$ und $1 \leq a_1, \dots, a_l \leq n-1$ mit folgenden Eigenschaften:

(i) $\sigma = x_{a_1} \dots x_{a_l}$.

(ii) $a_i \neq a_{i-1} \leq a_i + 1$ für $i = 2, \dots, l$.

(iii) Die Folge (a_1, \dots, a_l) besitzt keinen Abschnitt der Form $(a, a-1, \dots, a-r, a)$ mit $r \geq 1$.

Ggf. ist $\sigma = x_{a_1} \dots x_{a_l}$ ein reduziertes Wort, d. h. $l = l(\sigma)$.

Beweis. Wir wenden folgenden Algorithmus auf eine beliebige Darstellung $\sigma = x_{a_1} \dots x_{a_k}$ an:

(1) Ist $a_i = a_{i+1}$ für ein i , so lösche $x_{a_i} x_{a_{i+1}} = 1$ aus der Darstellung.

- (2) Ist $a_{i-1} > a_i + 1$, so tausche $x_{a_{i-1}}$ und x_{a_i} und beginne wieder bei (1). Dies ist erlaubt, da $x_{a_{i-1}}$ und x_{a_i} disjunkt sind.
- (3) Besitzt (a_1, \dots, a_k) einen Abschnitt der Form $(a, a-1, \dots, a-r, a)$, so ersetze diesen durch $(a-1, a, a-1, \dots, a-r)$ und beginne wieder bei (1). Dies verändert σ nicht, denn

$$x_a x_{a-1} \dots x_{a-r} x_a = x_a x_{a-1} x_a x_{a-2} x_{a-3} \dots x_{a-r} = x_{a-1} x_a x_{a-1} x_{a-2} \dots x_{a-r}$$

nach der Zopfrelation.

Durch (1) und (3) wird $\sum_{i=1}^k a_i$ reduziert, während (2) die lexikographische Ordnung der Folge (a_1, \dots, a_k) verringert. Daher muss der Algorithmus nach endlich vielen Schritten abbrechen. Am Ende sind die Bedingungen (i)–(iii) erfüllt.

Eine Folge (a_1, \dots, a_l) , die (ii) und (iii) erfüllt, nennen wir *regulär*. Für $n = 2$ gibt es nur die regulären Folgen $a = ()$ (mit $l = 0$) und $a = (1)$. Induktiv nehmen wir an, dass es genau $(n-1)!$ reguläre Folgen (a_1, \dots, a_l) gibt mit $1 \leq a_1, \dots, a_l \leq n-2$. Sei nun (a_1, \dots, a_l) mit $a_k = n-1$. Dann gilt $(a_k, a_{k+1}, \dots, a_l) = (n-1, n-2, \dots, n-r)$ für ein $r \geq 1$ wegen (ii) und (iii). Für (a_1, \dots, a_{k-1}) gibt es induktiv genau $(n-1)!$ Möglichkeiten, während es für r genau $n-1$ Möglichkeiten gibt. Daher existieren $(n-1)!(n-1)$ reguläre Folgen, die $n-1$ enthalten. Zusammen mit den $(n-1)!$ Folgen, die $n-1$ nicht enthalten, erhält man genau $n! = |S_n|$ reguläre Folgen. Jede Permutation kann also nur durch eine reguläre Folge repräsentiert werden.

Wendet man obigen Algorithmus auf ein reduziertes Wort an, so kann die Länge l nicht kleiner werden. Es gilt also $l = l(\sigma)$. \square

Beispiel 10.21. In S_5 gilt

$$\begin{aligned} x_4 x_3 x_2 x_3 x_1 x_4 x_2 &= x_4 x_3 (x_2 x_1 x_2) x_3 x_4 = x_4 x_3 (x_1 x_2 x_1) x_3 x_4 = x_1 x_4 (x_3 x_2 x_1 x_3) x_4 \\ &= x_1 x_4 (x_2 x_3 x_2 x_1) x_4 = x_1 x_2 (x_4 x_3 x_2 x_1 x_4) = x_1 x_2 x_3 x_4 x_3 x_2 x_1. \end{aligned}$$

Etwas schneller findet man eine reduzierte Darstellung, wenn man rekursiv vorgeht. Sei $\sigma \in S_n$ und $a := \sigma^{-1}(n)$. Dann gilt $\tau := \sigma x_a x_{a+1} \dots x_{n-1} \in S_{n-1}$. Nach Induktion besitzt τ eine Darstellung in der gewünschten Form. Daher hat auch $\sigma = \tau t_{n-1} t_{n-2} \dots t_a$ diese Eigenschaft.

Satz 10.22. Die Abbildung $I \mapsto G_I$ ist ein Isomorphismus von Verbänden, d. h. es gilt

- (i) $I \subseteq J \iff G_I \leq G_J$.
- (ii) $G_{I \cup J} = \langle G_I, G_J \rangle$.
- (iii) $G_{I \cap J} = G_I \cap G_J$.

Beweis.

- (i) Aus $I \subseteq J$ folgt offensichtlich $G_I \leq G_J$. Ist $G_I \leq G_J$, so folgt

$$\{x_i : i \in I\} = \{x_1, \dots, x_n\} \cap G_I \subseteq \{x_1, \dots, x_n\} \cap G_J = \{x_j : j \in J\}$$

aus Lemma 10.17.

- (ii) Trivial.

- (iii) Offenbar ist $G_{I \cap J} \leq G_I \cap G_J$. Die umgekehrte Inklusion folgt aus Lemma 10.17. \square

Satz 10.23. Für $g \in G$ ist $l(g)$ die Anzahl der positiven Wurzeln, die unter g auf negative Wurzeln abgebildet werden, d. h. $l(g) = |\Pi \cap g^{-1}(-\Pi)| \leq |\Pi|$. Insbesondere ist diese Zahl endlich.

Beweis. Induktion nach $l(g)$: O. B. d. A. $g \neq 1$. Sei zunächst $g = x_i$ für ein $1 \leq i \leq n$. Wegen ${}^g b_i = -b_i$ müssen wir ${}^g v > 0$ für alle $v \in \Pi \setminus \{b_i\}$ zeigen. Da alle Wurzeln normiert sind, ist v kein Vielfaches von b_i . Sei also $v = \sum_{j=1}^n \lambda_j b_j$ mit $\lambda_k > 0$ für mindestens ein $k \neq i$. In ${}^g v = \sigma_i(v) = v - 2[v, b_i]b_i$ hat b_k immer noch den positiven Koeffizienten λ_k . Daher ist ${}^g v > 0$.

Sei nun $l(g) \geq 2$ und $1 \leq i \leq n$ mit $l(gx_i) = l(g) - 1$. Nach Lemma 10.13 ist ${}^g b_i < 0$, d. h. $b_i \in \Pi \cap g^{-1}(-\Pi)$. Mit dem eben Bewiesenen folgt

$$\Pi \cap (gx_i)^{-1}(-\Pi) = x_i(x_i(\Pi) \cap g^{-1}(-\Pi)) = x_i(\Pi \cap g^{-1}(-\Pi) \setminus \{b_i\}).$$

Induktion zeigt

$$|\Pi \cap g^{-1}(-\Pi)| = |\Pi \cap (gx_i)^{-1}(-\Pi)| + 1 = l(gx_i) + 1 = l(g). \quad \square$$

Bemerkung 10.24. Ist die Länge in G beschränkt, sagen wir durch m , so gilt $|G| \leq n^m < \infty$. In unendlichen Coxetergruppen muss es daher unendlich viele (positive) Wurzeln geben. Insbesondere ist $-\text{id}_V \notin \sigma(G)$ (anderenfalls hätte $-\text{id}$ unendliche Länge).

Folgerung 10.25. Ist G endlich, so gibt es genau ein Element $g \in G$ mit maximaler Länge.

Beweis. Angenommen $g, h \in G$ haben maximale Länge $l(g) = l(h)$. Dann gilt $l(gx_i) < l(g)$ und ${}^g b_i < 0$ für $i = 1, \dots, n$. Da jede positive Wurzel eine nicht-negative Linearkombination der b_i ist, muss g (und h) alle positiven Wurzeln auf negative Wurzeln abbilden, d. h. $g(\Pi) = -\Pi$. Damit ist $g^2(\Pi) = \Pi = gh(\Pi)$ und $l(g^2) = 0 = l(gh)$. Dies zeigt $h = g^{-1} = g$. \square

Beispiel 10.26.

(i) Für $G = \langle x, y \rangle \cong D_{2m}$ ist $z := xy \dots = yx \dots$ (je m Faktoren) das Element maximaler Länge (vgl. Beispiel 10.12). Ist m gerade, so ist $\sigma(z) = -\text{id}$, also die Drehung um π .

(ii) Für $g \in G = S_n$ und $i < j$ gilt

$${}^g \left(\frac{1}{\sqrt{2}}(e_i - e_j) \right) < 0 \iff \frac{1}{\sqrt{2}}(e_{g(i)} - e_{g(j)}) < 0 \iff g(i) > g(j)$$

(Beispiel 10.12). Daher ist $l(g)$ die Anzahl der *Fehlstände* von g , also Paare $i < j$ mit ${}^g i > {}^g j$. Das Element maximaler Länge ist daher

$$g = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix} = (1, n)(2, n-1) \dots = t_1 \dots t_{n-1}$$

mit $t_i = (i+1, i) \dots (2, 1)$ und $l(g) = 1 + \dots + n-1 = n(n-1)/2 = |\Pi|$.

Lemma 10.27 (TITS). Sei $g \in G$ und $v \in \Pi$. Dann gilt $l(gx_v) > l(g) \iff {}^g v > 0$.

Beweis. Wie in Lemma 10.13 genügt es $l(gx_v) > l(g) \Rightarrow {}^g v > 0$ zu zeigen. Induktion nach $l(g)$. Der Fall $g = 1$ ist klar. Sei nun $l(g) > 0$ und $l(x_i g) < l(g)$. Wegen

$$l(x_i g x_v) \geq l(gx_v) - 1 > l(g) - 1 = l(x_i g)$$

gilt ${}^{x_i g} v > 0$ nach Induktionsvoraussetzung. Nehmen wir ${}^g v < 0$ an. Nach Satz 10.23 gilt dann ${}^g v = -b_i$. Dies zeigt ${}^{g^{-1}x_i g} v = {}^{g^{-1}} b_i = -v$ und $g^{-1}x_i g = x_v$ nach Bemerkung 10.11. Dies widerspricht aber $l(gx_v) > l(g) > l(x_i g) = l(gx_v)$. \square

Bemerkung 10.28. Im Folgenden benutzen wir die Schreibweise $x_1 \dots \check{x}_i \dots x_k := x_1 \dots x_{i-1} x_{i+1} \dots x_k$.

Satz 10.29.

- (i) (Austauschbedingung) Sei $g = x_{i_1} \dots x_{i_k} \in G$ und $v \in \Phi$ mit $l(gx_v) < l(g)$. Dann existiert $1 \leq s \leq k$ mit $gx_v = x_{i_1} \dots \check{x}_{i_s} \dots x_{i_k}$. Ist $l(g) = k$, so ist s eindeutig bestimmt.
- (ii) (Löschbedingung) Sei $g = x_{i_1} \dots x_{i_k} \in G$ mit $l(g) < k$. Dann existieren $1 \leq s < t \leq k$ mit $g = x_{i_1} \dots \check{x}_{i_s} \dots \check{x}_{i_t} \dots x_{i_k}$.

Beweis.

- (i) Wegen $x_v = x_{-v}$ können wir $v > 0$ annehmen. Aus Lemma 10.27 folgt ${}^g v < 0$. Wegen $v > 0$ existiert ein s mit ${}^{x_{i_{s+1}} \dots x_{i_k}} v > 0$ und ${}^{x_{i_s} \dots x_{i_k}} v < 0$. Aus Satz 10.23 folgt ${}^{x_{i_{s+1}} \dots x_{i_k}} v = b_{i_s}$. Dies zeigt $(x_{i_{s+1}} \dots x_{i_k})x_v(x_{i_{s+1}} \dots x_{i_k})^{-1} = x_{i_s}$, also $gx_v = x_{i_1} \dots \check{x}_{i_s} \dots x_{i_k}$. Sei nun $l(g) = k$. Angenommen es existieren $s < t$ mit $x_{i_1} \dots \check{x}_{i_s} \dots x_{i_k} = gx_v = x_{i_1} \dots \check{x}_{i_t} \dots x_{i_k}$. Dies liefert $x_{i_{s+1}} \dots x_{i_t} = x_{i_s} \dots x_{i_{t-1}}$ und $x_{i_s} \dots x_{i_t} = x_{i_{s+1}} \dots x_{i_{t-1}}$. Dann wäre aber $g = x_{i_1} \dots \check{x}_{i_s} \dots \check{x}_{i_t} \dots x_{i_k}$ und $l(g) < k$.
- (ii) Wegen $l(g) < k$ existiert ein t mit $l(x_{i_1} \dots x_{i_t}) < l(x_{i_1} \dots x_{i_{t-1}})$. Aus (i) folgt $x_{i_1} \dots x_{i_t} = x_{i_1} \dots \check{x}_{i_s} \dots x_{i_{t-1}}$ für ein $s < t$. \square

Bemerkung 10.30.

- (i) Es gilt

$$l(x_v g) < l(g) \implies l(g^{-1} x_v) < l(g^{-1}) \implies g^{-1} x_v = x_{i_k} \dots \check{x}_{i_s} \dots x_{i_1} \implies gx_v = x_{i_1} \dots \check{x}_{i_s} \dots x_{i_k}.$$

- (ii) Man kann zeigen, dass jede Gruppe, die die Austauschbedingung (oder Löschbedingung) bzgl. eines Erzeugendensystems von Involutionen erfüllt, eine Coxetergruppe ist.
- (iii) Die Löschbedingung zeigt, dass man aus einer beliebigen Darstellung $g = x_{i_1} \dots x_{i_k}$ durch suggestives Löschen eine reduzierte Darstellung erhält.

Definition 10.31.

- Man nennt G *irreduzibel*, falls keine Partition $\{1, \dots, n\} = I \dot{\cup} J$ mit $G = G_I \times G_J$ existiert.
- Der *Coextergraph* $C(G)$ besteht aus den Ecken e_1, \dots, e_n und den Kanten (e_i, e_j) mit $m_{ij} \geq 3$. Im Fall $m_{ij} > 3$ werden die Kanten mit m_{ij} beschriftet. Offenbar ist G durch $C(G)$ bis auf Reihenfolge der x_i eindeutig bestimmt.

Beispiel 10.32. Es gilt $C(S_n)$: $\bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet$ und $C(D_{2m})$: $\bullet \xrightarrow{m} \bullet$ nach Beispiel 10.4.

Satz 10.33. Genau dann ist G irreduzibel, falls $C(G)$ zusammenhängend ist.

Beweis. Ist $G = G_I \times G_J$, so gilt $m_{ij} = 2$ für $i \in I$ und $j \in J$. Also gibt es keinen Weg zwischen e_i und e_j in $C(G)$. Ist umgekehrt $C(G)$ unzusammenhängend, so existiert eine Partition $\{1, \dots, n\} = I \cup J$ mit $[x_i, x_j] = 1$ (Kommutator) für alle $i \in I$ und $j \in J$. Insbesondere ist $[G_I, G_J] = 1$. Nach Satz 10.22 ist $G = G_{I \cup J} = \langle G_I, G_J \rangle$ und $G_I \cap G_J = G_{I \cap J} = 1$. Dies zeigt $G = G_I \times G_J$. \square

Bemerkung 10.34. Achtung: Der Isomorphietyp von G bestimmt nicht, ob G als Coxetergruppe irreduzibel ist. Zum Beispiel ist $G = D_{12}$ irreduzibel mit zwei Erzeugern, aber auch reduzibel mit drei Erzeugern $G \cong D_6 \times S_2$.

Lemma 10.35. Sei G irreduzibel und $V_0 := \{v \in V : [v, V]_G = 0\} \leq V$. Dann operiert G trivial auf V_0 und jeder echte G -invariante Unterraum von V liegt in V_0 .

Beweis. Für $v \in V_0$ gilt $^{x_i}v = \sigma_i(v) = v - 2[v, b_i]_G b_i = v$. Da G von x_1, \dots, x_n erzeugt wird, operiert G trivial auf V_0 .

Sei nun $W < V$ G -invariant. Angenommen es existiert $v \in W \setminus V_0$. Dann existiert ein i mit $[v, b_i]_G \neq 0$. Es folgt $b_i = \frac{v - \sigma_i(v)}{2[v, b_i]_G} \in W$. Für b_j mit $m_{ij} \geq 3$ gilt $[b_i, b_j]_G \neq 0$ und $b_j = \frac{b_i - \sigma_j(b_i)}{2[b_i, b_j]_G} \in W$. Da $C(G)$ zusammenhängend ist, erhält man $b_1, \dots, b_n \in W$ im Widerspruch zu $W < V$. \square

Satz 10.36. Sei G eine endliche irreduzible Coxetergruppe und $z \in G$ mit maximaler Länge. Dann gilt $Z(G) \leq \langle z \rangle$. Insbesondere ist $|Z(G)| \leq 2$.

Beweis. Sei $g \in Z(G) \setminus \{1\}$. Aus $^{x_i}(gb_i) = ^{g x_i}b_i = -^g b_i$ folgt $^g b_i = \pm b_i$ (Satz 10.23). Daher ist $b_i \in E_1(\sigma(g)) \cup E_{-1}(\sigma(g))$ (Eigenräume zum Eigenwert 1 bzw. -1). Wegen $g \in Z(G)$ sind $E_1(\sigma(g))$ und $E_{-1}(\sigma(g))$ G -invariant und $E_1(\sigma(g)) < V$, da $g \neq 1$. Im Fall $E_{-1}(\sigma(g)) < V$ wäre $b_i \in V_0$ nach Lemma 10.35. Allerdings ist $[b_i, b_i]_G = 1$. Dies zeigt $\sigma(g) = -\text{id}$ und $^g v < v$ für alle $v \in \Pi$. Aus Satz 10.23 folgt $g = z$. \square

Lemma 10.37. Sei $H \leq \text{GL}(n, \mathbb{R})$ endlich und irreduzibel als Matrixgruppe. Dann gilt:

- (i) Es existiert eine H -invariante positiv definite Bilinearform auf \mathbb{R}^n .
- (ii) Angenommen es existieren $h \in H$ und $\lambda \in \mathbb{R}$, sodass der Eigenraum $E_\lambda(h)$ ungerade Dimension hat. Dann ist $C_{\text{GL}(n, \mathbb{R})}(H) = \mathbb{R}^\times 1_n$.²⁰ Insbesondere gilt dies, falls n ungerade ist.
- (iii) Ist $C_{\text{GL}(n, \mathbb{R})}(H) = \mathbb{R}^\times 1_n$, so unterscheiden sich je zwei nicht-ausgeartete H -invariante Bilinearform auf \mathbb{R}^n nur durch eine Konstante.

Beweis.

- (i) Für $v, w \in \mathbb{R}^n$ definiert

$$[v, w]_H := \sum_{h \in H} [hv, hw]$$

eine H -invariante positiv definite Bilinearform, wobei $[\cdot, \cdot]$ das Standardskalarprodukt ist.

- (ii) Sei $f \in C_{\text{GL}(n, \mathbb{R})}(H)$. Dann operiert f auf $E_\lambda(h)$. Da $\dim E_\lambda(h)$ ungerade ist, besitzt f auf $E_\lambda(h)$ einen reellen Eigenwert μ . Nun ist $0 \neq E_\mu(f) \leq \mathbb{R}^n$ H -invariant und es folgt $E_\mu(f) = \mathbb{R}^n$ sowie $f = \mu 1_n$, da H irreduzibel ist. Die zweite Aussage erhält man mit $h = 1$.

²⁰Man sagt: H ist absolut irreduzibel.

- (iii) Seien $[\cdot, \cdot]_1$ und $[\cdot, \cdot]_2$ zwei nicht-ausgeartete H -invariante Bilinearformen auf $V := \mathbb{R}^n$. Sei $V^* := \text{Hom}(V, \mathbb{R})$ der Dualraum von V . Dann sind $\varphi_i: V \rightarrow V^*$, $v \mapsto [v, \cdot]_i$ für $i = 1, 2$ Isomorphismen von Vektorräumen (beachte $\dim V = \dim V^*$). Also ist $f := \varphi_2^{-1} \circ \varphi_1: V \rightarrow V$ ein Isomorphismus mit $[v, w]_1 = [f(v), w]_2$ für alle $v, w \in V$. Für $h \in H$ folgt

$$[f(hv), hw]_2 = [hv, hw]_1 = [v, w]_1 = [f(v), w]_2 = [hf(v), hw]_2.$$

Dies zeigt $fh = hf$, d. h. $f \in \text{C}_{\text{GL}(n, \mathbb{R})}(H) = \mathbb{R}^\times 1_n$. \square

Bemerkung 10.38. Wir betrachten den Dualraum $V^* := \text{Hom}(V, \mathbb{R})$ mit der dualen Basis β_1, \dots, β_n , wobei $\beta_i(\beta_j) = \delta_{ij}$. Durch ${}^g\varphi(v) := \varphi(g^{-1}v)$ für $v \in V$, $\varphi \in V^*$ und $g \in G$ operiert G auf V^* . Die Abbildung $\Gamma: V \rightarrow V^*$, $v \mapsto [v, \cdot]_G$ vermittelt einen Isomorphismus zwischen den Operationen auf V und V^* , denn

$$({}^g\Gamma(v))(w) = \Gamma(v)({}^{g^{-1}}w) = [v, {}^{g^{-1}}w]_G = [{}^gv, w]_G = \Gamma({}^gv)(w)$$

für $v, w \in V$ und $g \in G$. Sei $\sigma^*: G \rightarrow \text{GL}(V^*)$ der entsprechende Monomorphismus. Wir definieren

$$C := \{\varphi \in V^* : \forall i : \varphi(\beta_i) > 0\} \subseteq V^*.$$

Bzgl. der dualen Basis ist $C = \mathbb{R}_{>0}^n$ eine offene Menge im euklidischen Raum \mathbb{R}^n . Da die Determinante $\mathbb{R}^{n \times n} \rightarrow \mathbb{R}$ stetig ist, ist $\text{GL}(V^*) = \det^{-1}(\mathbb{R} \setminus \{0\})$ offen in $\mathbb{R}^{n \times n}$.

Satz 10.39. *Das Bild $\sigma^*(G)$ ist eine diskrete Untergruppe von $\text{GL}(V^*)$, d. h. für alle $a \in \sigma^*(G)$ existiert eine offene Umgebung $U(a) \subseteq \text{GL}(V^*)$ mit $U(a) \cap \sigma^*(G) = \{a\}$. Insbesondere ist $\sigma^*(G)$ abgeschlossen.*

Beweis. Wir identifizieren G mit $\sigma^*(G)$. Sei $c \in C$ und $F: \text{GL}(V^*) \rightarrow V^*$, $a \mapsto {}^ac = a(c)$. Da die Matrix-Vektormultiplikation stetig ist, ist F stetig und $D := F^{-1}(C) \subseteq \text{GL}(V^*)$ ist eine offene Umgebung von $1 \in \text{GL}(V^*)$. Für $g \in G \setminus \{1\}$ existiert x_i mit $l(g^{-1}x_i) < l(g)$. Aus Tits Lemma folgt ${}^{g^{-1}}\beta_i < 0$ und ${}^gc(\beta_i) = c({}^{g^{-1}}\beta_i) < 0$. Dies zeigt $D \cap G = \{1\}$. Für ein beliebiges $g \in G$ ist gD eine offene Umgebung um g mit $gD \cap G = g(D \cap G) = \{g\}$.

Sei nun $(a_i) \subseteq G$ eine konvergente Folge. Dann existiert $k \in \mathbb{N}$ mit $a_i \in U(a_k) \cap G = \{a_k\}$ für alle $i \geq k$. Also wird die Folge konstant und der Grenzwert liegt in G . Dies zeigt, dass G abgeschlossen ist. \square

Satz 10.40. *Genau dann ist G endlich, wenn $[\cdot, \cdot]_G$ positiv definit auf V ist.*

Beweis. Sei G endlich. Wir argumentieren durch Induktion nach n . Im Fall $n = 1$ ist $[b_1, b_1]_G = 1$ und wir sind fertig. Sei $n > 1$. Nehmen wir an, dass $G = G_I \times G_J$ reduzibel ist. Dann gilt $V = V_I \oplus V_J$ mit $V_I := \langle \beta_i : i \in I \rangle$ und analog V_J . Nach Induktion sind $[\cdot, \cdot]_{G_I}$ und $[\cdot, \cdot]_{G_J}$ positiv definit auf V_I bzw. V_J . Für $i \in I$ und $j \in J$ gilt $[b_i, b_j]_G = -\cos \frac{\pi}{2} = 0$. Für $v = v_I + v_J \neq 0$ folgt

$$[v, v]_G = [v_I, v_I]_{G_I} + [v_J, v_J]_{G_J} > 0.$$

Also ist $[\cdot, \cdot]_G$ positiv definit auf V .

Sie nun G irreduzibel und $V_0 = \{v \in V : [v, V]_G = 0\} \leq V$. Nach Maschke besitzt V_0 ein G -invariantes Komplement $W \leq V$. Lemma 10.35 zeigt $W = V$ und $V_0 = 0$, d. h. $[\cdot, \cdot]_G$ ist nicht-ausgeartet. Das gleiche Argument zeigt auch, dass $\sigma(G)$ als Matrixgruppe irreduzibel ist. Wegen $\dim E_{-1}(\sigma(x_1)) = \dim E_{-1}(\sigma_1) = 1$ ist $[\cdot, \cdot]_G$ bis auf eine Konstante eindeutig bestimmt nach Lemma 10.37. Lemma 10.37 besagt aber auch, dass eine G -invariante positiv definite Bilinearform existiert. Also ist $[\cdot, \cdot]_G$ positiv definit.

Sei nun umgekehrt $[\cdot, \cdot]_G$ positiv definit. Durch den Isomorphismus $\Gamma: V \rightarrow V^*$, $v \mapsto [v, \cdot]_G$ aus Bemerkung 10.38 erhält man eine G -invariante positiv definite Bilinearform auf V^* (nämlich $[\varphi, \mu] := [\Gamma^{-1}(\varphi), \Gamma^{-1}(\mu)]_G$ für $\varphi, \mu \in V^*$). Nach Sylvesters Trägheitssatz besitzt V^* eine Orthonormalbasis Δ bzgl. dieser Bilinearform. Schreibt man $g \in \sigma^*(G)$ als Matrix bzgl. Δ , so haben die Spalten Norm 1. Da alle Normen auf dem \mathbb{R}^n äquivalent sind, ist $\sigma^*(G)$ beschränkt (bzgl. der euklidischen Norm). Nach Satz 10.39 ist $\sigma^*(G)$ zusätzlich abgeschlossen und daher kompakt. Für $a \in \sigma^*(G)$ wählen wir gemäß Satz 10.39 eine offene Umgebung $U(a) \subseteq \mathbb{R}^{n \times n}$ mit $U(a) \cap \sigma^*(G) = \{a\}$. Nach Heine-Borel überdeckt bereits eine endliche Auswahl dieser Umgebungen $\sigma^*(G)$. Daher muss $\sigma^*(G) \cong G$ endlich sein. \square

Satz 10.41. *Die endlichen Coxetergruppen sind genau die Spiegelungsgruppen.*

Beweis. Sei G eine endliche Coxetergruppe. Nach Satz 10.9 und Satz 10.14 ist $G \cong \sigma(G) \leq \text{GL}(V)$ eine Spiegelungsgruppe.

Sei nun umgekehrt $V := \mathbb{R}^n$ und $S \leq \text{GL}(V)$ eine Spiegelungsgruppe. Sei $\Phi \subseteq V$ die Menge der Einheitsvektoren b , sodass die Spiegelung σ_b an b^\perp in S liegt. Wir zeigen, dass Φ die Eigenschaften eines Wurzelsystems hat. Aus $|S| < \infty$ folgt $|\Phi| < \infty$. Wegen $b^\perp = (-b)^\perp$ ist $-\Phi = \Phi$. Wir ordnen die $b \in \Phi$ lexikografisch entsprechend der Koeffizienten bzgl. der Standardbasis von \mathbb{R}^n . Sei $\Pi := \{b \in \Phi : b > 0\}$ die Menge der *positiven Wurzeln* ($b > 0$ bedeutet, dass die erste von 0 verschiedene Komponente von b positiv ist). Dann gilt $\Phi = \Pi \cup (-\Pi)$. Sei $\Delta \subseteq \Phi$ eine minimale Teilmenge, sodass für alle $b \in \Pi$ Zahlen $\lambda_s \geq 0$ mit $b = \sum_{s \in \Delta} \lambda_s s$ existieren. Im Folgenden sei $[\cdot, \cdot]$ das Standardskalarprodukt auf \mathbb{R}^n .

Schritt 1: $[b, c] \leq 0$ für alle verschiedenen $b, c \in \Delta$.

Angenommen $[b, c] > 0$. Für $\mu := 2[b, c] > 0$ gilt $\sigma_b(c) = c - \mu b$. Wegen $\sigma_b \sigma_c \sigma_b = \sigma_{\sigma_b(c)} \in S$ gilt $\sigma_b(c) \in \Phi$. Sei zunächst $\sigma_b(c) \in \Pi$. Dann existieren $\lambda_s \geq 0$ mit $\sigma_b(c) = \sum_{s \in \Delta} \lambda_s s$. Im Fall $\lambda_c < 1$ erhält man

$$(1 - \lambda_c)c = \sigma_b(c) + \mu b - \lambda_c c = \mu b + \sum_{s \neq c} \lambda_s s.$$

Nun könnte man aber c aus Δ entfernen im Widerspruch zur Minimalität von Δ . Also gilt $\lambda_c \geq 1$ und

$$(\lambda_c - 1)c + \mu b + \sum_{s \neq c} \lambda_s s = 0.$$

Wegen $\mu > 0$ widerspricht dies aber der Definition von Π . Dies zeigt $-\sigma_b(c) \in \Pi$. Mit $-\sigma_b(c) = \sum_{s \in \Delta} \lambda_s s$ folgt

$$(\mu - \lambda_b)b = -\sigma_b(c) + c - \lambda_b b = c + \sum_{s \neq b} \lambda_s s.$$

Im Fall $\lambda_b < \mu$ könnte man b aus Δ entfernen. Also ist $\lambda_b \geq \mu$. Dann wäre aber

$$(\lambda_b - \mu)b + c + \sum_{s \neq b} \lambda_s s = 0$$

ein Widerspruch zur Definition von Π . Insgesamt muss also $[b, c] \leq 0$ gelten.

Schritt 2: Δ ist linear unabhängig.

Sei $\sum_{s \in \Delta} \lambda_s s = 0$ mit $\lambda_s \in \mathbb{R}$ für $s \in \Delta$. Trennen der positiven und negativen Koeffizienten liefert $b := \sum_{\lambda_s \geq 0} \lambda_s s = -\sum_{\lambda_t < 0} \lambda_t t$. Aus Schritt 2 folgt

$$0 \leq [b, b] = \sum_{\lambda_s \geq 0} \sum_{\lambda_t < 0} \lambda_s (-\lambda_t) [s, t] \leq 0$$

und $b = 0$. Da b eine nicht-negative Linearkombination positiver Wurzeln ist, folgt $\lambda_s = 0$ für alle $s \in \Delta$.

Schritt 3: $S = \langle \sigma_b : b \in \Delta \rangle$.

Nach Schritt 2 lässt sich jede Wurzel in Φ eindeutig als Linearkombination von Δ schreiben, wobei entweder alle Koeffizienten nicht-negativ oder alle Koeffizienten nicht-positiv sind. Sei $T := \langle \sigma_b : b \in \Delta \rangle \leq S$ und $b \in \Pi$. Unter allen Elementen in der Bahn ${}^T b$ wählen wir $c = \sum_{s \in \Delta} \lambda_s s \in \Pi$, sodass $h(c) := \sum_{s \in \Delta} \lambda_s$ möglichst klein ist. Nehmen wir $c \notin \Delta$ an. Wegen $1 = [c, c] = \sum_{s \in \Delta} \lambda_s [c, s]$ existiert ein $t \in \Delta$ mit $[c, t] > 0$. Es gilt $\sigma_t(c) = c - 2[c, t]t$. Wegen $c \in \Pi \setminus \Delta$ ist c kein Vielfaches von t . Nach Schritt 2 ist die Darstellung von $\sigma_t(c)$ bzgl. Δ eindeutig. Wegen $\Phi = \Pi \cup (-\Pi)$ kann es keine Koeffizienten mit verschiedenen Vorzeichen geben. Dies zeigt $\lambda_t \geq 2[c, t]$ und man hat den Widerspruch $h(\sigma_t(c)) < h(c)$ zur Wahl von c . Also ist $c \in \Delta$ und es existiert $t \in T$ mit $b = t(c)$. Wie bereits bemerkt folgt $\sigma_b = t\sigma_c t^{-1} \in T$. Also gilt $S = \langle \sigma_b : b \in \Pi \rangle = T$.

Schritt 4: S ist eine Coxetergruppe.

Sei $\Delta = \{b_1, \dots, b_n\}$ und $\sigma_i = \sigma_{b_i}$ für $i = 1, \dots, n$. Sei $|\langle \sigma_i \sigma_j \rangle| = m_{ij}$ für $1 \leq i, j \leq n$. Nach Schritt 2 ist $m_{ij} \geq 2$ für $i \neq j$. Ggf. ist $\sigma_i \sigma_j$ eine Drehung um den Winkel $\varphi := 2\pi/m_{ij} \leq \pi$ in der Ebene $\langle b_i, b_j \rangle$. Es folgt

$$\begin{aligned} \cos \varphi &= [b_j, \sigma_i \sigma_j(b_j)] = -[b_j, \sigma_i(b_j)] = -[b_j, b_j - 2[b_j, b_i]b_i] = -1 + 2[b_i, b_j]^2, \\ [b_i, b_j]^2 &= \frac{\cos \varphi + 1}{2} = \frac{\cos(\varphi/2)^2 - \sin(\varphi/2)^2 + 1}{2} = \cos(\varphi/2)^2. \end{aligned}$$

Aus Schritt 1 erhält man $[b_i, b_j] = -\cos(\varphi/2) = -\cos(\pi/m_{ij})$. Sei $G = \langle x_1, \dots, x_n \rangle$ die Coxetergruppe mit den Parametern m_{ij} . Mit den Bezeichnungen aus Definition 10.8 ist nun $[\cdot, \cdot]_G$ das Standardskalarprodukt und der Monomorphismus σ aus Satz 10.9 bildet G nach S ab. Wegen Schritt 3 ist σ surjektiv und $S \cong G$ ist eine Coxetergruppe. \square

Bemerkung 10.42.

- (i) Genau dann ist G endlich, wenn die Matrix $(-\cos(\pi/m_{ij}))_{ij}$ positiv definit ist. Für $G = S_n$ erhält man die Matrix

$$\begin{pmatrix} 1 & -1/2 & & 0 \\ -1/2 & \ddots & \ddots & \\ & \ddots & 1 & -1/2 \\ 0 & & -1/2 & 1 \end{pmatrix}.$$

- (ii) Im Folgenden nennen wir G *positiv semidefinit*, falls $[\cdot, \cdot]_G$ positiv semidefinit ist. Insbesondere ist jede endliche Coxetergruppe positiv semidefinit.

Lemma 10.43. Sei $A = (a_{ij}) \in \mathbb{R}^{n \times n}$ symmetrisch, positiv semidefinit und unzerlegbar (d. h. zu jeder Partition $\{1, \dots, n\} = I \dot{\cup} J$ existieren $i \in I, j \in J$ mit $a_{ij} \neq 0$). Für $i \neq j$ sei außerdem $a_{ij} \leq 0$. Dann gilt

- (i) $\text{Ker}(A) = \{v \in \mathbb{R}^n : vAv^t = 0\}$ und $\dim \text{Ker}(A) \leq 1$.

- (ii) Der Eigenraum zum kleinsten Eigenwert von A wird von einem positiven Eigenvektor (d. h. alle Komponenten sind positiv) aufgespannt.

Beweis.

- (i) Sicher liegt $\text{Ker}(A)$ in $N := \{v \in \mathbb{R}^n : vAv^t = 0\}$. Sei umgekehrt $v \in N$. Nach dem Spektralsatz existiert eine orthogonale Matrix S mit $D := SAS^t = \text{diag}(d_1, \dots, d_n)$ und $d_1, \dots, d_n \geq 0$. Für $w := vS^t$ folgt

$$\sum_{i=1}^n w_i^2 d_i = wDw^t = vAv^t = 0.$$

Also ist $w_i = 0$ oder $d_i = 0$ für alle i . Dies zeigt $0 = S^t Dw^t = Av^t$ und $N \subseteq \text{Ker}(A)$.

Sei nun $x \in N \setminus \{0\}$ und $z = (|x_1|, \dots, |x_n|)$. Wegen $a_{ij} \leq 0$ für $i \neq j$ gilt

$$0 \leq zAz^t = \sum_{i,j=1}^n a_{ij}|x_i x_j| \leq \sum_{i,j=1}^n a_{ij}x_i x_j = xAx^t = 0,$$

also $z \in N$. Sei $I := \{1 \leq i \leq n : z_i = 0\}$ und $J = \{1, \dots, n\} \setminus I$. Aus $z \in \text{Ker}(A)$ folgt $\sum_{j \in J} a_{ij}z_j = 0$ für $i = 1, \dots, n$. Wegen $z_j > 0$ geht dies nur falls $a_{ij} = 0$ für alle $i \in I$ und $j \in J$. Da A unzerlegbar ist, muss $I = \emptyset$ gelten, d. h. alle Komponenten von z sind positiv und alle Komponenten von x sind ungleich 0. Da $x \neq 0$ beliebig war, schließen wir $\dim N \leq 1$ (anderenfalls könnte man aus zwei linear unabhängigen Vektoren eine Linearkombination mit 0-Komponente kombinieren).

- (ii) Sei $d := \min\{d_1, \dots, d_n\} \geq 0$. Dann erfüllt auch $B := A - d1_n$ die Voraussetzungen des Satzes. Die Behauptung folgt nun aus dem Beweis von (i) für B . \square

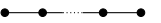
Lemma 10.44. *Sei G irreduzibel und positiv semidefinit. Wir konstruieren aus $C(G)$ einen echten Teilgraphen D , indem wir Ecken oder Kanten entfernen oder Kantengewichte reduzieren. Dann ist die Coxetergruppe zu D endlich.*

Beweis. Wir nummerieren die Ecken von $C(G)$, sodass D aus den ersten k Ecken gebildet wird. Seien $A = (a_{ij}) = ([b_i, b_j]_G) \in \mathbb{R}^{k \times k}$ und $B = (b_{ij}) = (-\cos(\pi/m'_{ij})) \in \mathbb{R}^{k \times k}$ die entsprechenden Matrizen. Dann gilt $b_{ij} \geq -\cos(\pi/m_{ij}) = a_{ij}$. Angenommen B ist nicht positiv definit. Sei $v \in \mathbb{R}^k \setminus \{0\}$ mit $vBv^t \leq 0$ und $w = (|v_1|, \dots, |v_k|, 0, \dots, 0) \in \mathbb{R}^n$. Da G positiv semidefinit ist, folgt

$$0 \leq wAw^t = \sum_{i,j=1}^k a_{ij}|v_i||v_j| \leq \sum_{i,j=1}^k b_{ij}|v_i||v_j| \leq \sum_{i,j=1}^k b_{ij}v_i v_j = vBv^t \leq 0$$


und $wAw^t = 0$. Nach Lemma 10.43 sind alle Komponenten von w positiv, d. h. $k = n$ und $v_i \neq 0$ für $i = 1, \dots, k$. Daraus ergibt sich $a_{ij} = b_{ij}$. Nun ist D aber kein echter Teilgraph mehr. Widerspruch. \square


Satz 10.45 (COXETER). *Jede endliche irreduzible Coxetergruppe G gehört zu einer der folgenden Familien.²¹*


(A_n)  mit $n \geq 1$.

(B_n)  mit $n \geq 2$.

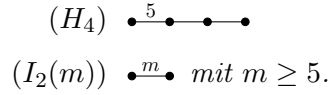
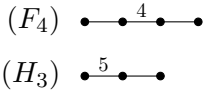
(D_n)  mit $n \geq 4$.

(E_6) 

(E_7) 

(E_8) 

²¹Diese speziellen Graphen heißen *Dynkin-Diagramme*.



Beweis.

Existenz: Da die angegebenen Graphen zusammenhängend sind, sind die entsprechenden Gruppen irreduzibel (Satz 10.33). Wir zeigen, dass sie alle endlich sind. Alle Graphen sind Bäume. Entfernt man ein geeignetes Blatt, so erhält man einen Baum, der auch einen der angegebenen Typen besitzt. Wir können daher durch Induktion argumentieren und müssen nur zeigen, dass die Matrix $M := 2([b_i, b_j])$ positive Determinante hat (Sylvester-Kriterium). Für $n = 2$ erhält man

$$\det M = 4(1 - \cos(\pi/m)^2) = 4 \sin(\pi/m)^2 > 0$$

wegen $m = m_{12} \geq 3$. Sei nun $n \geq 3$. Wir nummerieren die Ecken e_1, \dots, e_n , sodass e_n ein Blatt ist und die dazugehörige Kante $\{e_{n-1}, e_n\}$ Gewicht $m = 3$ oder 4 hat. Laplace-Entwicklung nach der letzten Spalte zeigt

$$\det M = 2 \det M_{n-1} - 4 \cos(\pi/m)^2 \det M_{n-2} = 2 \det M_{n-1} - \lambda \det M_{n-2}$$

mit $\lambda \in \{1, 2\}$, denn $\cos(\pi/3) = 1/2$ und $\cos(\pi/4) = 1/\sqrt{2}$. Unter Benutzung von $\sin(\pi/5) = \sqrt{10 - 2\sqrt{5}}/4$ berechnet man induktiv

$$(A_n): \det M = 2n - (n - 1) = n + 1,$$

$$(B_n): \det M = 2 \cdot 2 - 2 = 2,$$

$$(D_n): \det M = 2 \cdot 4 - 4 = 4,$$

$$(E_6): \det M = 2 \cdot 4 - 5 = 3,$$

$$(E_7): \det M = 2 \cdot 3 - 4 = 2,$$

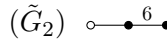
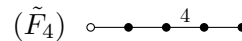
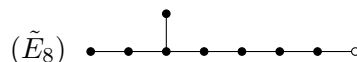
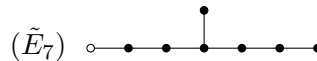
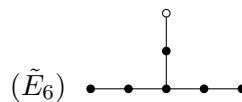
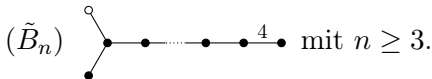
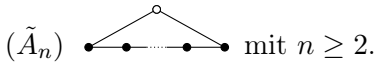
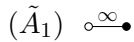
$$(E_8): \det M = 2 \cdot 2 - 3 = 1,$$

$$(F_4): \det M = 2 \cdot 2 - 3 = 1,$$

$$(H_3): \det M = 2 \cdot 4 \sin(\pi/5)^2 - 2 = \frac{10 - 2\sqrt{5} - 4}{2} = 3 - \sqrt{5} > 0,$$

$$(H_4): \det M = 2(3 - \sqrt{5}) - 4 \sin(\pi/5)^2 = \frac{12 - 4\sqrt{5} - 5 + \sqrt{5}}{2} = \frac{7 - 3\sqrt{5}}{2} > 0.$$

Hilfsgraphen: Wir fügen an einige der Graphen eine weitere Ecke hinzu und erhalten die folgenden Coxetergraphen²² (die Anzahl der Ecken ist nun $n + 1$):



²²Die Bezeichnungen sind in der Literatur nicht einheitlich.

Wir zeigen, dass die entsprechende Bilinearform positiv semidefinit, aber nicht positiv definit ist. Für \tilde{A}_n sind die Zeilensummen von M alle $2 - 1 - 1 = 0$, d.h. 0 ist ein Eigenwert und $\det M = 0$. In allen anderen Fällen kann man obige Rekursionsformel anwenden (beachte $\sin(\pi/6) = 1/2$):

$$\begin{aligned}(\tilde{B}_n): \det M &= 2 \cdot 2 - 2 \cdot 2 = 0, \\(\tilde{C}_n): \det M &= 2 \cdot 2 - 2 \cdot 2 = 0, \\(\tilde{D}_n): \det M &= 2 \cdot 4 - 2 \cdot 4 = 0, \\(\tilde{E}_6): \det M &= 2 \cdot 3 - 6 = 0, \\(\tilde{E}_7): \det M &= 2 \cdot 2 - 4 = 0, \\(\tilde{E}_8): \det M &= 2 \cdot 1 - 2 = 0, \\(\tilde{F}_4): \det M &= 2 \cdot 1 - 2 = 0, \\(\tilde{G}_2): \det M &= 2 \cdot 1 - 2 = 0.\end{aligned}$$

Fügt man eine Ecke zu H_3 und H_4 hinzu, so erhält man folgende Coxetergraphen:

$$(Z_4): \circ \text{---} \overset{5}{\bullet} \text{---} \bullet \quad (Z_5): \bullet \text{---} \overset{5}{\bullet} \text{---} \bullet \text{---} \bullet \text{---} \circ$$

Wegen

$$\begin{aligned}(Z_4): \det M &= 2(3 - \sqrt{5}) - 3 = 3 - 2\sqrt{5} < 0, \\(Z_5): \det M &= 7 - 3\sqrt{5} - (3 - \sqrt{5}) = 4 - 2\sqrt{5} < 0\end{aligned}$$

sind die entsprechenden Bilinearformen nicht mehr positiv semidefinit.

Eindeutigkeit: Sei nun G eine endliche irreduzible Coxetergruppe vom Rang n . Sei m das größte Kantengewicht. Nehmen wir an, dass $C(G)$ nicht zu den oben beschriebenen positiv (semi)definiten Graphen gehört.

- (1) Da alle zusammenhängenden Graphen mit $n = 2$ bereits aufgelistet wurden, gilt $n \geq 3$.
- (2) Nach Lemma 10.44 ist \tilde{A}_1 kein Teilgraph von $C(G)$ und daher $m < \infty$.
- (3) Da \tilde{A}_k kein Teilgraph ist, muss $C(G)$ ein Baum sein. Nehmen wir zunächst $m = 3$ an.
- (4) Wegen $C(G) \neq A_n$ besitzt $C(G)$ einen Verzweigungspunkt.
- (5) Da \tilde{D}_k kein Teilgraph ist, gibt es genau einen Verzweigungspunkt e .
- (6) Da \tilde{D}_4 kein Teilgraph ist, besitzt e genau drei Äste. Seien $a \leq b \leq c$ die Anzahl der Ecken der drei Äste.
- (7) Da \tilde{E}_6 kein Teilgraph ist, ist $a = 1$.
- (8) Da \tilde{E}_7 kein Teilgraph ist, ist $b \leq 2$.
- (9) Wegen $C(G) \neq D_n$ ist $b = 2$.
- (10) Da \tilde{E}_8 kein Teilgraph ist, ist $c \leq 4$.
- (11) Da $C(G)$ weder E_6 , E_7 noch E_8 ist, kann der Fall $m = 3$ nicht eintreten. Sei also $m \geq 4$.
- (12) Da \tilde{C}_k kein Teilgraph ist, kann es nur eine Kante mit Gewicht > 3 geben.
- (13) Da \tilde{B}_k kein Teilgraph ist, gibt es keine Verzweigungspunkte, d.h. $C(G)$ ist eine Linie. Nehmen wir nun $m = 4$ an.

(14) Wegen $C(G) \neq B_n$ haben die beiden äußeren Kanten Gewicht 3.

(15) Da \tilde{F}_4 kein Teilgraph ist, muss $n = 4$ gelten.

(16) Wegen $C(G) \neq F_4$ kann $m = 4$ nicht gelten. Sei also $m \geq 5$.

(17) Da \tilde{G}_2 kein Teilgraph ist, gilt $m = 5$.

(18) Da Z_4 kein Teilgraph ist, muss eine äußere Kante Gewicht m haben.

(19) Da Z_5 kein Teilgraph ist, muss $n \leq 4$ gelten.

(20) Nun wäre aber $C(G)$ gleich H_3 oder H_4 . Widerspruch. \square

Satz 10.46. Für die Gruppen in Satz 10.45 gilt

$$(A_n) \quad G \cong S_{n+1}$$

$$(E_8) \quad G = 2.\Omega^+(8, 2).2 \text{ mit } |G| = 696.729.600 = 2^{14}3^55^27.$$

$$(B_n) \quad G \cong C_2 \wr S_n.$$

$$(F_4) \quad G \cong (C_2^3 \rtimes S_4) \rtimes S_3.$$

$$(E_6) \quad G \cong \text{Aut}(\text{SU}(4, 2)) \cong \text{SU}(4, 2) \rtimes C_2 \text{ mit } |G| = 51.840 = 2^73^45.$$

$$(H_3) \quad G \cong A_5 \times C_2.$$

$$(E_7) \quad G \cong \text{Sp}(6, 2) \times C_2 \text{ mit } |G| = 2.903.040 = 2^{10}3^45 \cdot 7.$$

$$(H_4) \quad |G| = 14.400 = 2^63^25^2.$$

$$(I_2(m)) \quad G \cong D_{2m}.$$

Beweisskizze. Für (A_n) und $(I_2(m))$ ist die Behauptung aus Beispiel 10.32 bekannt. Da $[\cdot, \cdot]_G$ positiv definit ist, stimmt $[\cdot, \cdot]_G$ bis auf Basiswahl mit dem Standardskalarprodukt auf \mathbb{R}^n überein. Wir wählen konkrete Vektoren b_1, \dots, b_n mit den vorgegebenen Werten $[b_i, b_j]$ und bestimmen $\sigma(G)$ explizit. Sei e_1, \dots, e_n die Standardbasis von \mathbb{R}^n .

(B_n) Definiere $b_i := \frac{1}{\sqrt{2}}(e_i - e_{i+1})$ für $i = 1, \dots, n-1$ und $b_n = e_n$. Es gilt $[b_i, b_i] = 1$, $[b_i, b_j] = 0$ für $|j - i| > 1$, $[b_i, b_{i+1}] = -1/2 = -\cos(\pi/3)$ für $i = 1, \dots, n-2$ und $[b_{n-1}, b_n] = -1/\sqrt{2} = -\cos(\pi/4)$ wie gewünscht. Es gilt $b_i^\perp = \langle e_j, e_i + e_{i+1} : j \neq i \rangle$. Bezüglich e_1, \dots, e_n entspricht $\sigma(x_i)$ der Permutationsmatrix zur Transposition $(i, i+1)$ für $i = 1, \dots, n-1$ und $\sigma(x_n) = \text{diag}(1, \dots, 1, -1)$. Daher ist $\sigma(G)$ die Gruppe der vorzeichenbehafteten Permutationsmatrizen. Dies zeigt $G \cong C_2 \wr S_n$.

(D_n) Definiere $b_i := \frac{1}{\sqrt{2}}(e_i - e_{i+1})$ für $i = 1, \dots, n-1$ und $b_n = \frac{1}{\sqrt{2}}(e_{n-1} + e_n)$. Es gilt $[b_{n-2}, b_{n-1}] = [b_{n-2}, b_n] = -1/2$ und $[b_{n-1}, b_n] = 0$. Wieder sind $\sigma(x_i)$ für $i < n$ Permutationsmatrizen und

$$\sigma(x_n) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & -1 \\ & & & -1 & 0 \end{pmatrix}.$$

Daher besteht $\sigma(G)$ aus den vorzeichenbehafteten Permutationsmatrizen mit einer geraden Anzahl von -1 -Einträgen. Die entsprechenden Diagonalmatrizen bilden einen Normalteiler C_2^{n-1} mit Komplement S_n in G .

(H_3) Für $x := x_3x_2$, $y := x_2x_1$ gilt $|\langle x \rangle| = 3$, $|\langle y \rangle| = 5$ und $|\langle xy \rangle| = 2$. Nach Beispiel 2.16 existiert ein Epimorphismus $A_5 \rightarrow \langle x, y \rangle =: H$. Da A_5 einfach ist, folgt $H \cong A_5$. Aus $\sigma(H) \leq \text{SL}(3, \mathbb{R})$ und $\det(\sigma_1) = -1$ ergibt sich $|G| = 2|H| = 120$. Nach Bemerkung 6.3 gilt $G \in \{S_5, A_5 \times C_2\}$. Im Fall $G \cong S_5$ wäre $D_{10} \cong \langle x_1, x_2 \rangle \leq A_5$ im Widerspruch zu $\det(x_1) = -1$.

Die anderen Fällen sind recht aufwendig und können mit GAP behandelt werden:

```
for para in [{"E",6}, {"E",7}, {"E",8}, {"F",4}] do
  L:=SimpleLieAlgebra(para[1],para[2],Rationals);
  R:=RootSystem(L);;
  W:=WeylGroup(R);
  Print(para, " ", Order(W), "\n");
od;
F:=FreeGroup("a","b","c","d");;
AssignGeneratorVariables(F);
H4:=F/[a^2,b^2,c^2,d^2,(a*b)^5,(b*c)^3,(c*d)^3,Comm(a,c),Comm(a,d),Comm(b,d)];
#Comm(a,b)=[a,b]
Size(H4);
```

□

Bemerkung 10.47.

- (i) Die Matrix -1_n liegt offenbar im Zentrum der Coxetergruppe $G \cong C_2^n \rtimes S_n$ vom Typ (B_n) (Permutationsmatrizen mit Vorzeichen). Nach Satz 10.36 ist $Z(G) = \langle -1_n \rangle$. Wenn n ungerade ist, gilt $G = Z(G) \times H$, wobei H zur Coxetergruppe vom Typ (D_n) isomorph ist (Permutationsmatrizen mit einer geraden Anzahl an -1 -Einträgen). Dennoch ist G irreduzibel. Für $n = 3$ erhält man

$$G \cong C_2 \times (C_2^2 \rtimes S_3) \cong C_2 \times S_4.$$

Diese Gruppe permutiert die acht Eckpunkte des Würfels $(\pm 1, \pm 1, \pm 1)$ und ist daher dessen Symmetriegruppe (und des Oktaeders mit Ecken $(\pm 1, 0, 0)$, $(0, \pm 1, 0)$, $(0, 0, \pm 1)$). Für $n \geq 4$ erhält man die Symmetriegruppe des n -dimensionalen Hyperwürfels. Die Coxetergruppe $H \cong C_2^2 \rtimes S_3 \cong S_4$ vom Typ (D_3) permutiert die vier Eckpunkte $(1, 1, 1)$, $(1, -1, -1)$, $(-1, 1, -1)$, $(-1, -1, 1)$ des Tetraeders und ist daher dessen Symmetriegruppe. Bekanntlich ist S_4 auch die Coxetergruppe vom Typ (A_3) .

- (ii) Man kann zeigen, dass die Coxetergruppe vom Typ (H_3) die Symmetriegruppe des Dodekaeders (bzw. des Ikosaeders) ist. Die Coxetergruppe vom Typ (F_4) ist eine Erweiterung der Gruppe vom Typ (D_4) mit S_3 . Die Coxetergruppe vom Typ (E_7) ist eine Schur-Erweiterung der orthogonalen Gruppe $GO^+(8, 2) \cong \Omega^+(8, 2).2$ mit Zentrum C_2 .
- (iii) Eine (komplexe) *Lie-Algebra* ist ein endlich-dimensionaler \mathbb{C} -Vektorraum L mit einer alternierenden bilinearen Abbildung $L \times L \rightarrow L$, $(v, w) \mapsto [v, w]$, die die *Jacobi-Identität*

$$[u, [v, w]] + [v, [w, u]] + [w, [u, v]] = 0$$

erfüllt. Zum Beispiel $L = \mathbb{C}^{n \times n}$ mit $[v, w] := vw - wv$. Man nennt L *einfach*, falls $[L, L] \neq 0$ und falls kein Unterraum $0 < U < L$ mit $[L, U] \subseteq U$ existiert. Die Klassifikation der einfachen Lie-Algebren führt auf die Diagramme $A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4$ und G_2 . Diese entsprechen mehr oder weniger den einfachen Gruppen vom Lie-Typ (zum Beispiel entspricht A_n der Familie $\text{PSL}(n+1, q)$ und C_n der Familie $\text{PSp}(2n, q)$).

- (iv) Man nennt $\sigma \in \text{GL}(\mathbb{C}^d)$ eine *komplexe Spiegelung*, falls $|\langle \sigma \rangle| < \infty$ und $\dim \text{Ker}(\sigma - \text{id}) = d - 1$. Eine *komplexe Spiegelungsgruppe* ist eine endliche Untergruppe $G \leq \text{GL}(\mathbb{C}^d)$, die von komplexen Spiegelungen erzeugt wird. Jede Spiegelungsgruppe ist offenbar auch eine komplexe Spiegelungsgruppe. Shephard und Todd haben die irreduziblen komplexen Spiegelungsgruppen vollständig klassifiziert. Abgesehen von 34 Ausnahmen hat jede solche Gruppe die Form

$$G(m, d, n) := \langle (x_1, \dots, x_n; \sigma) \in C_m \wr S_n : (x_1 \dots x_n)^{m/d} = 1 \rangle,$$

wobei $n, m, d \in \mathbb{N}$ und $d \mid m$. Offenbar ist $G(m, 1, 1) \cong C_m$, $G(1, 1, n) \cong S_n$, $G(2, 1, n) \cong C_2 \wr S_n$ (Typ (B_n)), $G(2, 2, n)$ Typ (D_n) und $G(m, m, 2) \cong D_{2m}$ (Typ $(I_2(m))$). Die 34 Ausnahme-Gruppen sind leider nur in der alten GAP-Version 3 verfügbar.²³

Definition 10.48. Für $a, b, c \in \mathbb{Z} \setminus \{0\}$ nennt man

$$D(a, b, c) := \langle x, y \mid x^a = y^b = (xy)^c = 1 \rangle$$

eine *von-Dyck-Gruppe*.

Lemma 10.49. $D(a, b, c)$ hängt nicht von der Reihenfolge und der Vorzeichen von a, b, c ab.

Beweis. Die Unabhängigkeit vom Vorzeichen ist offensichtlich. Sei also $a, b, c \geq 1$. Wegen $(xy)^c = 1 \iff (yx)^c = 1$ kann man a und b vertauschen. Sei nun $x' := xy$ und $y' := y^{-1}$. Dann ist $x^a = y^b = (xy)^c = 1$ äquivalent zu $(x')^c = (y')^b = (x'y')^a = 1$. Also kann man auch a und c vertauschen. \square

Satz 10.50. Genau dann ist $D(a, b, c)$ endlich, wenn $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} > 1$. Ggf. tritt einer der folgenden Fälle ein:

- (i) $D(1, b, c) \cong C_{\text{ggT}(b, c)}$.
- (ii) $D(2, 2, c) \cong D_{2c}$.
- (iii) $D(2, 3, 3) \cong A_4$.
- (iv) $D(2, 3, 4) \cong S_4$.
- (v) $D(2, 3, 5) \cong A_5$.

Beweis. Nach Lemma 10.49 können wir $1 \leq a \leq b \leq c$ annehmen. Sei zunächst $a = 1$. Nach Euklid existieren $\alpha, \beta \in \mathbb{Z}$ mit $\text{ggT}(b, c) = \alpha b + \beta c$. Also ist $y^{\text{ggT}(b, c)} = (y^b)^\alpha + (y^c)^\beta = 1$ in $D(1, b, c)$. Es folgt $|D(1, b, c)| \leq \text{ggT}(b, c)$. Umgekehrt erfüllt auch $C_{\text{ggT}(b, c)}$ die Relationen von $D(1, b, c)$. Also gilt (i).

Im Fall $a = b = 2$ folgt die Behauptung aus Beispiel 1.17. Der Fall $(a, b, c) = (2, 3, 3)$ wurde in Aufgabe 2 behandelt.

Sei $(a, b, c) = (2, 3, 4)$ und $G := \langle x, y \mid x^4 = y^2 = (xy)^3 = 1 \rangle \cong D(2, 3, 4)$ und $H := \langle x \rangle \leq G$. Wir betrachten die Nebenklassen

$$H, yH, xyH, x^2yH, x^3yH, yx^2yH.$$

Wegen $xyx = yx^{-1}y$ und $xyx^2y = yx^{-1}yxy = yx^2xyxy = yx^2yx^{-1}$ werden die Nebenklassen durch Linksmultiplikation von x permutiert. Wegen $xyy = x^{-1}yx^{-1} = x^3yx^3$ permutiert auch y diese Nebenklassen und wir sehen, dass jedes Element in G in einer dieser Nebenklassen enthalten ist. Also ist $|G| \leq |G : H| |H| \leq 24$. Andererseits sieht man, dass $x' := (1, 2, 3, 4)$ und $y' := (1, 2)$ in S_4 auch

²³<https://webusers.imj-prg.fr/~jean.michel/gap3/>

die Relationen von G erfüllen. Dies liefert (iv). Der Fall $(a, b, c) = (2, 3, 5)$ wurde bereits mehrfach behandelt (Bemerkung 1.18, Beispiel 2.16). Man sieht leicht, dass in allen anderen Fällen $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} \leq 1$ gilt.

Sei

$$H := \langle u, v, w \mid u^2 = v^2 = w^2 = (uv)^a = (vw)^b = (uw)^c = 1 \rangle$$

eine Coxetergruppe. Offenbar ist $N := \langle uv, vw \rangle \leq H$ mit $|H : N| = 2$. Außerdem existiert ein Epimorphismus $D(a, b, c) \rightarrow N$. Es genügt also zu zeigen, dass H unendlich ist für $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} \leq 1$. Im Fall $a \geq 3$ ist $C(H)$ ein Kreis und $|H| = \infty$ nach Satz 10.45. Sei also $a = 2$ und $\frac{1}{b} + \frac{1}{c} \leq \frac{1}{2}$. Dann ist $b, c \geq 3$ und H ist irreduzibel. Für $b = 3$ ist $c \geq 6$ und die Behauptung folgt in jedem Fall aus Satz 10.45. \square

Bemerkung 10.51. Eine endliche Gruppe $G \neq 1$ heißt *Hurwitz-Gruppe*, falls $G = \langle x, y \rangle$ mit $x^2 = y^3 = (xy)^7 = 1$ gilt. Dies sind also genau die endlichen nicht-trivialen Faktorgruppen der unendlichen von-Dyck-Gruppe $D(2, 3, 7)$. Nach Aufgabe 36 sind alle Hurwitz-Gruppen perfekt und tatsächlich sind viele einfache Gruppen, u. a. A_n für $n \geq 168$, $\mathrm{GL}(3, 2)$ und die sporadische *Monstergruppe* Hurwitz-Gruppen.

Satz 10.52. Für $n \in \mathbb{N}$ gibt es unendlich viele Primzahlen $p \equiv 1 \pmod{n}$.²⁴

Beweis. Seien p_1, \dots, p_s Primzahlen mit $p_i \equiv 1 \pmod{n}$ für $i = 1, \dots, s$ (der Fall $s = 0$ ist zugelassen). Sei $m := np_1 \dots p_s$. Das Kreisteilungspolynom Φ_m induziert als normiertes Polynom eine unbeschränkte Funktion $\mathbb{R} \rightarrow \mathbb{R}$. Daher existiert ein $k \in \mathbb{N}$ mit $\Phi_m(km) > 1$. Sei p ein Primteiler von $\Phi_m(km)$. Wegen $\Phi_m(km) \mid ((km)^m - 1)$ ist $p \nmid m$ und die Ordnung r von $mk + p\mathbb{Z} \in \mathbb{F}_p^\times$ teilt $\mathrm{ggT}(m, p-1)$. Nehmen wir $r < m$ an und setzen $a := (mk)^r \equiv 1 \pmod{p}$. Dann gilt

$$\frac{m}{r} \equiv 1 + a + \dots + a^{\frac{m}{r}-1} = \frac{a^{\frac{m}{r}} - 1}{a - 1} = \frac{(mk)^n - 1}{(mk)^r - 1} = \prod_{\substack{d \mid m \\ d \nmid r}} \Phi_d(mk) \equiv 0 \pmod{p}$$

im Widerspruch zu $p \nmid m$. Also gilt $r = m$ ist $m \mid p-1$, d. h. $p \equiv 1 \pmod{m}$. Wegen $n \mid m$ gilt auch $p \equiv 1 \pmod{n}$. Andererseits ist $m = np_1 \dots p_s$ und $p \notin \{p_1, \dots, p_s\}$. Wir haben also eine neue Primzahl in der Restklasse $1 + n\mathbb{Z}$ gefunden. \square

Satz 10.53 (MILLER). Für $a, b, c \in \mathbb{N} \setminus \{1\}$ existiert eine endliche Gruppe $G = \langle x, y \rangle$ mit $|\langle x \rangle| = a$, $|\langle y \rangle| = b$ und $|\langle xy \rangle| = c$.

Beweis (HOLT). Anstatt G als Quotienten einer von-Dyck-Gruppe zu konstruieren, geben wir einen unabhängigen Beweis. Satz 10.52 garantiert die Existenz einer Primzahl $p \equiv 1 \pmod{2abc}$. Seien $\zeta_a, \zeta_b, \zeta_c \in \mathbb{F}_p^\times$ Elemente mit Ordnung $2a, 2b$ bzw. $2c$. Sei $\lambda \in \mathbb{F}_p$ zunächst beliebig. Dann haben

$$x := \begin{pmatrix} \zeta_a & 1 \\ 0 & \zeta_a^{-1} \end{pmatrix} \in \mathrm{SL}(2, p), \quad y := \begin{pmatrix} \zeta_b & 0 \\ \lambda & \zeta_b^{-1} \end{pmatrix} \in \mathrm{SL}(2, p)$$

die Eigenwerte $\zeta_a \neq \zeta_a^{-1}$ bzw. $\zeta_b \neq \zeta_b^{-1}$. Insbesondere sind x, y diagonalisierbar und es folgt $|\langle x \rangle| = 2a$ und $|\langle y \rangle| = 2b$. Wegen $\mathrm{tr}(xy) = 2\zeta_a\zeta_b + \lambda$ kann man λ so wählen, dass $\mathrm{tr}(xy) = \zeta_c + \zeta_c^{-1}$ gilt. Für die Eigenwerte e, f von xy (in einem Zerfällungskörper) gilt $e + f = \mathrm{tr}(xy)$ und $ef = \det(xy) =$

²⁴Dies ist ein Spezialfall des DIRICHLETSchen Primzahlsatz: Die Primzahlen verteilen sich gleichmäßig auf die primen Restklassen modulo n , d. h. für $\mathrm{ggT}(k, n) = 1$ beträgt der Anteil der Primzahlen in $k + n\mathbb{Z}$ genau $1/\varphi(n)$.

$\det(x)\det(y) = 1$. Dies zeigt $\{e, f\} = \{\zeta_c, \zeta_c^{-1}\}$ und xy ist ebenfalls diagonalisierbar mit Ordnung $2c$. Da x^a , x^b und $(xy)^c$ den doppelten Eigenwert -1 haben, gilt $x^a = y^b = (xy)^c = -1_2 \in Z := Z(\mathrm{SL}(2, p))$. Mit $\bar{x} := xZ$ und $\bar{y} := yZ$ erfüllt $G = \langle \bar{x}, \bar{y} \rangle \leq \mathrm{PSL}(2, p)$ die Behauptung. \square

11 Freie Produkte und Amalgame

Beispiel 11.1. Das direkte Produkt $G \times H$ von zwei Gruppen G und H ist die größte Gruppe D mit folgenden Eigenschaften:

- $G, H \leq D$ und $D = \langle G, H \rangle$,
- $xy = yx$ für alle $x \in G$ und $y \in H$.

Wir konstruieren die größte Gruppe, die nur die erste Eigenschaft erfüllt.

Definition 11.2. Sei $G_I := \{G_i : i \in I\}$ eine nichtleere Familie von Gruppen. Ein *freies Produkt* von G_I ist eine Gruppe G mit Homomorphismen $\lambda_i : G_i \rightarrow G$ ($i \in I$) mit folgender universeller Eigenschaft: Für jede Gruppe H und Homomorphismen $\rho_i : G_i \rightarrow H$ existiert genau ein Homomorphismus $\varphi : G \rightarrow H$ mit $\rho_i = \varphi\lambda_i$ für alle $i \in I$.

Lemma 11.3.

- (i) Die Homomorphismen λ_i sind injektiv und $G = \langle \lambda_i(G_i) : i \in I \rangle$.
- (ii) Bis auf Isomorphie gibt es höchstens ein freies Produkt von G_I .

Beweis.

- (i) Sei $H := G_i$, $\rho_i := \mathrm{id}_H$ und $\rho_j := 1$ für $j \neq i$. Dann existiert ein $\varphi : G \rightarrow H$ mit $\mathrm{id}_H = \rho_i = \varphi\lambda_i$. Insbesondere ist λ_i injektiv. Sei nun $H := \langle \lambda_i(G_i) : i \in I \rangle \leq G$ und $\rho_i := \lambda_i : G_i \rightarrow H$. Dann existiert genau ein $\varphi : G \rightarrow H$ mit $\lambda_i = \varphi\lambda_i$ für $i \in I$. Aus dem gleichen Grund existiert genau ein Homomorphismus $\varphi' : G \rightarrow G$ mit $\lambda_i = \varphi'\lambda_i$. Offensichtlich muss $\varphi' = \mathrm{id}_G$ gelten. Interpretiert man φ als Abbildung $G \rightarrow G$, so gilt auch $\varphi = \varphi'$. Dies zeigt $G = H$.
- (ii) Sei H ebenfalls ein freies Produkt von G_I mit Homomorphismen $\mu_i : G_i \rightarrow H$. Dann existieren Homomorphismen $\varphi : G \rightarrow H$ und $\psi : H \rightarrow G$ mit $\mu_i = \varphi\lambda_i$ und $\lambda_i = \psi\mu_i$ für $i \in I$. Es folgt $\varphi\psi\lambda_i = \psi\mu_i = \lambda_i$ und $\varphi\psi\mu_i = \varphi\lambda_i = \mu_i$. Nun sind, wie in (i), id_G und id_H die einzigen Homomorphismen mit $\mathrm{id}_G\lambda_i = \lambda_i$ und $\mathrm{id}_H\mu_i = \mu_i$. Dies zeigt $\varphi\psi = \mathrm{id}_H$ und $\psi\varphi = \mathrm{id}_G$. Insbesondere ist $\varphi : G \rightarrow H$ ein Isomorphismus. \square

Bemerkung 11.4. Nach Lemma 11.3 kann man von *dem* freien Produkt von G_I sprechen ohne die Homomorphismen λ_i zu erwähnen. Man schreibt $G = \mathrm{Fr}_{i \in I} G_i$ oder $G_1 * \dots * G_n$ falls $I = \{1, \dots, n\}$.²⁵ Da die λ_i injektiv sind, kann man $G_i \leq G$ annehmen (dies entspricht dem formalen Unterschied zwischen direktem Produkt und direkter Summe).

Satz 11.5. Für jede nichtleere Familie von Gruppen G_I existiert $\mathrm{Fr}_{i \in I} G_i$.

²⁵Achtung: Verwechslungsgefahr mit dem Zentralprodukt.

Beweis. Wir modifizieren Definition 11.2. O. B. d. A. sei $G_i \cap G_j = \emptyset$ für $i \neq j$. Sei W die Menge aller formalen Worte der Form $w = g_1 \dots g_n$ mit $n \in \mathbb{N}_0$ und $g_1, \dots, g_n \in \bigcup_{i \in I} G_i$. Man nennt w *reduziert*, falls $g_1, \dots, g_n \neq 1$ und $\{g_i, g_{i+1}\} \not\subseteq G_j$ für $i = 1, \dots, n-1$ und alle $j \in I$. Offenbar lässt sich w stets reduzieren. Wörter $v, w \in W$ heißen *äquivalent*, falls sie sich zu dem gleichen Wort reduzieren lassen. Sei $G = \{[w] : w \in W\}$ die Menge der Äquivalenzklassen dieser Relation. Offenbar ist G eine Gruppe bzgl. Konkatination. Wir definieren $\lambda_i: G_i \rightarrow G$ durch $\lambda_i(g) := [g]$ für $g \in G_i$. Sei nun H eine weitere Gruppe und $\rho_i: G_i \rightarrow H$ Homomorphismen für $i \in I$. Offenbar ist die Abbildung $\varphi: G \rightarrow H$ mit $[w] \mapsto \rho_1(g_1) \dots \rho_n(g_n)$ ein wohldefinierter Homomorphismus mit $\rho_i = \varphi \lambda_i$ für $i \in I$. Da G nach Konstruktion durch die Elemente $[g]$ mit $g \in \bigcup G_i$ erzeugt wird, ist φ durch ρ_i eindeutig bestimmt. \square

Lemma 11.6. *Jedes Element in $\text{Fr}_{i \in I} G_i$ lässt sich eindeutig als reduziertes Wort schreiben.*

Beweis. Wir gehen wie in Lemma 1.7 vor. Sei R die Menge der reduzierten Worte $r = g_1 \dots g_n$ mit $g_1, \dots, g_n \in \bigcup G_i$. Für $g \in G_j$ sei

$$g_r := \begin{cases} r & \text{falls } g = 1, \\ gg_1 \dots g_n & \text{falls } g_1 \notin G_j, \\ g_2 \dots g_n & \text{falls } g = g_1^{-1}, \\ (gg_1)g_2 \dots g_n & \text{sonst.} \end{cases}$$

Man sieht leicht, dass dies eine Operation $G_j \rightarrow \text{Sym}(R)$ beschreibt. Nach der universellen Eigenschaft lässt sich die Operation zu $G \rightarrow \text{Sym}(R)$ fortsetzen. Für $v, w \in R$ mit $[v] = [w]$ gilt nun $v = [v]_1 = [w]_1 = w$. \square

Bemerkung 11.7. Im Folgenden werden wir $[w]$ durch w ersetzen. Jedes Element in $\text{Fr } G_i$ lässt sich dann eindeutig in der reduzierten Form $g_1 \dots g_n$ schreiben. Hat man umgekehrt $H = \langle G_i : i \in I \rangle$, sodass sich jedes Element in H eindeutig in reduzierter Form schreiben lässt, so folgt $H \cong \text{Fr}_{i \in I} G_i$, denn man kann die Inklusionen $\sigma_i: G_i \hookrightarrow H$ zu einem Isomorphismus fortsetzen.

Beispiel 11.8.

- (a) Ein freies Produkt von freien Gruppen ist frei: Sei $F_i = F_{X_i}$ mit $X_i \cap X_j = \emptyset$ für $i \neq j$. Sei $X := \bigcup_{i \in I} X_i$ und $F := F_X$. Seien $\rho_i: F_i \rightarrow H$ Homomorphismen. Dann existiert genau ein Homomorphismus $\varphi: F \rightarrow H$ mit $\varphi(x) := \rho_i(x)$ für $x \in X_i$. Wegen $F_i = \langle X_i \rangle$ ist $\rho_i = \varphi|_{F_i}$. Als Spezialfall erhält man $F_n = \mathbb{Z} * \dots * \mathbb{Z}$.
- (b) Sei $G = \langle x \rangle * \langle y \rangle \cong C_2 * C_2$ und $z := xy \in G$. Wegen $z^{-1} = yx$ lässt sich jedes Element in G eindeutig in der Form $z^a x^b$ mit $a \in \mathbb{Z}$ und $b \in \{0, 1\}$ schreiben. Wegen $xzx^{-1} = z^{-1}$ ist $G = \langle z \rangle \rtimes \langle x \rangle \cong \mathbb{Z} \rtimes C_2 \cong D_\infty$.

Lemma 11.9. *Es gilt $\text{PSL}(2, \mathbb{Z}) \cong C_2 * C_3$.*

Beweis. Seien $A := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $B := \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ in $\text{SL}(2, \mathbb{Z})$. Wir zeigen zunächst $\text{SL}(2, \mathbb{Z}) = \langle A, B \rangle$. Sei indirekt $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \setminus \langle A, B \rangle$ mit $|a| + |c|$ minimal. Nehmen wir $a \neq 0 \neq c$ an. Dann ist

$$\begin{aligned} (AB)^s C &= \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + sc & b + sd \\ c & d \end{pmatrix} \notin \langle A, B \rangle, \\ (BA)^{-r} C &= \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ ra + c & rb + d \end{pmatrix}. \end{aligned}$$

Im Fall $|a| \geq |c|$ kann man s so wählen, dass $|a + sc| + |c| < |a| + |c|$ gilt. Anderenfalls kann man r so wählen, dass $|a| + |ra + c| < |a| + |c|$ gilt. Widerspruch. Also ist $a = 0$ oder $c = 0$. Im ersten Fall wäre

$$C = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & d \end{pmatrix} \in \{BA^2(AB)^{-d-1}, B(AB)^{d-1}\}$$

und im zweiten Fall wäre

$$C = \begin{pmatrix} \pm 1 & b \\ 0 & \mp 1 \end{pmatrix} \in \{(AB)^b, A^2(AB)^{-b}\}.$$

Dies zeigt $\mathrm{SL}(2, \mathbb{Z}) = \langle A, B \rangle$.

Wegen $A^2 = -1 = B^3$ haben $\overline{A}, \overline{B} \in \mathrm{PSL}(2, \mathbb{Z})$ Ordnung 2 bzw. 3 (beachte $Z(\mathrm{SL}(2, \mathbb{Z})) = \langle -1_2 \rangle$). Sei $G := \langle x \rangle * \langle y \rangle \cong C_2 * C_3$. Dann existiert ein Epimorphismus $\varphi: G \rightarrow \mathrm{PSL}(2, \mathbb{Z})$ mit $\varphi(x) = \overline{A}$ und $\varphi(y) = \overline{B}$. Angenommen es existiert $w \in \mathrm{Ker}(\varphi) \setminus \{1\}$. Dann ist w ein alternierendes Produkt von x und $y^{\pm 1}$. Nach Konjugation können wir $w = xy^{\epsilon_1} \dots xy^{\epsilon_n}$ mit $\epsilon_1, \dots, \epsilon_n \in \{\pm 1\}$ annehmen. Die Matrizen AB und $AB^{-1} = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$ haben nicht-negative bzw. nicht-positive Einträge. Die gleiche Eigenschaft müsste auch für

$$\overline{AB^{\epsilon_1} \dots AB^{\epsilon_{n-1}} AB^{-\epsilon_n}} = \varphi(wy^{\epsilon_n}) = \varphi(w)\varphi(y^{\epsilon_n}) = \overline{B^{\epsilon_n}}$$

gelten. Tatsächlich hat B^{ϵ_n} aber sowohl positive als auch negative Einträge. Also ist φ ein Isomorphismus. \square

Lemma 11.10. *Sei $F := \mathrm{Fr}_{i \in I} G_i$ mit $G_i \neq 1$ für alle $i \in I$. Dann gilt:*

- (i) *Jedes Element $g \in F$ endlicher Ordnung liegt bis auf Konjugation in einem G_i .*
- (ii) *Für $g \in G_i \setminus \{1\}$ gilt $C_F(g) = C_{G_i}(g)$.*
- (iii) *Für $|I| \geq 2$ gilt $|F| = \infty$ und $Z(F) = 1$.*

Beweis.

- (i) Sei $g = g_1 \dots g_n \in F$ reduziert mit $n \geq 2$. Nach Konjugation können wir annehmen, dass g_1 und g_n in unterschiedlichen Faktoren G_i liegen. Offenbar ist dann $g^k \neq 1$ für alle $k \geq 1$.
- (ii) Sei $x = x_1 \dots x_n \in C_F(g)$ reduziert und o. B. d. A. $x_n \notin G_i$. Dann wäre auch ngx^{-1} reduziert und $ngx^{-1} \neq g$.
- (iii) Für $g \in G_i \setminus \{1\}$ und $h \in G_j \setminus \{1\}$ mit $i \neq j$ ist gh reduziert mit unendlicher Ordnung. Außerdem ist $Z(F) \leq C_F(g) \cap C_F(h) \leq G_i \cap G_j = 1$ nach (ii). \square

Satz 11.11. *Seien $G = \mathrm{Fr}_{i \in I} G_i$ und $H = \mathrm{Fr}_{i \in I} H_i$ freie Produkte über der gleichen Indexmenge I . Seien $\sigma_i: G_i \rightarrow H_i$ Homomorphismen für $i \in I$. Dann gibt es genau einen Homomorphismus $\varphi: G \rightarrow H$, der alle σ_i fortsetzt. Außerdem ist $\mathrm{Ker}(\varphi)$ der normale Abschluss von $\bigcup_{i \in I} \mathrm{Ker}(\sigma_i)$ in G .*

Beweis. Die Existenz und Eindeutigkeit von φ folgt aus der universellen Eigenschaft. Sei $N \trianglelefteq G$ der normale Abschluss von $\bigcup_{i \in I} \mathrm{Ker}(\sigma_i)$ in G . Sicher ist $N \subseteq \mathrm{Ker}(\varphi)$. Nehmen wir $\mathrm{Ker}(\varphi) \not\subseteq N$ an und wählen $g = g_1 \dots g_n \in \mathrm{Ker}(\varphi) \setminus N$ reduziert mit minimalem n und $g_k \in G_{i_k}$ für $k = 1, \dots, n$. Gilt $\sigma_{i_k}(g_k) \neq 1$ für $k = 1, \dots, n$, so wäre $1 = \varphi(g) = \sigma_{i_1}(g_1) \dots \sigma_{i_n}(g_n)$ reduziert in H . Dieser Widerspruch zeigt $\sigma_{i_k}(g_k) = 1$ für ein $1 \leq k \leq n$. Dann wäre aber $g_1 \dots g_{k-1} g_{k+1} \dots g_n \in \mathrm{Ker}(\varphi) \setminus N$ im Widerspruch zur Wahl von n . \square

Folgerung 11.12. Seien $G_i = \langle X_i \mid R_i \rangle$ Präsentationen für $i \in I$. Dann ist

$$\mathrm{Fr}_{i \in I} G_i \cong \langle \bigcup_{i \in I} X_i \mid \bigcup_{i \in I} R_i \rangle.$$

Beweis. Sei $F_i := F_{X_i}$ und F die freie Gruppe bzgl. $\bigcup_{i \in I} X_i$. Nach Beispiel 11.8 ist $F = \mathrm{Fr}_{i \in I} F_i$. Sei $\sigma_i: F_i \rightarrow G_i$ der kanonische Epimorphismus. Nach Satz 11.11 existiert ein Epimorphismus $\varphi: F \rightarrow \mathrm{Fr}_{i \in I} G_i$ mit $\mathrm{Ker}(\varphi) = \langle \bigcup \mathrm{Ker}(\sigma_i) \rangle^F = \langle \bigcup R_i^F \rangle^F = \langle \bigcup R_i \rangle^F$. Dies zeigt die Behauptung. \square

Bemerkung 11.13.

(i) KUROSCH hat gezeigt, dass jede Untergruppe H von $F := \mathrm{Fr}_{i \in I} G_i$ die Form

$$F_0 * \mathrm{Fr}_{i \in I} \mathrm{Fr}_{HxG_i \in H \backslash F/G_i} (H \cap xG_i x^{-1})$$

hat, wobei F_0 frei ist (hierbei ist $H \backslash F/G_i$ die Menge der *Doppelnebenklassen* bzgl. H und G_i).

(ii) Aus direkten Produkten kann man Zentralprodukte machen, indem man zentrale Untergruppen heraufsteilt. Wir konstruieren eine nicht-kommutative Variante.

Definition 11.14. Sei $G_I = \{G_i : i \in I\}$ eine Familie von Gruppen. Sei H eine Gruppe und $\sigma_i: H \rightarrow G_i$ Monomorphismen für $i \in I$. Sei N der normale Abschluss von $\{\sigma_i(h)^{-1} \sigma_j(h) : h \in H, i, j \in I\}$ in $F := \mathrm{Fr}_{i \in I} G_i$. Man nennt F/N das *Amalgam von G_I bzgl. H* .

Bemerkung 11.15. Wegen $\sigma_i(h) \equiv \sigma_j(h) \pmod{N}$ gilt $\sigma_i(H)N/N = \sigma_j(H)N/N \leq F/N$. Man identifiziert also die isomorphen Kopien von H in G_i . Im Fall $H = 1$ ist $N = 1$ und man erhält das gewöhnliche freie Produkt. Im Gegensatz zum freien Produkt hängt F/N auch von der Wahl der Monomorphismen σ_i ab.

Beispiel 11.16. Wir hatten $\mathrm{PSL}(2, \mathbb{Z}) = \langle \overline{A}, \overline{B} \rangle \cong C_2 * C_3$ in Lemma 11.9 bewiesen. Man sieht leicht, dass $\mathrm{SL}(2, \mathbb{Z}) = \langle A, B \rangle$ ein Amalgam von $\langle A \rangle = C_4$ und $\langle B \rangle \cong C_6$ bzgl. $\langle A^2 \rangle = \langle B^3 \rangle = \langle -1_2 \rangle = \mathrm{Z}(\mathrm{SL}(2, \mathbb{Z}))$ ist.

Lemma 11.17. In der Situation von Definition 11.14 sei R_i ein Repräsentantensystem für die Nebenklassen von $\sigma_i(H)$ in G_i mit $1 \in R_i$. Dann lässt sich jedes Element in F/N eindeutig in der reduzierten Form $r_1 \dots r_n h N$ mit $n \in \mathbb{N}_0$, $r_k \in R_{i_k} \setminus \{1\}$, $i_k \neq i_{k+1}$ und $h \in \sigma_{i_n}(H)$ schreiben.

Beweis. Sei $g = g_1 \dots g_n N \in F/N$ mit $g_k \in G_{i_k}$ beliebig. Dann existieren $r_1 = \overline{g_1} \in R_{i_1}$ und $h_1 \in H$ mit $g_1 = r_1 \sigma_{i_1}(h_1)$. Wegen $\sigma_{i_1}(h_1)N = \sigma_{i_2}(h_1)N$ existieren $r_2 = \overline{\sigma_{i_2}(h_1)g_2} \in R_{i_2}$ und $h_2 \in H$ mit $g = r_1(\sigma_{i_2}(h_1)g_2)g_3 \dots g_n N = r_1 r_2 \sigma_{i_2}(h_2)g_3 \dots g_n N$ usw. Elemente $r_i = 1$ kann man weglassen. Auf diese Weise lässt sich g auf die reduzierte Form bringen.

Sei nun $R := \{r_1 \dots r_n \sigma_{i_n}(h) : r_i \in R_i, h \in H\} \subseteq F$ die Menge der reduzierten Wörter. Wir zeigen wie in Lemma 11.6, dass F auf R operiert. Es genügt zu zeigen, dass jedes G_j auf R operiert. Sei $x = \overline{x} \sigma_j(h_1) \in G_j$ und $r = r_1 \dots r_n \sigma_{i_n}(h) \in R$. Wir nehmen zunächst $j \neq i_1$ an und definieren

$$x_r := \overline{x \sigma_{i_1}(h_1) r_1 \sigma_{i_2}(h_2) r_2 \dots \sigma_{i_n}(h_n) r_n \sigma_{i_n}(h_{n+1} h)} \in R$$

mit $\sigma_{i_k}(h_k) r_k = \overline{\sigma_{i_k}(h_k) r_k \sigma_{i_k}(h_{k+1})}$ für $k = 1, \dots, n$ (im Fall $x \in \sigma_j(H)$ muss man \overline{x} entfernen). Für $y \in G_j$ folgt

$$y(x_r) = \overline{y x \sigma_{i_1}(h'_1 h_1) r_1 \dots \sigma_{i_n}(h'_n h_n) r_n \sigma_{i_n}(h'_{n+1} h_{n+1} h)}$$

mit $y\bar{x} = \overline{yx}\sigma_j(h'_1)$ und $\sigma_{i_k}(h'_k)\overline{\sigma_{i_k}(h_k)r_k} = \overline{\sigma_{i_k}(h'_k h_k)r_k}\sigma_{i_k}(h'_{k+1})$ für $k = 1, \dots, n$. Andererseits ist

$${}^{yx}r = \overline{yx}\sigma_{i_1}(h''_1)r_1 \dots \overline{\sigma_{i_n}(h''_n)r_n}\sigma_{i_n}(h''_{n+1}h)$$

mit $yx = \overline{yx}\sigma_j(h''_1)$ und $\sigma_{i_k}(h''_k)r_k = \overline{\sigma_{i_k}(h''_k)r_k}\sigma_{i_k}(h''_{k+1})$ für $k = 1, \dots, n$. Es folgt

$$\overline{yx}\sigma_j(h''_1) = yx = \overline{yx}\sigma_j(h'_1) = \overline{yx}\sigma_j(h'_1 h_1)$$

und $h''_1 = h'_1 h_1$, da σ_j injektiv ist. Durch Induktion nach k ergibt sich

$$\begin{aligned} \overline{\sigma_{i_k}(h''_k)r_k}\sigma_{i_k}(h''_{k+1}) &= \sigma_{i_k}(h''_k)r_k = \sigma_{i_k}(h'_k h_k)r_k = \sigma_{i_k}(h'_k)\overline{\sigma_{i_k}(h_k)r_k}\sigma_{i_k}(h_{k+1}) \\ &= \overline{\sigma_{i_k}(h'_k h_k)r_k}\sigma_{i_k}(h'_{k+1}h_{k+1}) = \overline{\sigma_{i_k}(h''_k)r_k}\sigma_{i_k}(h'_{k+1}h_{k+1}), \end{aligned}$$

d. h. $h'_{k+1}h_{k+1} = h''_{k+1}$. Der Fall $j = i_1$ funktioniert analog. Damit ist ${}^y(xr) = {}^{yx}r$ bewiesen und F operiert auf R mit ${}^x[r] \equiv [xr] \pmod{N}$. Für $h \in H$ hat $\sigma_i(h)$ die gleiche Wirkung auf R wie $\sigma_j(h)$ für $i, j \in I$. Also operiert N trivial und F/N operiert auf R . Für $v, w \in R$ mit $[v]N = [w]N$ gilt nun $v = [v]N1 = [w]N1 = w$. \square

Lemma 11.18. Sei $G = F/N$ ein Amalgam von G_I bzgl. H und $\sigma_i: H \rightarrow G_i$. Dann existieren Untergruppen $H \cong \overline{H} \leq G$ und $G_i \cong \overline{G_i} \leq G$ mit $G = \langle \overline{G_i} : i \in I \rangle$ und $\overline{H} = \overline{G_i} \cap \langle \overline{G_j} : j \neq i \rangle$ für alle $i \in I$.

Beweis. Sei $\overline{G_i} := G_i N / N$ und $\overline{H} := \sigma_i(H)N / N \leq G$ (hängt nicht von i ab). Aus Lemma 11.17 folgt $\overline{G_i} \cong G_i / G_i \cap N \cong G_i$. Wegen $\overline{H} \leq \overline{G_i}$ ist auch $\overline{H} \cong H$. Aus $F = \langle G_i : i \in I \rangle$ folgt $G = \langle \overline{G_i} : i \in I \rangle$. Schließlich folgt auch $\overline{H} = \overline{G_i} \cap \langle \overline{G_j} : j \neq i \rangle$ aus Lemma 11.17. \square

Bemerkung 11.19. Wir werden im Folgenden die Gruppen G_i und H als Untergruppen von $G = F/N$ auffassen. Sei R_i ein Repräsentantensystem für G_i/H mit $1 \in R_i$ für $i \in I$. Jedes Element in G lässt sich dann eindeutig in der reduzierten Form $r_1 \dots r_n h$ mit $r_k \in R_{i_k} \setminus \{1\}$ und $h \in H$ schreiben.

Lemma 11.20. Sei G ein Amalgam von G_I bzgl. H . Dann gilt

- (i) Jedes Element endlicher Ordnung von G liegt bis auf Konjugation in einem G_i .
- (ii) Existieren verschiedene $i, j \in I$ mit $G_i \neq H \neq G_j$, so ist $|G| = \infty$.

Beweis.

- (i) Sei $g = r_1 \dots r_n h$ in reduzierter Form mit endlicher Ordnung. Nach Konjugation können wir $i_1 \neq i_n$ annehmen (Achtung: es werden möglicherweise alle r_i verändert). Dann sind die Elemente g, g^2, \dots aber alle verschieden. Dieser Widerspruch zeigt $n \leq 1$ und $g \in G_{i_1}$.
- (ii) Für $g_1 \in G_i \setminus H$ und $g_2 \in G_j \setminus H$ hat $g_1 g_2$ unendliche Ordnung. \square

Satz 11.21. Jede endliche Gruppe G ist eine Untergruppe einer endlichen Gruppe \hat{G} mit folgender Eigenschaft: Sind $H, K \leq G$ isomorphe Untergruppe und $\varphi: H \rightarrow K$ ein Isomorphismus, so existiert ein $x \in \hat{G}$ mit $\varphi(h) = x h x^{-1}$ für alle $h \in H$. Insbesondere sind H und K in \hat{G} konjugiert.

Beweis. Wir setzen $\hat{G} := \text{Sym}(G)$ und betten G mittels der regulären Darstellung $\sigma: G \rightarrow \hat{G}$, $x \mapsto \sigma_x$ mit $\sigma_x(y) = xy$ ein. Sei $\hat{\varphi} \in \hat{G}$ eine beliebige bijektive Fortsetzung von φ . Für $h \in H$ und $k \in K$ gilt nun

$$(\hat{\varphi}\sigma_h\hat{\varphi}^{-1})(k) = \varphi(h\varphi^{-1}(k)) = \varphi(h)k = \sigma_{\varphi(h)}(k)$$

und $\hat{\varphi}\sigma_h\hat{\varphi}^{-1} = \sigma_{\varphi(h)}$. \square

Bemerkung 11.22. Der Beweis von Satz 11.21 funktioniert nicht mehr für unendliche Gruppen. Beispielsweise lässt sich der kanonische Isomorphismus $\varphi: \mathbb{Z} \rightarrow 2\mathbb{Z}$ nicht zu einer Bijektion $\mathbb{Z} \rightarrow \mathbb{Z}$ fortsetzen.

Satz 11.23 (HIGMAN-NEUMANN-NEUMANN). *Sei G eine Gruppe, $H, K \leq G$ und $\varphi: H \rightarrow K$ ein Isomorphismus. Dann ist G eine Untergruppe einer Gruppe \hat{G} , sodass ein $x \in \hat{G}$ mit $\varphi(h) = xhx^{-1}$ für alle $h \in H$ existiert. Insbesondere sind H und K in \hat{G} konjugiert.*

Beweis. Sei $\langle a_i \rangle \cong \mathbb{Z}$ und $G_i := G * \langle a_i \rangle$ für $i = 1, 2$. Nach der universellen Eigenschaft existieren Homomorphismen $\sigma_1: G * H \rightarrow G_1$ und $\sigma_2: G * H \rightarrow G_2$ mit $(\sigma_i)|_G = \text{id}$ und $\sigma_1(h) := a_1ha_1^{-1}$ sowie $\sigma_2(h) := a_2\varphi(h)a_2^{-1}$ für $h \in H$. Nach Lemma 11.6 sind σ_1 und σ_2 injektiv. Sei \hat{G} das Amalgam von G_1 und G_2 bzgl. $G * H$. Nach Lemma 11.18 kann man G mit $\sigma_1(G) = \sigma_2(G)$ in \hat{G} identifizieren. Für $h \in H$ gilt $a_1ha_1^{-1} = \sigma_1(h) = \sigma_2(h) = a_2\varphi(h)a_2^{-1}$ und die Behauptung folgt mit $x := a_2^{-1}a_1 \in \hat{G}$. \square

Bemerkung 11.24. In der Situation von Satz 11.23 nennt man $\langle G, x \rangle \leq \hat{G}$ eine HNN-Erweiterung von G bzgl. $\varphi: H \rightarrow K$. Ist G torsionsfrei, so auch jede HNN-Erweiterung nach Lemma 11.20.

Satz 11.25. *Jede abzählbare Gruppe ist eine Untergruppe einer Gruppe mit zwei Erzeugern.*

Beweis. Sei $G = \{1 = g_0, g_1, \dots\}$ eine abzählbare Gruppe. Ist G endlich, so folgt die Behauptung aus $G \leq \text{Sym}(G)$. Sei also $|G| = \infty$. Sei $F_2 = \langle x, y \rangle$, $X := \{y^kxy^{-k} : k \geq 0\}$ und

$$Y := \{x^k y x^{-k} g_k : k \geq 0\} \subseteq G * F_2.$$

Aus Lemma 11.6 folgt leicht: $\langle X \rangle \cong F_X \cong F_Y \cong \langle Y \rangle$. Sei $\varphi: \langle X \rangle \rightarrow \langle Y \rangle$, $y^kxy^{-k} \mapsto x^k y x^{-k} g_k$ für $k \geq 0$. Sei $\hat{G} := \langle G * F_2, s \rangle$ eine HNN-Erweiterung von $G * F_2$ bzgl. φ . Dann gilt $sy^kxy^{-k}s^{-1} = x^k y x^{-k} g_k$ für $k \geq 0$. Insbesondere ist $y = sxs^{-1} \in \langle x, s \rangle$ und $g_k = (x^k y x^{-k})^{-1}sy^kxy^{-k}s^{-1} \in \langle x, s \rangle$ für $k \geq 1$. Dies zeigt $G \leq \hat{G} = \langle x, s \rangle$. \square

Satz 11.26. *Es existiert eine unendliche Gruppe mit genau zwei Konjugationsklassen.*

Beweis. Sei zunächst $G = G_1 = \{1 = g_0, g_1, g_2, \dots\}$ eine beliebige abzählbare torsionsfreie Gruppe (zum Beispiel $G = \mathbb{Z}$). Induktiv existiert eine torsionsfreie abzählbare HNN-Erweiterung G_{n+1} von G_n , sodass g_1 und g_{n+1} in G_{n+1} konjugiert sind. In der torsionsfreien abzählbaren Gruppe $G^* := \bigcup_{n \in \mathbb{N}} G_n$ sind dann alle g_i konjugiert. Wir setzen nun $H_1 := G$ und $H_{n+1} := H_n^*$ für $n \geq 1$. Sei schließlich $H := \bigcup_{n \geq 1} H_n$. Für $x, y \in H \setminus \{1\}$ existiert ein $n \geq 1$ mit $x, y \in H_n$. Nach Konstruktion sind x und y in $H_{n+1} \leq H$ konjugiert. Also besitzt H nur zwei Konjugationsklassen. \square

Bemerkung 11.27. Sei G eine Torsionsgruppe mit Klassenzahl 2. Dann hat jedes nicht-triviale Element in G die gleiche Ordnung p . Sicher ist p eine Primzahl. Im Fall $p > 2$ kann $x \in G \setminus \{1\}$ nicht zu x^{-1} konjugiert sein. Also ist $p = 2$ und G ist abelsch. Es folgt $G \cong C_2$.

12 Das Burnside-Problem

Bemerkung 12.1. BURNSIDE fragte 1902:

- (I) Ist jede endlich erzeugte Torsionsgruppe endlich?
- (II) Ist jede endlich erzeugte periodische Gruppe endlich?²⁶
- (III) Gibt es für $d, e \in \mathbb{N}$ höchstens endlich viele endliche Gruppen mit d Erzeugern und Exponenten e ?

Die erste Frage wurde 1964 von GOLOD negativ beantwortet. NOVIKOV und ADJAN beantworteten 1968 auch (II) negativ. ZELMANOV hingegen bewies 1989, dass (III) richtig ist (er bekam dafür die Fieldsmedaille).²⁷

Satz 12.2 (GOLOD). *Für jede Primzahl $p > 2$ existiert eine unendliche p -Gruppe mit zwei Erzeugern.*

Beweis (GUPTA).

Schritt 1: Konstruktion von G .

Sei $\langle a \rangle \cong \langle t \rangle \cong C_p$ und $H = \langle a \rangle * \langle t \rangle$. Sei $a_i := t^i a t^{-i}$ und

$$A := \langle a \rangle^H = \langle a_0, a_1, \dots, a_{p-1} \rangle.$$

Da sich jedes Element aus A eindeutig in der Form $a_{i_1}^{n_1} \dots a_{i_s}^{n_s}$ mit $1 \leq n_1, \dots, n_s < p$ und $i_k \neq i_{k+1}$ schreiben lässt, ist $A \cong \langle a_0 \rangle * \dots * \langle a_{p-1} \rangle$ (Bemerkung 11.7). Außerdem gilt $H = A \rtimes \langle t \rangle$. Für $0 \leq k < p$ sei $\theta_k: A \rightarrow H$ der Homomorphismus mit $\theta_k(a_k) := a$ und $\theta_k(a_i) := t^{i-k}$ für $i \neq k$. Setze $N_0 = 1$ und

$$N_{k+1} := \{x \in A : \forall i : \theta_i(x) \in N_k\}.$$

Offenbar ist $1 = N_0 \leq N_1 \leq \dots$. Wir zeigen $N_k \trianglelefteq H$. Dies ist klar für $k = 0$. Sei induktiv $N_k \trianglelefteq H$. Dann ist zunächst $N_{k+1} \trianglelefteq A$. Sei $w = w(a_0, \dots, a_{p-1}) \in N_{k+1}$. Wegen $\theta_i(a_j) = \theta_{i-1}(a_{j-1})$ ist

$$\theta_i(twt^{-1}) = \theta_i(w(a_1, \dots, a_{p-1}, a_0)) = \theta_{i-1}(w(a_0, \dots, a_{p-1})) \in N_k$$

und $twt^{-1} \in N_{k+1}$. Dies zeigt $N_{k+1} \trianglelefteq H$. Also ist auch $N := \bigcup_{k \geq 0} N_k \trianglelefteq H$. Sei schließlich

$$G := H/N.$$

Schritt 2: G ist eine endlich erzeugte p -Gruppe.

Sicher ist $G = \langle aN, tN \rangle$. Für $h = wt^i \in H$ mit $w = a_{j_1}^{w_1} \dots a_{j_k}^{w_k} \in A$ reduziert und $0 \leq i < p$ sei

$$l(h) := \begin{cases} 1+k & \text{falls } i \neq 0, \\ k & \text{falls } i = 0. \end{cases}$$

Wir zeigen $h^{p^{l(h)}} \in N_{l(h)}$ für alle $h \in H$. Dann ist G eine p -Gruppe. Für $l(h) \leq 1$ ist $h \in \langle t \rangle \cup \langle a_0 \rangle \cup \dots \cup \langle a_{p-1} \rangle$ und $h^p = 1 \in N_0$. Sei $l(h) = n+1$ und die Behauptung für n bereits bewiesen. Nehmen wir zunächst $i \neq 0$ an. Dann ist $l(w) = n$ und

$$h^p = (wt^i)^p = wt^i wt^{-i} t^{2i} wt^{-2i} \dots t^{(p-1)i} wt^{-(p-1)i}.$$

²⁶Erinnerung: Periodisch bedeutet, dass die Ordnung aller Elemente global beschränkt ist (also $\exp(G) < \infty$).

²⁷Der Beweis benutzt Schreiers Vermutung und basiert damit auf der CFSG.

Für $w = w(a_0, \dots, a_{p-1})$ gilt $t^{ji}wt^{-ji} = w(a_{ji}, a_{ji+1}, \dots, a_{ji+p-1})$, wobei die Indizes modulo p zu lesen sind. Sei d_k die Anzahl der Potenzen von a_k in w . Die Anzahl der Potenzen von a_k in h^p ist dann höchstens

$$\sum_{j=0}^{p-1} d_{k-ji} = \sum_{j=0}^{p-1} d_j \leq n$$

wegen $p \nmid i$. Die Anzahl der Potenzen von a in $\theta_k(h^p)$ ist also ebenfalls $\leq n$. Wir zählen wie viele t in $\theta_k(h^p)$ auftreten. Für $r \neq k$ sei s_r die Summe der Exponenten aller a_r in w . Der Beitrag dieser Potenzen in der Exponentensumme von t in $\theta_k(h^p)$ ist dann

$$\sum_{j=0}^{p-1} s_r(r + ij - k) \equiv s_r \left(p(r - k) + i \binom{p}{2} \right) \equiv 0 \pmod{p},$$

da $p > 2$ (man beachte, dass für $ij + r = k$ nichts gezählt wird). Wegen $A \trianglelefteq H$ lassen sich alle t in $\theta_k(h^p)$ nach rechts schieben, ohne dass sich die Exponentensumme ändert. Dies zeigt $\theta_k(h^p) \in A$. Durch das Verschieben der t werden einige der a in a_j umgewandelt. Deren Anzahl ist aber nach wie vor $\leq n$, d. h. $l(\theta_k(h^p)) \leq n$. Nach Induktion ist $\theta_k(h^{p^{n+1}}) = \theta_k(h^p)^{p^n} \in N_n$ für alle k , d. h. $h^{p^{n+1}} \in N_{n+1}$.

Sei nun $i = 0$, also $h = w \in A$. Nach Konjugation können wir annehmen, dass w nicht mit dem gleichen a_j beginnt und endet. Gilt bereits $l(\theta_k(w)) \leq n$ für alle k , so ist $\theta_k(w^{p^n}) \in N_n$ nach Induktion und es folgt $w^{p^n} \in N_{n+1}$ sowie $w^{p^{n+1}} \in N_{n+1}$. Nehmen wir also $l(\theta_k(w)) = n + 1$ für ein k an (man beachte, dass die Länge nicht größer werden kann). Enthält w zwei Potenzen von a_j mit $j \neq k$, so werden diese unter θ_k in Potenzen von t überführt. Nachdem man alle t in $\theta_k(w)$ nach rechts schiebt, erhält man den Widerspruch $l(\theta_k(w)) \leq n$. Also kann w höchstens eine Potenz von jedem a_j mit $j \neq k$ enthalten. Andererseits beginnt und endet w mit verschiedenen a_j . Dies zeigt $n = 2$ und nach Konjugation hat w die Form $w = a_k^r a_j^s$ mit $j \neq k$. Es folgt $\theta_k(w) = a^r t^{j-k}$. Wie im Fall $i \neq 0$ ergibt sich $\theta_m(\theta_k(w)^p) \in A$ mit $l(\theta_m(\theta_k(w)^p)) \leq 1$ für $m = 0, \dots, p-1$ (an dieser Stelle hatten wir noch keine Induktion benutzt). Also ist $\theta_m(\theta_k(w^{p^2})) = 1$ und $\theta_k(w^{p^2}) \in N_1$. Vertauscht man die Rollen von k und j , so erhält man $\theta_j(w^{p^2}) \in N_1$. Für $m \notin \{k, j\}$ ist sogar $\theta_m(w^p) = 1$. Also ist $w^{p^2} \in N_2$ wie behauptet.

Schritt 3: $|G| = \infty$.

Angenommen G ist endlich. Nach Reidemeister-Schreier ist dann N endlich erzeugt. Insbesondere ist $N = N_n$ für ein $n \in \mathbb{N}$. Wir definieren $v_0 := [a_1, a] \in A$ und $v_{k+1} = [v_k, a] \in A$ für $k \geq 0$. Dann gilt $\theta_0(v_0) = [t, a] = a_1 a^{-1}$ und $\theta_0(v_1) = [a_1 a^{-1}, a] = v_0$. Induktiv folgt $\theta_0(v_{k+1}) = v_k$ für $k \geq 0$. Nach Lemma 11.10 haben alle v_i unendliche Ordnung, denn ihre reduzierte Form beginnt mit a_1 und endet mit a^{-1} . Sei $r \geq 0$ mit $v_0^r \in N_2$. Dann ist $\theta_0(v_0^r) = (a_1 a^{-1})^r \in N_1$ und man erhält $(ta^{-1})^r = \theta_0(a_1 a^{-1})^r = 1$. Dies zeigt $p \mid r$. Es folgt

$$1 = ((ta^{-1})^p)^{r/p} = ((at^{-1})^p)^{-r/p} = (a_0 a_{p-1} \dots a_1)^{-r/p}$$

und $r = 0$. Wir haben damit $\langle v_0 \rangle \cap N_2 = 1$ bewiesen. Sei nun induktiv $\langle v_{k-1} \rangle \cap N_{k+1} = 1$ und $v_k^r \in N_{k+2}$. Dann ist $v_{k-1}^r = \theta_0(v_k)^r \in N_{k+1}$ und $r = 0$. Somit gilt $\langle v_k \rangle \cap N_{k+2} = 1$ für alle $k \geq 0$. Andererseits ist $v_n^{p^{l(v_n)}} \in N = N_n = N_{n+2}$ nach Schritt 2. Widerspruch. \square

Definition 12.3. Für $d, e \in \mathbb{N}$ sei $B(d, e) := F_d / \langle g^e : g \in F_d \rangle$ die *Burnside-Gruppe* mit d Erzeugern und Exponent e . Das Burnside-Problem (II) ist äquivalent zu $|B(d, e)| < \infty$ für alle $d, e \in \mathbb{N}$.

Satz 12.4. Für $d, e \in \mathbb{N}$ gilt

- (i) $B(1, e) \cong C_e$.

- (ii) $B(d, 2) \cong C_2^d$.
- (iii) $|B(d, 3)| \leq 3^{3^{d-1}}$.

Beweis.

- (i) Trivial.
- (ii) Jede Gruppe vom Exponent 2 ist abelsch. Nach Burnside's Basissatz ist C_2^d die größte elementarabelsche Gruppe mit d Erzeugern.
- (iii) Induktion nach d : Der Fall $d = 1$ folgt aus (i). Sei $d \geq 2$ und $G := B(d, 3) = \langle x_1, \dots, x_d \rangle$. Nach Induktion hat $H := \langle x_1, \dots, x_{d-1} \rangle$ Ordnung $\leq 3^{3^{d-2}}$. Jedes $g \in G$ hat die Form $g = h_1 x_d^{\epsilon_1} h_2 \dots x_d^{\epsilon_n} h_{n+1} \dots$ mit $\epsilon_i \in \{\pm 1\}$ und $h_i \in H$. Wegen $\exp(G) = 3$ gilt

$$x^{\pm 1} y x^{\pm 1} = y^{-1} x^{\mp 1} y^{-1} \quad x^{\pm 1} y x^{\mp 1} = y^{-1} x^{\mp 1} y^{-1} x^{\pm 1}$$

für alle $x, y \in G$. Also gilt $g = h_1 x_d h_2 x_d^{-1} h_3$ mit $h_1, h_2, h_3 \in H$. Es folgt $|G| \leq |H|^3 \leq 3^{3^{d-1}}$. \square

Definition 12.5 (Wiederholung GT). Für $x_1, \dots, x_n \in G$ sei $[x_1, x_2] := x_1 x_2 x_1^{-1} x_2^{-1}$ und

$$[x_1, \dots, x_n] := [x_1, [x_2, \dots, x_n]]$$

für $n \geq 3$. Wir setzen $G^{[1]} := G$ und $G^{[k]} := [G, G^{[k-1]}]$ für $k \geq 2$.

Lemma 12.6. Für $G = \langle X \rangle$ und $k \geq 1$ gilt $G^{[k]} = \langle [x_1, \dots, x_k] : x_1, \dots, x_k \in X \rangle G^{[k+1]}$.

Beweis. Die Behauptung gilt für $k = 1$, wenn man $[x] = x$ interpretiert. Sei nun die Behauptung für ein $k \geq 1$ bereits bewiesen. Sei $N := \langle [x_1, \dots, x_{k+1}] : x_1, \dots, x_{k+1} \in X \rangle G^{[k+2]} \leq G^{[k+1]}$. Für $g \in G$ und $x_1, \dots, x_{k+1} \in X$ gilt

$$g[x_1, \dots, x_{k+1}]g^{-1} = [g, x_1, \dots, x_{k+1}][x_1, \dots, x_{k+1}] \leq G^{[k+2]}N = N.$$

Daraus folgt $N \trianglelefteq G$. Modulo N ist jeder der Erzeuger $x \in X$ von G mit den Erzeugern $[x_1, \dots, x_k]$ und $g \in G^{[k+1]}$ von $G^{[k]}$ vertauschbar. Dies zeigt $G^{[k+1]} = [G, G^{[k]}] \leq N$. \square

Lemma 12.7 (LEVI). Sei G eine Gruppe vom Exponenten 3. Dann gilt

- (i) $[x, x, y] = 1$ für $x, y \in G$.
- (ii) $[x, y, z] = [y, z, x] = [x, z, y]^{-1}$ für $x, y, z \in G$.
- (iii) G ist nilpotent mit Klasse höchstens 3.

Beweis.

- (i) Folgt aus

$$x \cdot xyx^{-1} = (xy)^2 y^{-2} = (xy)^{-1} y = y^{-1} x^{-1} y = y^2 (y^{-1} x)^{-1} = y^2 (y^{-1} x)^2 = yxy^{-1} \cdot x.$$

(ii) Aus (i) folgt, dass je zwei Konjugierte von x vertauschbar sind. Also ist $\langle x \rangle^G$ abelsch. Es folgt

$${}^x[y, z][x, z] = [xy, z] = {}^{xy}[xy, z] = {}^{xy}(\underbrace{{}^x[y, z][x, z]}_{\in \langle y \rangle^G}) = {}^x({}^x[y, z] \cdot {}^y[x, z]) = {}^{x^{-1}}[y, z] \cdot {}^y[x, z].$$

Konjugation mit x^{-1} liefert

$${}^x[y, z] \cdot {}^y[x, z] = \underbrace{[y, z]}_{\in \langle z \rangle^G} \underbrace{[x, z]}_{\in \langle z \rangle^G} = [x, z][y, z].$$

Nun ist

$$[x, y, z] = {}^x[y, z][z, y] = {}^y[z, x][x, z][y, z][z, y] = {}^y[z, x][x, z] = [y, z, x].$$

Wegen

$$[x, y^{-1}] = [x, yy] = [x, y] \cdot {}^y[x, y] = [x, y]^2 = [x, y]^{-1}$$

$$\text{ist } [x, y, z]^{-1} = [x, [y, z]^{-1}] = [x, z, y].$$

(iii) Aus (ii) folgt $[x, y, z, w] = [x, [y, z, w]] = [x, z, w, y]$ und

$$[x, y, z, w] = [x, y, [z, w]] = [x, [z, w], y]^{-1} = [y, x, [z, w]]^{-1} = [y, x, z, w]^{-1}.$$

Für $\pi \in \langle (1, 2), (2, 3, 4) \rangle = S_4$ und $x_1, \dots, x_4 \in G$ gilt also

$$[x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, x_{\pi(4)}] = [x_1, x_2, x_3, x_4]^{\text{sgn}(\pi)}.$$

Andererseits ist

$$\begin{aligned} [x, y, z, w] &= [x, y, [z, w]] = [[z, w], x, y] = [[z, w], [x, y]] = [[x, y], [z, w]]^{-1} \\ &= [[x, y], z, w]^{-1} = [z, w, [x, y]]^{-1} \stackrel{\pi=(1,3)(2,4)}{=} [x, y, z, w]^{-1}. \end{aligned}$$

Dies zeigt $[x, y, z, w] = 1$ für alle $x, y, z, w \in G$ und die Behauptung folgt. \square

Bemerkung 12.8.

- (i) Bekanntlich ist jede Gruppe vom Exponenten 2 abelsch, also nilpotent der Klasse höchstens 1. Für p -Gruppen mit Exponent $p \geq 5$ gibt es hingegen keine absolute Schranke mehr für die Nilpotenzklasse (sofern die Gruppe nilpotent ist).
- (ii) Für $p > 10^{75}$ bewies OLSCHANSKI die Existenz unendlicher p -Gruppen, sodass jede nicht-triviale echte Untergruppe Ordnung p hat. Man nennt diese Gruppen *Tarski-Monster* (wie das sporadische Monster sind sie einfache Gruppen).
- (iii) Der nächste Satz verbessert Satz 12.4.

Satz 12.9 (LEVI, VAN DER WAERDEN). *Für $d \geq 1$ gilt $|B(d, 3)| = 3^{d(d^2+5)/6}$.*

Beweis. Sei $G := B(d, 3) = \langle x_1, \dots, x_d \rangle$. Nach von-Dyck existiert ein Epimorphismus $G \rightarrow C_3^d$. Da G/G' von d Elementen erzeugt wird, folgt $G/G' \cong C_3^d$. Nach Lemma 12.6 wird die elementarabelsche Gruppe $G'/G^{[3]}$ von den Elementen $[x_i, x_j]G^{[3]}$ mit $i < j$ erzeugt. Dies zeigt $|G'/G^{[3]}| \leq 3^{\binom{d}{2}}$. Nach Lemma 12.7 ist auch $G^{[3]}$ elementarabelsch mit $[x, y, z] = [y, z, x]$ sowie $[x, y, z] = [x, z, y]^{-1}$. Nach

Lemma 12.6 wird $G^{[3]}$ daher von den Elementen $[x_i, x_j, x_k]$ mit $i < j < k$ erzeugt. Somit ist $|G^{[3]}| \leq 3^{\binom{d}{3}}$ und $|G| \leq 3^k$ mit $k = d + \binom{d}{2} + \binom{d}{3} = d(d^2 + 5)/6$.

Jedes Element in G hat die Form

$$x_1^{a_1} \dots x_d^{a_d} [x_1, x_2]^{b_{12}} \dots [x_{d-1}, x_d]^{b_{d-1,d}} [x_1, x_2, x_3]^{c_{123}} \dots [x_{d-2}, x_{d-1}, x_d]^{c_{d-2,d-1,d}}$$

mit $a_i, b_{ij}, c_{ijk} \in \{0, 1, 2\}$. Nehmen wir an, dass ein Element g zwei verschiedene Faktorisierungen dieser Art besitzt. Diese Faktorisierungen müssen in G/G' gleich sein, denn $|G/G'| = 3^d$. Wir können also $g \in G'$ annehmen. Wegen $G'' \subseteq G^{[4]} = 1$ (GT-Lemma 3.11) ist G' abelsch. Durch Umstellen erhält man eine nicht-triviale Relation der Form

$$[x_1, x_2]^{b_{12}} \dots [x_{d-1}, x_d]^{b_{d-1,d}} [x_1, x_2, x_3]^{c_{123}} \dots [x_{d-2}, x_{d-1}, x_d]^{c_{d-2,d-1,d}} = 1.$$

Seien $i, j, k \in \{0, 1, 2\}$ mit $b_{ij} \neq 0$ oder $c_{i,j,k} \neq 0$. Indem wir alle anderen $x_l = 1$ setzen, erhalten wir eine nicht-triviale Relation in $B(3, 3)$. Wenn wir $|B(3, 3)| = 3^{3(3^2+5)/6} = 3^7$ zeigen können, hätten wir den gewünschten Widerspruch. In GAP lässt sich $B(3, 3) \cong \text{SmallGroup}(3^7, 4487)$ zeigen.²⁸ Wir geben dennoch ein theoretisches Argument.

Sei $A := \langle a, b, c, d \rangle \cong C_3^4$ und $x \in \text{Aut}(A)$ mit $x(a) = ad$ und $[x, b] = [x, c] = [x, d] = 1$. Offenbar ist $x^3(a) = ad^3 = a$ und $x^3 = 1$. In $B := A \rtimes \langle x \rangle$ gilt

$$(a^{\pm 1}x)^3 = a^{\pm 1}xa^{\pm 1}x^{-1}x^2a^{\pm 1}x^{-2} = a^{\pm 3}d^{\pm 3} = 1.$$

Also ist $\exp(B) = 3$. Sei $y \in \text{Aut}(B)$ mit $y(b) = bd^{-1}$, $y(x) = cx$ und $[y, a] = [y, c] = [y, d] = 1$. Da die Bilder von y die gleichen Relationen wie a, b, c, d, x erfüllen, ist y tatsächlich ein Automorphismus. Wegen $y^3(b) = bd^{-3} = b$ und $y^3(x) = c^3x = x$ hat y Ordnung 3. In $C := B \rtimes \langle y \rangle$ gilt

$$(b^i x^j y)^3 = b^i x^j \cdot b^i d^{-i} c^j x^j \cdot b^i d^i c^{-j} x^j = 1.$$

Also ist $\exp(C) = 3$. Sei schließlich $z \in \text{Aut}(C)$ mit $y' := z(y) = a^{-1}y$, $x' := z(x) = b^{-1}x$, $c' := z(c) = cd^{-1}$ und $[z, a] = [z, b] = [z, d] = 1$. Wegen

$$y'(x') = a^{-1}yb^{-1}xy^{-1}a = a^{-1}b^{-1}dyxy^{-1}a = a^{-1}b^{-1}dcxa = a^{-1}b^{-1}dcadx = c'x'$$

ist z tatsächlich ein Automorphismus. Wie zuvor hat z Ordnung 3. In $G := C \rtimes \langle z \rangle$ gilt

$$\begin{aligned} (a^{i_a} b^{i_b} c^{i_c} d^{i_d} x^j y^k z)^3 &= a^{i_a} b^{i_b} c^{i_c} d^{i_d} \cdot a^{i_a-k} b^{i_b-j} c^{i_c+jk} d^{i_d-i_c-i_bk+i_a j} \cdot x^{2j} y^{2k} z^2 a^{i_a} b^{i_b} c^{i_c} d^{i_d} x^j y^k z \\ &= a^{i_a} b^{i_b} c^{i_c} d^{i_d} \cdot a^{i_a-k} b^{i_b-j} c^{i_c+jk} d^{i_d-i_c-i_bk+i_a j} \cdot a^{i_a+k} b^{i_b+j} c^{i_c-jk} d^{i_d+i_c+i_bk-i_a j} = 1, \end{aligned}$$

d. h. $\exp(G) = 3$. Wegen ist $G = \langle x, y, z \rangle$ und $|G| = 3^7$ ist $G \cong B(3, 3)$. □

Satz 12.10 (SANOV). Für $d \geq 1$ gilt $|B(d, 4)| < \infty$.

Beweis. Sei $G := B(d, 4)$. O.B.d.A. sei $d \geq 2$. Nach Induktion ist $H := \langle x_1, \dots, x_{d-1} \rangle$ endlich. Sei $y := x_d^2$. Wir zeigen zunächst, dass $K := \langle y, H \rangle$ endlich ist. Die Behauptung folgt dann mit dem gleichen Argument für K und x_d anstelle von H und y . Jedes $g \in K$ hat die Form $g = h_1 y h_2 \dots y h_n$ mit $h_1, \dots, h_n \in H$. Sei dabei n so klein wie möglich. Nehmen wir $n \geq 2|H| + 3$ an. Dann gibt es unter den Elementen $h_2 h_3^{-1}$, $h_2 h_4 (h_3 h_5)^{-1}$, $h_2 h_4 (h_3 h_5 h_7)^{-1}$, ... zwei gleiche, sagen wir

$$h_2 h_4 \dots h_{2r} (h_3 h_5 \dots h_{2r+1})^{-1} = h_2 \dots h_{2s} (h_3 \dots h_{2s+1})^{-1}$$

²⁸Zum Beispiel mit `OneGroup(3^7, RankPGroup, 3, Exponent, 3);`

mit $r < s \leq (n-1)/2$. Also ist

$$h_{2r+2}h_{2r+4}\dots h_{2s}(h_{2r+3}h_{2r+5}\dots h_{2s+1})^{-1} = 1.$$

Wegen $\exp(G) = 4$ und $y^2 = 1$ ist

$$yhy = h^{-1}y^{-1}h^{-1}y^{-1}h^{-1} = h^{-1}yh^{-1}yh^{-1}$$

für $h \in H$. Wir wenden dieser Regel auf $h = h_{2s+1}$ in g an:

$$g = h_1yh_2\dots h_{2s}h_{2s+1}^{-1}yh'_{2s+1}y\dots yh_n.$$

Durch erneute Anwendung mit $h = h_{2s}h_{2s+1}^{-1}$ wird h_{2s-1} durch $h_{2s-1}(h_{2s}h_{2s+1}^{-1})^{-1} = h_{2s-1}h_{2s+1}h_{2s}^{-1}$ ersetzt. Danach wird h_{2s-2} durch $h_{2s-2}h_{2s}(h_{2s-1}h_{2s+1})^{-1}$ ersetzt usw. Schließlich wird h_{2r+2} durch 1 ersetzt. Dies widerspricht der Minimalität von n . Folglich ist $n \leq 2|H|+2$ und man erhält $|K| < \infty$. \square

Beispiel 12.11. Sei $F := F_2$ und $N := \langle x^2 : x \in F \rangle$. Dann ist $|F/N| = 4$ und Schreiers Formel zeigt $N \cong F_5$. Daher hat $M := \langle x^2 : x \in N \rangle$ Index 32 in N . Da N charakteristisch in G ist, gilt $M \trianglelefteq G$. Nun hat $G = F/M$ Ordnung 2^7 , Exponent 4 und zwei Erzeugern. Dies zeigt $|B(2, 4)| \geq 2^7$. Das gleiche Argument liefert $|B(2, 8)| \geq 2^{7+2^7+1} = 2^{136}$ und $|B(3, 4)| \geq 2^{3+17} = 2^{20}$.

Bemerkung 12.12. Es gilt $|B(2, 4)| = 2^{12}$, $|B(3, 4)| = 2^{69}$, $|B(4, 4)| = 2^{422}$ und $|B(5, 4)| = 2^{2728}$. Hall bewies

$$|B(d, 6)| = 2^{1+3^a(d-1)} 3^{b+\binom{b}{2}+\binom{b}{3}}$$

mit $a = d + \binom{d}{2} + \binom{d}{3}$ und $b = 1 + 2^d(d-1)$. Man weiß $|B(d, e)| = \infty$ für alle $d \geq 2$ und $e \geq 8000$ (und alle ungeraden $e \geq 557$).²⁹³⁰

Definition 12.13.

- Sei M der Durchschnitt aller Normalteiler von $B(d, e)$ mit endlichem Index und $B_0(d, e) := B(d, e)/M$. Das Burnside-Problem (III) ist äquivalent zu $|B_0(d, e)| < \infty$ für alle $d, e \in \mathbb{N}$.
- Sei G eine endliche Gruppe und p eine Primzahl. Wir definieren $N_0 := 1$ und

$$N_{2k-1}/N_{2k-2} := \text{O}_{p'}(G/N_{2k-2}), \quad N_{2k}/N_{2k-1} := \text{O}_p(G/N_{2k-1})$$

für $k \geq 1$. Existiert ein $k \geq 0$ mit $N_k = G$, so nennt man G *p-auflösbar*. Ggf. nennt man die kleinste Zahl $l := l_p(G) \geq 0$ mit $N_{2l+1} = G$ die *p-Länge* von G .

Bemerkung 12.14.

- Ist G *p*-auflösbar, kann man die Normalreihe $N_0 < \dots < N_k$ zu einer Hauptreihe und einer Kompositionsreihe verfeinern. Daher sind alle Haupt- und Kompositionsfaktoren *p*-Gruppen oder *p'*-Gruppen. Insbesondere ist jeder minimale Normalteiler von G eine *p*-Gruppe oder eine *p'*-Gruppe.
- Offenbar ist jede auflösbare Gruppe *p*-auflösbar für jede Primzahl *p*.

²⁹Siehe <https://arxiv.org/abs/2303.15997v5>

³⁰Magnus kommentierte die erste Arbeit dieser Art als "This paper is possibly the most difficult paper to read that has ever been written on mathematics."

Lemma 12.15 (HALL-HIGMAN). Sei G eine p -auflösbare Gruppe mit $O_{p'}(G) = 1$. Dann ist

$$C_G(O_p(G)) \leq O_p(G).$$

Beweis. O.B.d.A. $N := O_p(G)$. Dann ist $C_G(N)N/N \trianglelefteq G/N$. Im Fall $C_G(N) \not\leq N$ existiert ein minimaler Normalteiler $M/N \trianglelefteq G/N$ mit $M \leq C_G(N)N$. Wegen $O_p(G/N) = 1$ ist M/N eine p' -Gruppe (Bemerkung 12.14). Nach Schur-Zassenhaus ist $M = N \rtimes H$. Da $C_G(N)N/C_G(N) \cong N/Z(N)$ eine p -Gruppe ist, gilt $H \leq C_G(N)$ und $M = N \times H$. Dann wäre aber $H \leq O_{p'}(M) \leq O_{p'}(G) = 1$. \square

Satz 12.16. Sei G p -auflösbar und c_p die Nilpotenzklasse einer p -Sylowgruppe von G . Dann gilt $l_p(G) \leq c$.

Beweis. Induktion nach c : Im Fall $c = 0$ ist $G = O_{p'}(G)$ und $l_p(G) = 0$. Sei nun $c > 0$ und $P \in \text{Syl}_p(G)$. O.B.d.A. sei $O_{p'}(G) = 1$ und $N := O_p(G) > 1$. Nach Hall-Higman ist $Z(P) \leq C_G(P) \leq C_G(N) \leq N$. Die p -Sylowgruppe

$$PN/N \cong P/P \cap N \cong (P/Z(P))/((N \cap P)/Z(P))$$

von G/N hat also Nilpotenzklasse $\leq c - 1$. Nach Induktion ist $l_p(G) = l_p(G/N) + 1 \leq c$. \square

Satz 12.17. Für $d \geq 1$ gilt $|B_0(d, 6)| \leq |B_0(d, 12)| < \infty$.

Beweis. Da $B_0(d, 6)$ eine Faktorgruppe von $B_0(d, 12)$ ist, genügt es $|B_0(d, 12)| < \infty$ zu zeigen. Sei G eine endliche Gruppe mit d Erzeugern und Exponent 12. Nach Burnside's $p^a q^b$ -Satz ist G auflösbar. Eine 3-Sylowgruppe P von G hat Exponent ≤ 3 und Nilpotenzklasse ≤ 3 nach Lemma 12.7. Nach Satz 12.16 ist $l_3(G) \leq 3$. Sei also $1 = N_0 \leq \dots \leq N_7 = G$ wie in Definition 12.13. Dann ist G/N_6 eine 2-Gruppe mit d Erzeugern und Exponent ≤ 4 . Nach Satz 12.10 ist $|G/N_6|$ durch eine Funktion in d beschränkt. Nach Reidemeister-Schreier ist die Anzahl der Erzeuger von N_6 durch eine Funktion in d beschränkt. Außerdem hat N_6/N_5 Exponent ≤ 3 . Nach Satz 12.9 ist auch $|N_6/N_5|$ durch eine Funktion in d beschränkt. Führt man auf diese Weise fort, so erhält man eine obere Schranke für $|G|$. \square

Bemerkung 12.18. Hall und Higman zeigten, dass man die p -Länge von G durch eine Funktion in dem Exponenten einer p -Sylowgruppe von G abschätzen kann. Mit Hilfe der CFSG kann man die Frage $|B_0(d, n)| < \infty$ nun auf den Fall zurückführen, in dem $n = p^k$ eine Primzahlpotenz ist. Zelmanov bewies schließlich $|B_0(d, p^k)| < \infty$.

Definition 12.19. Sei $G = \langle x_1, \dots, x_n \rangle$. Wir definieren rekursiv eine Menge von *Basiskommutatoren* c_1, c_2, \dots wie folgt:

- Für $i = 1, \dots, n$ seien $c_i := x_i$ die Basiskommutatoren mit *Gewicht* $\omega(c_i) := 1$.
- Die Basiskommutatoren c_1, \dots, c_k seien bereits definiert. Für $1 \leq i < j \leq k$ ist $c := [c_i, c_j]$ ein Basiskommutator, falls entweder $\omega(c_j) = 1$ oder $c_j = [c_s, c_t]$ mit $i \geq s$ gilt. Ggf. sei $\omega(c) := \omega(c_i) + \omega(c_j)$.
- Die Basiskommutatoren werden aufsteigend nach Gewicht nummeriert, wobei die Reihenfolge der Kommutatoren mit dem gleichen Gewicht keine Rolle spielt.

Für $k \in \mathbb{N}$ sei $\delta_n(k)$ die (endliche) Anzahl der Basiskommutatoren mit Gewicht k . Hierbei gelten Basiskommutatoren als verschieden, selbst wenn sie die gleichen Gruppenelemente repräsentieren (z. B. wenn G abelsch ist). Wir zeigen in Bemerkung 12.31, dass in der freien Gruppe $G = F_n$ Basiskommutatoren tatsächlich paarweise verschieden sind.

Beispiel 12.20. Offenbar gilt $\delta_n(1) = n$ und $\delta_n(2) = \binom{n}{2}$. Für $n = 3$ und $(x_1, x_2, x_3) = (x, y, z)$ sind

$$x, y, z, [x, y], [x, z], [y, z], [x, x, y], [x, x, z], [y, x, y], [y, x, z], [y, y, z], [z, x, y], [z, x, z], [z, y, z]$$

die Basiskommutatoren mit Gewicht ≤ 3 . Es gilt also $\delta_3(3) = 8$.

Satz 12.21. Sei $G = \langle x_1, \dots, x_n \rangle$ und $k \in \mathbb{N}$. Dann wird $G^{[k]}/G^{[k+1]}$ von den Nebenklassen der Basiskommutatoren mit Gewicht k erzeugt.

Beweis. Für $k = 1$ ist die Behauptung klar denn $G^{[1]} = G$. Sei die Aussage bereits für $k - 1$ bewiesen. Nach Definition wird $G^{[k]}$ von den Kommutatoren $[g, h]$ mit $g \in G$ und $h \in G^{[k-1]}$ erzeugt. Wegen $G^{[k]}/G^{[k+1]} \leq Z(G/G^{[k+1]})$ gilt

$$\begin{aligned} [xy, h] &= {}^x[y, h][x, h] \equiv [x, h][y, h] \pmod{G^{[k+1]}}, \\ [x^{-1}, h] &= [x^{-1}, h][xx^{-1}, h]^{-1} \equiv [x^{-1}, h]([x, h][x^{-1}, j])^{-1} \equiv [x, h]^{-1} \pmod{G^{[k+1]}} \end{aligned}$$

für alle $x, y \in G$. Wir können daher $g = x_i = c_i$ mit $1 \leq i \leq n$ annehmen. Nach Induktion existieren Basiskommutatoren c_{j_1}, \dots, c_{j_l} mit Gewicht $k - 1$ und $h' \in G^{[k]}$ mit $h = c_{j_1} \dots c_{j_l} h'$. Es gilt nun analog

$$[g, h] \equiv [g, c_{j_1}] \dots [g, c_{j_l}][g, h'] \equiv [g, c_{j_1}] \dots [g, c_{j_l}] \pmod{G^{[k+1]}}.$$

Wir können somit $h = c_j$ annehmen. Im Fall $k = 2$ ist $[c_i, c_j]$ oder $[c_j, c_i] = [c_i, c_j]^{-1}$ ein Basiskommutator. Sei also $k \geq 3$ und $c_j = [c_s, c_t]$ mit $s < t$. Im Fall $i \geq s$ ist $[c_i, c_j]$ wieder ein Basiskommutator. Sei daher $i < s < t$. Die Hall-Witt-Identität (GT-Lemma 3.6) vereinfacht sich zu

$$1 = {}^{c_s}[c_i, c_s^{-1}, c_t] \cdot {}^{c_t}[c_s, c_t^{-1}, c_i] \cdot {}^{c_i}[c_t, c_i^{-1}, c_s] \equiv [c_i, c_s^{-1}, c_t][c_s, c_t^{-1}, c_i][c_t, c_i^{-1}, c_s] \pmod{G^{[k+1]}}.$$

Es existiert ein $z \in G^{[k]}$ mit $[c_s^{-1}, c_t] = [c_s, c_t]^{-1}z$ und

$$[c_i, c_s^{-1}, c_t] \equiv [c_i, [c_s, c_t]^{-1}] \equiv [c_i, c_j]^{-1} \pmod{G^{[k+1]}}.$$

Wegen $[G^{[a]}, G^{[b]}] \leq G^{[a+b]}$ (GT-Lemma 3.11) erhält man analog

$$[c_s, c_t^{-1}, c_i] \equiv [c_s, [c_t, c_i]^{-1}] \equiv [c_s, c_i, c_t] \pmod{G^{[k+1]}}$$

und $[c_t, c_i^{-1}, c_s] \equiv [c_t, c_i, c_s]^{-1} \pmod{G^{[k+1]}}$. Insgesamt ist

$$[c_i, c_j] \equiv [c_s, c_i, c_t][c_t, c_i, c_s]^{-1} \pmod{G^{[k+1]}}.$$

Sei $c_u := [c_i, c_t]$ und $c_v := [c_i, c_s]$. Wegen $\omega(c_u) = \omega(c_t) + 1$ ist $s < t < u$. Daher ist $[c_s, c_i, c_t] = [c_s, c_u]$ ein Basiskommutator. Im Fall $t < v$ ist auch $[c_t, c_i, c_s] = [c_t, c_v]$ ein Basiskommutator. Im Fall $t = v$ ist $[c_t, c_v] = 1$. Es bleibt also der Fall $t > v$. Sei $c_t = [c_w, c_y]$. Da $c_j = [c_s, c_t]$ ein Basiskommutator ist, gilt $s \geq w$. Wegen $\omega(c_v) = \omega(c_s) + 1$ ist $v > s \geq w$. Dies zeigt, dass $[c_t, c_v]^{-1} = [c_v, c_t]$ ein Basiskommutator ist. \square

Folgerung 12.22. Jede nilpotente Gruppe, die von endlich vielen Elementen endlicher Ordnung erzeugt wird, ist endlich.

Beweis. Sei $G = \langle x_1, \dots, x_n \rangle$ nilpotent mit Elementen x_1, \dots, x_n endlicher Ordnung. Dann ist $|G/G'| < \infty$. Induktiv können wir $e := |G/G^{[k]}| < \infty$ annehmen. O. B. d. A. sei $G^{[k+1]} = 1$. Nach Satz 12.21 wird $G^{[k]}$ von endlichen vielen Kommutatoren erzeugt. Aus GT-Aufgabe 16 folgt

$$[x, y]^e = [x^e, y] \in G^{[k+1]} = 1$$

für alle $[x, y] \in G^{[k]} \leq Z(G)$. Also ist auch $G^{[k]}$ endlich. \square

Bemerkung 12.23. Der Beweis zeigt: Wird eine nilpotente Gruppe G von endlichen vielen p -Elementen erzeugt, so ist G eine p -Gruppe.

Lemma 12.24. Seien c_1, c_2, \dots die Basiskommutatoren von $G = \langle x_1, \dots, x_n \rangle$. Für alle $k \geq 1$ gibt es genau n^k Folgen $(a_1, a_2, \dots) \in \mathbb{N}_0^\infty$ mit $a_1 \geq a_2 \geq \dots$ und $\sum_{a_i \geq 1} \omega(c_{a_i}) = k$.

Beweis. Für $s \in \mathbb{N}$ sei F_s die Menge aller Folgen $(a_1, a_2, \dots) \in \mathbb{N}_0^\infty$, sodass gilt:

- (i) Es existiert ein $l \in \mathbb{N}_0$ mit $a_1, \dots, a_{l-1} \geq s$, $a_l > s$, $s \geq a_{l+1} \geq a_{l+2} \geq \dots$
- (ii) Gilt $c_{a_m} = [c_i, c_j]$ für ein $m \leq l$, so ist $i < s$.
- (iii) $\sum_{a_i \geq 1} \omega(c_{a_i}) = k$.

Wenn s groß genug ist, so gilt $\omega(c_s) > k$. Ggf. ist $l = 0$ in (i) und (ii) liefert keine Einschränkungen. Daher besteht F_s genau aus den Folgen, die wir zählen wollen. Für $s = 1$ gilt $\omega(c_{a_i}) = 1$ für alle $i \in \mathbb{N}$. Nach (iii) ist dann $a_k > 0 = a_{k+1} = a_{k+2} = \dots$. Ansonsten gibt es keine weiteren Einschränkungen an die Folge. Wegen $a_i \in \{1, \dots, n\}$ folgt $|F_1| = n^k$.

Für ein gegebenes $s \geq 1$ genügt es eine Bijektion $\varphi: F_s \rightarrow F_{s+1}$ zu konstruieren. Sei $a := (a_i) \in F_s$ und l wie in (i). Wir durchlaufen die Folge von rechts nach links beginnend bei a_l . Treffen wir dabei auf ein Paar $(a_i, a_{i+1}) = (s, t)$ mit $t > s$, so ist $c_j := [c_s, c_t]$ nach (ii) ein Basiskommutator. Wir ersetzen ggf. (a_i, a_{i+1}) durch j . Dadurch verändert sich (iii) nicht. Anschließend betrachten wir das Paar (a_{i-1}, j) und iterieren. Die so konstruierte Folge bezeichnen wir mit $\varphi(a)$. Nach Konstruktion gilt $\varphi(a)_i \geq s+1$ für $i = 1, \dots, l$. Im Fall $\varphi(a)_1 = \dots = \varphi(a)_l = s+1$, gilt (i) mit $l = 0$ bzgl. $s+1$. Anderenfalls gilt (i) mit $l := \max\{i : a_i > s+1\}$. Nach Konstruktion erfüllt $\varphi(a)$ auch (ii). Daher gilt $\varphi(a) \in F_{s+1}$.

Sei nun umgekehrt $(b_i)_i \in F_{s+1}$ mit l wie in (i) gegeben. Wir durchlaufen b von links nach rechts beginnend bei b_1 . Gilt $c_{b_i} = [c_s, c_t]$ für ein $i \leq l$, so ersetzen wir b_i durch das Paar (s, t) . Anschließend betrachten wir t bzw. c_t . Dieser Prozess muss wegen $\sum_{b_j \geq 1} \omega(c_{b_j}) = k$ nach endlich vielen Schritten enden. Das Endergebnis bezeichnen wir mit $\psi(b)$. Offenbar gilt $\psi(b) \in F_s$ und die Abbildungen φ und ψ sind zueinander inverse Bijektionen. \square

Lemma 12.25. Für $k \in \mathbb{N}$ gilt

$$\sum_{d|k} \delta_n(d) d = n^k.$$

Beweis. Sei S_k die Menge der Folgen $(a_1, a_2, \dots) \in \mathbb{N}_0^\infty$ aus Lemma 12.24. Kommt ein Basiskommutator c_j genau t -mal in $(a_i)_i \in S_k$ vor, so trägt er $t\omega(c_j)$ zur Summe $\sum_{a_i \geq 1} \omega(c_{a_i}) = k$ bei. Sei K_w die Menge der Basiskommutatoren mit Gewicht w . Aus Lemma 12.24 erhält man eine Identität von formalen Potenzreihen:

$$\begin{aligned} \prod_{w=1}^{\infty} (1 - X^w)^{-\delta_n(w)} &= \prod_{w=1}^{\infty} (1 + X^w + X^{2w} + \dots)^{\delta_n(w)} = \prod_{w=1}^{\infty} \prod_{c \in K_w} (1 + X^{\omega(c)} + X^{2\omega(c)} + \dots) \\ &= \prod_{i=1}^{\infty} (1 + X^{\omega(c_i)} + X^{2\omega(c_i)} + \dots) = 1 + \sum_{k=1}^{\infty} \sum_{(a_i) \in S_k} X^k = \sum_{k=0}^{\infty} n^k X^k = (1 - nX)^{-1}. \end{aligned}$$

Wir wenden auf beiden Seiten den formalen Logarithmus $\log(1 - X) := -\sum_{k=1}^{\infty} \frac{1}{k} X^k$ an:³¹

$$\sum_{k=1}^{\infty} \frac{n^k}{k} X^k = -\log(1 - nX) = -\sum_{w=1}^{\infty} \delta_n(w) \log(1 - X^w) = \sum_{w=1}^{\infty} \sum_{k=1}^{\infty} \frac{\delta_n(w)}{k} X^{wk} = \sum_{k=1}^{\infty} \sum_{d|k} \frac{d\delta_n(d)}{k} X^k.$$

Ein Koeffizientenvergleich zeigt die Behauptung. \square

Satz 12.26 (WITTS Formel). Sei $G = \langle x_1, \dots, x_n \rangle$ und $k \in \mathbb{N}$. Dann wird $G^{[k]}/G^{[k+1]}$ von

$$\delta_n(k) = \frac{1}{k} \sum_{d|k} \mu(d) n^{k/d}$$

Elementen erzeugt. Dabei ist μ die Möbius-Funktion aus der Zahlentheorie.

Beweis. Nach Satz 12.21 wird $G^{[k]}/G^{[k+1]}$ von den $\delta_n(d)$ Basiskommutatoren mit Gewicht k erzeugt. Die Formel für $\delta_n(d)$ folgt durch Möbius-Inversion aus Lemma 12.25. \square

Bemerkung 12.27. Wir zeigen als Nächstes, dass die Abschätzung für die Anzahl der Erzeuger von $G^{[k]}/G^{[k+1]}$ in Satz 12.26 für die freie Gruppe optimal ist.

Definition 12.28.

- Sei $M := \langle X_1, \dots, X_n \rangle$ das Monoid aller Monome $X_{i_1} \dots X_{i_k}$ mit $k \geq 0$ und $1 \leq i_1, \dots, i_k \leq n$ in den nicht-vertauschbaren Variablen X_1, \dots, X_n bzgl. Konkatenation (also die freie Gruppe ohne Inverse).
- Sei R ein kommutativer Ring und $A := RM$ der freie R -Modul mit Basis M . Indem man die Konkatenation distributiv fortsetzt, wird A zu einem Ring. Zum Beispiel gilt

$$(1 + X_2 X_1^2)(X_1 + X_3 X_2) = X_1 + X_2 X_1^3 + X_3 X_2 + X_2 X_1^2 X_3 X_2.$$

Man nennt A die *freie Algebra* über X_1, \dots, X_n .

- Sei $\deg(X_{i_1} \dots X_{i_k}) := k$ der *Grad* eines Monoms. Sei A_k der von den Monomen vom Grad k erzeugte freie R -Untermodule von A , d. h. A_k besteht aus allen *homogenen Polynomen* vom Grad k . Offenbar ist $\text{rk}(A_k) = n^k$ und $A = \bigoplus_{k \geq 0} A_k$.
- Der *Kommutator* von $a, b \in A$ ist $[a, b] := ab - ba$. Die Basiskommutatoren in A definiert man analog zu Definition 12.19. Anstatt c_i schreiben wir C_i . Für $n = 2$ und $(X_1, X_2) = (X, Y)$ ist zum Beispiel

$$C_4 = [C_1, C_3] = X[X, Y] - [X, Y]X = X(XY - YX) - (XY - YX)X = X^2Y - 2XYX + YX^2$$

(vgl. Beispiel 12.20).

Lemma 12.29. Für alle $k \in \mathbb{N}$ ist

$$B_k := \left\{ C_{a_1} \dots C_{a_m} : m \in \mathbb{N}, a_1 \geq \dots \geq a_m, \sum_{i=1}^m \omega(c_{a_i}) = k \right\}$$

eine Basis von A_k . Insbesondere sind die Basiskommutatoren mit Gewicht k linear unabhängig über \mathbb{Z} .

³¹Siehe Kombinatorik-Skript

Beweis. Man sieht leicht induktiv, dass ein Basiskommutator mit Gewicht k in A_k liegt. Daher gilt $B_k \subseteq A_k$. Nach Lemma 12.24 ist $|B_k| = n^k = \text{rk}(A_k)$. Wir zeigen zunächst, dass B_k ein Erzeugendensystem von A_k ist. Dafür betrachten wir die Mengen F_s aus dem Beweis von Lemma 12.24. Wenn s groß genug ist, so besteht B_k genau aus den Produkten $C_{a_1} \dots C_{a_m}$ mit $a = (a_i)_i \in F_s$ (Nullen werden aus der Folge entfernt). Andererseits entspricht F_1 genau den Monomen $X_{i_1} \dots X_{i_k}$. Es genügt daher zu zeigen, dass man $C := C_{a_1} \dots C_{a_m}$ mit $a \in F_s$ durch eine Linearkombination von $C_{b_1} \dots C_{b_{m'}}$ mit $b \in F_{s+1}$ ausdrücken kann. Wie im Beweis von Lemma 12.24 durchlaufen wir die Folge a von rechts nach links. Gilt $(a_i, a_{i+1}) = (s, t)$ mit $t > s$, ersetzen wir $C_s C_t$ in C durch den gleichwertigen Ausdruck $[C_s, C_t] + C_t C_s$. Mit $C_j = [C_s, C_t]$ gilt

$$C = C_{a_1} \dots C_{a_{i-1}} C_j C_{a_{i+2}} \dots C_{a_m} + C_{a_1} \dots C_{a_{i+1}} C_{a_i} \dots C_{a_m}.$$

Mit dem ersten Summanden verfahren wir wie zuvor. Im zweiten Summanden ist $C_{a_i} = C_s$ nach rechts gerückt. Die entsprechende Folge liegt immer noch in F_s und kann wie die Ausgangsfolge behandelt werden. Nach endlich vielen Schritten erreicht man eine Linearkombination von $C_{b_1} \dots C_{b_{m'}}$ mit $b \in F_{s+1}$.

Also ist B_k ein Erzeugendensystem von A_k .³² Es gibt daher eine Matrix $M \in R^{n^k \times n^k}$, sodass die Abbildung $\varphi: R^{n^k} \rightarrow A_k \cong R^{n^k}$, $v \mapsto Mv$ surjektiv ist. Für den i -ten Standardbasisvektor $e_i \in R^{n^k}$ existiert ein $x_i \in R^{n^k}$ mit $Mx_i = e_i$. Sei $L \in R^{n^k \times n^k}$ die Matrix mit Spalten x_1, \dots, x_{n^k} . Dann gilt $ML = 1_{n^k}$ und $\det(M) \in R^\times$. Für die zu M komplementäre Matrix M^* erhält man $\det(M)^{-1} M^* M = 1_{n^k}$. Dies zeigt, dass φ injektiv ist. Somit ist B_k linear unabhängig. \square

Definition 12.30. Wie zuvor sei $A := R\langle X_1, \dots, X_n \rangle$. Sei $I := A_{>k} := \sum_{l>k}^\infty A_l$ das von A_{k+1} erzeugte Ideal in A . Sei $\bar{A} := A/I$ und $\mathcal{A} := (1 + A_{>0} + I)/I \subseteq \bar{A}$.

Bemerkung 12.31. Für $a = 1 + a_1 + I \in \mathcal{A}$ gilt

$$a(1 - a_1 + a_1^2 \mp \dots \pm a_1^k + I) = 1 \pm a_1^{k+1} + I = 1.$$

Daher ist $\mathcal{A} \subseteq \bar{A}^\times$.

Satz 12.32. Sei F die freie Gruppe vom Rang n und $k \in \mathbb{N}$. Dann ist $F^{[k]}/F^{[k+1]}$ eine freie abelsche Gruppe vom Rang $\delta_n(k)$.

Beweis. Sei F frei bzgl. x_1, \dots, x_n . Wir betrachten $A = \mathbb{Z}\langle X_1, \dots, X_n \rangle$ mit $R = \mathbb{Z}$. Nach der universellen Eigenschaft von F existiert ein Homomorphismus $\varphi: F \rightarrow \mathcal{A}$ mit $\varphi(x_i) = 1 + X_i + I$. Wir zeigen

$$\varphi(c_i) \equiv 1 + C_i \pmod{\overline{A_{>\omega(c_i)}}}$$

für jeden Basiskommutator c_i . Dies ist klar für $\omega(c_i) = 1$. Sei $w_i := \omega(c_i)$ und $w_j := \omega(c_j)$. Nach Induktion existieren $\epsilon_i, \epsilon'_i \in \overline{A_{>w_i}}$ und $\epsilon_j, \epsilon'_j \in \overline{A_{>w_j}}$ mit $\varphi(c_i) = 1 + C_i + \epsilon_i$, $\varphi(c_i)^{-1} = 1 - C_i + \epsilon'_i$, $\varphi(c_j) = 1 + C_j + \epsilon_j$ und $\varphi(c_j)^{-1} = 1 - C_j + \epsilon'_j$ (Bemerkung 12.31). Aus

$$1 = \varphi(c_i)\varphi(c_i)^{-1} = (1 + C_i + \epsilon_i)(1 - C_i + \epsilon'_i) = 1 + \epsilon_i + \epsilon'_i - C_i^2 + C_i\epsilon'_i - \epsilon_i C_i + \epsilon_i \epsilon'_i$$

³²Da R im Allgemeinen kein Körper ist, folgt die lineare Unabhängigkeit nicht automatisch.

folgt

$$\begin{aligned}
\varphi([c_i, c_j]) &= (1 + C_i + \epsilon_i)(1 + C_j + \epsilon_j)(1 - C_i + \epsilon'_i)(1 - C_j + \epsilon'_j) \\
&\equiv 1 + C_i + C_j - C_i - C_j + \epsilon_i + \epsilon_j + \epsilon'_i + \epsilon'_j + C_i C_j - C_i C_j - C_j C_i + C_i C_j \\
&\quad - C_i^2 + C_i \epsilon'_i - \epsilon_i C_i + \epsilon_i \epsilon'_i - C_j^2 + C_j \epsilon'_j - \epsilon_j C_j + \epsilon_j \epsilon'_j \pmod{\overline{A_{>w_i+w_j}}} \\
&\equiv 1 + [C_i, C_j] \pmod{\overline{A_{>\omega([c_i, c_j])}}},
\end{aligned}$$

wie behauptet. Dies impliziert $\varphi(F^{[k+1]}) = 1$. Seien c_{i_1}, \dots, c_{i_m} die Basiskommutatoren von F mit Gewicht k . Nach Satz 12.21 wird $F^{[k]}/F^{[k+1]}$ von $c_{i_1}F^{[k+1]}, \dots, c_{i_m}F^{[k+1]}$ erzeugt. Seien $a_1, \dots, a_m \in \mathbb{Z}$ mit $g := c_{i_1}^{a_1} \dots c_{i_m}^{a_m} \in F^{[k+1]}$. Dann gilt

$$1 = \varphi(g) = (1 + C_{i_1})^{a_1} \dots (1 + C_{i_m})^{a_m} = 1 + a_1 C_{i_1} + \dots + a_m C_{i_m}.$$

Aus Lemma 12.29 folgt $a_1 = \dots = a_m = 0$. Also ist $c_{i_1}F^{[k+1]}, \dots, c_{i_m}F^{[k+1]}$ eine Basis von $F^{[k]}/F^{[k+1]}$. \square

Bemerkung 12.33. Nach Bemerkung 2.10 ist F'_2 frei mit (abzählbar) unendlichem Rang. Daher ist F'_2/F''_2 nicht endlich erzeugt.

Folgerung 12.34. Die freie nilpotente Gruppe $F_n/F_n^{[k+1]}$ vom Rang n und Nilpotenzklasse k ist torsionsfrei.

Satz 12.35. Für jede Primzahlpotenz $q = p^e$ gilt:

- (i) Es existiert genau eine Gruppe P mit n Erzeugern, Exponent q , Nilpotenzklasse $p - 1$ und $P^{[k]}/P^{[k+1]} \cong C_q^{\delta_n(k)}$ für $k = 1, \dots, p - 1$.
- (ii) Es existiert eine Gruppe P mit n Erzeugern, Exponent q und Nilpotenzklasse $q - 1$, sodass $P^{[k]}/P^{[k+1]}$ für $k = 1, \dots, q - 1$ Rang $\delta_n(k)$ besitzt.

Beweis. Sei F die freie Gruppe mit Erzeugern x_1, \dots, x_n . Sei $N := \langle g^q : g \in F \rangle \trianglelefteq F$ und $\overline{F} := F/N$.

- (i) Wir betrachten $A := R\langle X_1, \dots, X_n \rangle$ mit $R = \mathbb{Z}/q\mathbb{Z}$. In der Definition von \mathcal{A} sei $k < p$. Für $1 + a \in \mathcal{A}$ gilt dann

$$(1 + a)^q = 1 + qa + \binom{q}{2}a^2 + \dots + \binom{q}{p}a^p + \dots = 1.$$

Für die Abbildung $\varphi: F \rightarrow \mathcal{A}$, $x_i \mapsto 1 + X_i + I$ aus dem Beweis von Satz 12.32 gilt also $\varphi(N) = 1$. Die Nebenklassen der Basiskommutatoren $c_{i_1}, \dots, c_{i_m} \in F$ mit Gewicht k bilden wie bisher ein Erzeugendensystem von $\overline{F}^{[k]}/\overline{F}^{[k+1]}$. Seien $a_1, \dots, a_m \in R$ mit $g := c_{i_1}^{a_1} \dots c_{i_m}^{a_m} \in NF^{[k+1]}$. Dann gilt wie zuvor $\varphi(g) = 1$ und $a_1 = \dots = a_m = 0$. Dies zeigt, dass $\overline{F}^{[k]}/\overline{F}^{[k+1]} \cong F^{[k]}/F^{[k+1]}N$ ein freier R -Modul mit Rang $\delta_n(k)$ ist. Also hat $P := \overline{F}/\overline{F}^{[p]} \cong F/NF^{[p]}$ die gewünschten Eigenschaften.

Sei umgekehrt Q eine p -Gruppe mit den angegebenen Eigenschaften. Dann existiert ein Epimorphismus $\sigma: F \rightarrow Q$ mit $NF^{[p]} \leq \text{Ker}(\sigma)$. Insbesondere ist $|P| \geq |Q|$. Aus

$$|Q| = q^{\delta_n(1) + \dots + \delta_n(p-1)} = |P|$$

folgt $Q \cong P$.

- (ii) Diesmal betrachten wir $A = \mathbb{F}_p\langle X_1, \dots, X_n \rangle$ und $k < q$ in der Definition von \mathcal{A} . Für $1 + a \in \mathcal{A}$ gilt nach wie vor

$$(1 + a)^q = \sum_{k=0}^q \binom{q}{k} a^k = 1$$

wegen $\binom{q}{k} \equiv 0 \pmod{p}$ für $k = 1, \dots, q-1$. Man erhält also wieder einen Homomorphismus $\varphi: F \rightarrow \mathcal{A}$ mit $\varphi(N) = 1$. Da die Basiskommutatoren mit Gewicht k linear unabhängig über \mathbb{F}_p sind, hat $\overline{F}^{[k]}/\overline{F}^{[k+1]}$ Rang $\delta_n(k)$ (aber nicht unbedingt Exponent q). Um zu zeigen, dass $P := \overline{F}/\overline{F}^{[q]} \cong F/NF^{[q]}$ Exponent q hat, betrachten wir einen Epimorphismus $\psi: F \rightarrow C_q^n$. Wegen $\psi(NF') = 1$ ist $P/P' \cong F/F'N \cong C_q^n$. \square

Bemerkung 12.36.

- (i) Satz 12.35 zeigt $\lim_{p \rightarrow \infty} \log_p |B(n, p)| = \infty$ für $n \geq 2$. Für die Gruppe P aus Satz 12.35(i) gilt genauer

$$\log_q |P| = \sum_{k=1}^{q-1} \delta_n(k) = \sum_{k=1}^{q-1} \frac{1}{k} \sum_{d|k} \mu(d) n^{k/d} = \sum_{d=1}^{q-1} \frac{\mu(d)}{d} \sum_{e=1}^{\lfloor (q-1)/d \rfloor} \frac{n^e}{e}.$$

- (ii) Bekanntlich ist jede Gruppe mit Exponent 2 abelsch, d. h. die Nilpotenzklasse ist ≤ 1 . Man kann Satz 12.35 also nicht auf höhere Nilpotenzklassen übertragen.
- (iii) Sei $p = q > 2$ und P die Gruppe aus Satz 12.35(i). Dann ist $P/P^{[3]}$ eine maximale Schur-Erweiterung von C_p^n (Beispiel 5.21).
- (iv) In Satz 12.35(i) hat $\overline{F}^{[k]}/\overline{F}^{[k+1]}$ nicht unbedingt Exponent q . In der Tat gibt es keine Gruppe mit zwei Erzeugern, Ordnung 2^6 , Exponent 4 und Nilpotenzklasse 2:

`OneGroup(2^6, RankPGroup, 2, Exponent, 4, NilpotencyClassOfGroup, 2);`

Beispiel 12.37. Für $q \in \{3, 5\}$ erhält man $|B(n, 3)| \geq 3^{n+\binom{n}{2}} = 3^{\binom{n+1}{2}}$ (vgl. Satz 12.9) und $|B(2, 5)| \geq 5^{2+1+2+3} = 5^8$. Tatsächlich gilt $|B_0(2, 5)| = 5^{34}$ (ohne Beweis).

Bemerkung 12.38. Eindeutig bestimmte Gruppen mit gewissen Eigenschaften wie in Satz 12.35 werden wir allgemeiner in Satz 13.29 konstruieren.

13 Gruppenklassen und Varietäten

Definition 13.1. Eine Klasse \mathcal{X} von Gruppen heißt *Gruppenklasse*, falls $1 \in \mathcal{X}$ und $G \cong H \in \mathcal{X} \Rightarrow G \in \mathcal{X}$. Die Elemente von \mathcal{X} heißen \mathcal{X} -Gruppen oder Gruppen mit Eigenschaft \mathcal{X} . Eine Gruppe G heißt *residuale \mathcal{X} -Gruppe*, falls für alle $g \in G \setminus \{1\}$ ein $N \trianglelefteq G$ mit $g \notin N$ und $G/N \in \mathcal{X}$ existiert. Die residualen \mathcal{X} -Gruppen bilden die Gruppenklasse \mathcal{X}^r .

Bemerkung 13.2. Offenbar gilt $G \in \mathcal{X}^r$ genau dann, wenn $\bigcap_{\substack{N \trianglelefteq G \\ N \in \mathcal{X}}} N = 1$. Ggf. ist G zu einer Untergruppe von $\bigtimes_{\substack{N \trianglelefteq G \\ N \in \mathcal{X}}} G/N$ isomorph. Ist $\{G_i : i \in I\}$ eine beliebige Familie von Gruppen, so nennt man $H \leq \bigtimes_{i \in I} G_i$ *subdirektes Produkt*, falls die Projektion von H auf jedes G_i surjektiv ist.

Satz 13.3. Sei \mathcal{X} eine Gruppenklasse. Dann besteht \mathcal{X}^r genau aus den subdirekten Produkten von \mathcal{X} -Gruppen.

Beweis. Nach Bemerkung 13.2 ist jede residuale \mathcal{X} -Gruppe ein subdirektes Produkt von \mathcal{X} -Gruppen. Sei umgekehrt $H \leq \times_{i \in I} G_i$ ein subdirektes Produkt von \mathcal{X} -Gruppen G_i . Sei $\pi_i: H \rightarrow G_i$ die Projektion und $K_i := \text{Ker}(\pi_i) \trianglelefteq H$. Nach Voraussetzung ist $H/K_i \cong G_i \in \mathcal{X}$ und $\bigcap_{i \in I} K_i = 1$. \square

Beispiel 13.4. Ist \mathcal{X} die Gruppenklasse der abelschen Gruppen, so ist $\mathcal{X}^r = \mathcal{X}$.

Satz 13.5 (IWASAWA). Jede freie Gruppe ist eine residual endliche p -Gruppe für jede Primzahl p .

Beweis. Sei $a = x_1^{a_1} \dots x_n^{a_n} \in F_X \setminus \{1\}$ mit $x_i \neq x_{i+1}$ und $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$ wie in Folgerung 1.9. Sei q eine Potenz von p , die nicht $a_1 \dots a_n$ teilt. Sei $E_{st} \in \mathbb{Z}/q\mathbb{Z}^{(n+1) \times (n+1)}$ die Matrix mit einer 1 an Position (s, t) und sonst nur Nullen. Für $x \in X$ sei

$$\sigma(x) := \prod_{\substack{1 \leq i \leq n \\ x_i = x}} (1_{n+1} + E_{i,i+1}) \in \text{GL}(n+1, \mathbb{Z}/q\mathbb{Z}).$$

Offenbar besteht $G := \langle \sigma(x) : x \in X \rangle$ aus oberen Dreiecksmatrizen mit Einsen auf der Hauptdiagonale. Daher ist G eine endliche p -Gruppe. Nach der universellen Eigenschaft setzt sich σ zu einem Homomorphismus $\hat{\sigma}: F \rightarrow G$ fort. Wegen $E_{st}E_{uv} = \delta_{tu}E_{sv}$ und $x_i \neq x_{i+1}$ sind die Faktoren von $\sigma(x)$ paarweise vertauschbar. Dies zeigt

$$\sigma(x_i)^{a_i} = \prod_{x_j = x_i} (1_{n+1} + E_{j,j+1})^{a_i} = \prod_{x_j = x_i} (1_{n+1} + a_i E_{j,j+1}) = 1_{n+1} + a_i \sum_{x_j = x_i} E_{j,j+1}.$$

Daraus folgt

$$\hat{\sigma}(a) = \sigma(x_1)^{a_1} \dots \sigma(x_n)^{a_n} = 1_{n+1} + a_1 \dots a_n E_{1,n+1} + \dots \neq 1_{n+1}. \quad \square$$

Folgerung 13.6 (MAGNUS). Jede freie Gruppe ist residual nilpotent.

Bemerkung 13.7. Für jede nicht-abelsche freie Gruppe F gilt $F^{[\infty]} = \bigcap_{k=1}^{\infty} F^{[k]} = 1$ und $Z(F) = 1$. Die auf- und absteigenden Zentralreihen verhalten sich also völlig verschieden.

Lemma 13.8. Sei G eine endlich erzeugte Gruppe. Dann gilt:

- (i) Für jedes $n \in \mathbb{N}$ besitzt G nur endlich viele Untergruppen mit Index n .
- (ii) (HALL) Ist $H \leq G$ mit $|G : H| < \infty$, so existiert eine charakteristische Untergruppe $K \leq G$ mit $K \leq H$ und $|G : K| < \infty$.

Beweis.

- (i) Jede Untergruppe $H \leq G$ vom Index n induziert einen Homomorphismus $G \rightarrow S_n$ mit Kern H_G . Da G endlich erzeugt ist, existieren nur endlich viele solche Homomorphismen. Wegen $H_G \leq H$ gibt es mit H_G auch nur endlich viele Möglichkeiten für H .
- (ii) Nach (i) ist $\{\alpha(H) : \alpha \in \text{Aut}(G)\}$ endlich. Dann hat die charakteristische Untergruppe $K := \bigcap_{\alpha \in \text{Aut}(G)} \alpha(H)$ endlichen Index. \square

Satz 13.9 (BAUMSLAG). *Ist G endlich erzeugt und residual endlich, so ist auch $\text{Aut}(G)$ residual endlich.*

Beweis. Sei $\alpha \in \text{Aut}(G) \setminus \{1\}$ und $g \in G$ mit $\alpha(g) \neq g$. Dann existiert $N \trianglelefteq G$ mit $|G : N| < \infty$ und $\alpha(g)g^{-1} \notin N$. Nach Lemma 13.8 hat die charakteristische Untergruppe $M := \bigcap_{\beta \in \text{Aut}(G)} \beta(N)$ endlichen Index in G . Für $A := C_{\text{Aut}(G)}(G/M) \trianglelefteq \text{Aut}(G)$ gilt daher $|\text{Aut}(A)/A| \leq |\text{Aut}(G/M)| < \infty$. Offenbar ist $\alpha \notin A$. \square

Definition 13.10. Eine Gruppe G heißt *hopfsch*, falls G zu keiner echten Faktorgruppe von G isomorph ist. Das bedeutet, dass jeder Epimorphismus $G \rightarrow G$ ein Automorphismus ist.

Beispiel 13.11. Offenbar sind alle endlichen Gruppen und alle einfachen Gruppen hopfsch. Aus Dimensionsgründen sind auch alle Vektorräume hopfsch. Andererseits ist $C_2^{\mathbb{N}}$ nicht hopfsch.

Satz 13.12 (MAL'CEV). *Jede endlich erzeugte residual endliche Gruppe ist hopfsch.*

Beweis. Sei $\varphi: G \rightarrow G$ ein nicht-injektiver Epimorphismus. Sei $g \in \text{Ker}(\varphi) \setminus \{1\}$. Da G residual endlich ist, existiert ein $N \trianglelefteq G$ mit $g \notin N$ und $|G : N| < \infty$. Da G endlich erzeugt ist, gibt es nur endlich viele Homomorphismen $\gamma_1, \dots, \gamma_n: G \rightarrow G/N$. Dabei sei γ_1 der kanonische Epimorphismus. Aus der Surjektivität von φ folgt $\{\gamma_1, \dots, \gamma_n\} = \{\gamma_1\varphi, \dots, \gamma_n\varphi\}$. Sei also $\gamma_1 = \gamma_k\varphi$. Dann erhält man den Widerspruch $1 \neq gN = \gamma_1(g) = \gamma_k(\varphi(g)) = \gamma_k(1) = 1$. \square

Folgerung 13.13. *Jede freie Gruppe mit endlichem Rang ist hopfsch.*

Beweis. Folgt aus Satz 13.5. \square

Folgerung 13.14. *Sei F frei vom Rang $n < \infty$ und sei $F = \langle Y \rangle$ mit $|Y| = n$. Dann ist F frei bzgl. Y .*

Beweis. Sei $F = F_X$. Eine beliebige Bijektion $X \rightarrow Y \subseteq F$ setzt sich zu einem Epimorphismus $\sigma: F \rightarrow F$ fort. Nach Mal'cev ist $\sigma \in \text{Aut}(F)$. Sei G eine Gruppe und $\tau: Y \rightarrow G$. Dann setzt sich die Abbildung $\tau\sigma|_X$ zu einem Homomorphismus $\gamma: F \rightarrow G$ fort. Schließlich ist $\gamma\sigma^{-1}: F \rightarrow G$ eine Fortsetzung von τ . Wegen $F = \langle Y \rangle$ ist dies die einzige Fortsetzung. Also erfüllt F die universelle Eigenschaft bzgl. Y . \square

Satz 13.15. *Jede endlich erzeugte residual nilpotente Gruppe ist hopfsch.*

Beweis. Sei G endlich erzeugt und residual nilpotent. Nach Voraussetzung ist $\bigcap_{k=1}^{\infty} G^{[k]} = 1$ und nach Lemma 12.6 sind die Faktoren $G^{[k]}/G^{[k+1]}$ endlich erzeugte abelsche Gruppen. Nehmen wir $G \cong G/N$ für ein $1 \neq N \trianglelefteq G$ an. Sei $k \in \mathbb{N}$ mit $N \subseteq G^{[k]}$ und $N \not\subseteq G^{[k+1]}$. Dann ist

$$G^{[k]}/G^{[k+1]} \cong (G/N)^{[k]}/(G/N)^{[k+1]} \cong G^{[k]}/G^{[k+1]}N \cong (G^{[k]}/G^{[k+1]})/(G^{[k+1]}N/G^{[k+1]}).$$

Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen ist $G^{[k]}/G^{[k+1]}$ aber hopfsch. Widerspruch. \square

Satz 13.16 (HALL). *Es existiert eine endlich erzeugte auflösbare Gruppe, die nicht hopfsch ist.*

Beweis. Sei R der Ring aller Zahlen der Form $a2^b$ mit $a, b \in \mathbb{Z}$ und N die Gruppe der oberen 3×3 -Dreiecksmatrizen mit Einsen auf der Hauptdiagonale und Elementen aus R . Wir setzen

$$u := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad v := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad w := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Weiter sei t die Diagonalmatrix mit Diagonale $(1, 2, 1)$. Schließlich definieren wir $H := \langle t, N \rangle$.

Wir zeigen zuerst $H = \langle t, u, v \rangle$. Offenbar ist $u^a = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ für $a \in \mathbb{Z}$. Wegen

$$tu^at^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a2^{-1} & 0 \\ 0 & 2^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a2^{-1} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

ist $\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \langle t, u, v \rangle$ für alle $a \in R$. Analog ist $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} \in \langle t, u, v \rangle$ für alle $a \in R$. Schließlich ist

$$\begin{aligned} \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} v \begin{pmatrix} 1 & -a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} v^{-1} &= \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a & a \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & a \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \langle t, u, v \rangle \end{aligned}$$

für alle $a \in R$. Für $a, b, c \in R$ ist außerdem

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \langle t, u, v \rangle.$$

Dies zeigt $H = \langle N, t \rangle \subseteq \langle t, u, v \rangle \subseteq H$.

Wegen

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a2^{-1} & c \\ 0 & 2^{-1} & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a2^{-1} & c \\ 0 & 1 & b2 \\ 0 & 0 & 1 \end{pmatrix} \in N$$

ist $N \trianglelefteq H = N\langle t \rangle$ und offenbar $N \cap \langle t \rangle = 1$. Nun betrachten wir die Abbildung $f: H \rightarrow H$ mit

$$f \left(\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} t^d \right) = \begin{pmatrix} 1 & a & c2 \\ 0 & 1 & b2 \\ 0 & 0 & 1 \end{pmatrix} t^d$$

für $a, b, c \in R$ und $d \in \mathbb{Z}$. Wir zeigen, dass f ein Endomorphismus ist:

$$\begin{aligned}
f \left(\begin{pmatrix} 1 & a_1 & c_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix} t^{d_1} \begin{pmatrix} 1 & a_2 & c_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix} t^{d_2} \right) &= f \left(\begin{pmatrix} 1 & a_1 & c_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 2^{-d_1} & c_2 \\ 0 & 1 & b_2 2^{d_1} \\ 0 & 0 & 1 \end{pmatrix} t^{d_1+d_2} \right) \\
&= f \left(\begin{pmatrix} 1 & a_2 2^{-d_1} + a_1 & c_2 + a_1 b_2 2^{d_1} + c_1 \\ 0 & 1 & b_2 2^{d_1} + b_1 \\ 0 & 0 & 1 \end{pmatrix} t^{d_1+d_2} \right) = \begin{pmatrix} 1 & a_2 2^{-d_1} + a_1 & (c_2 + a_1 b_2 2^{d_1} + c_1) 2 \\ 0 & 1 & (b_2 2^{d_1} + b_1) 2 \\ 0 & 0 & 1 \end{pmatrix} t^{d_1+d_2} \\
&= \begin{pmatrix} 1 & a_1 & c_1 2 \\ 0 & 1 & b_1 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 2^{-d_1} & c_2 2 \\ 0 & 1 & b_2 2^{d_1+1} \\ 0 & 0 & 1 \end{pmatrix} t^{d_1+d_2} = \begin{pmatrix} 1 & a_1 & c_1 2 \\ 0 & 1 & b_1 2 \\ 0 & 0 & 1 \end{pmatrix} t^{d_1} \begin{pmatrix} 1 & a_2 & c_2 2 \\ 0 & 1 & b_2 2 \\ 0 & 0 & 1 \end{pmatrix} t^{d_2} \\
&= f \left(\begin{pmatrix} 1 & a_1 & c_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix} t^{d_1} \right) f \left(\begin{pmatrix} 1 & a_2 & c_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix} t^{d_2} \right).
\end{aligned}$$

Offenbar ist f auch bijektiv. Wegen

$$\begin{aligned}
uw &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = wu \\
vw &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = wv
\end{aligned}$$

ist $w \in Z(H)$. Insbesondere ist $\langle w \rangle \trianglelefteq H$. Der Automorphismus f induziert nun einen Isomorphismus $H/\langle w \rangle \cong H/\langle w^2 \rangle$. Also ist $G = H/\langle w^2 \rangle$ eine endlich erzeugte Gruppe die nicht hopfsch ist. Da $H/Z(H)$ abelsch ist, ist H auflösbar. \square

Definition 13.17. Sei $w = w(x_1, \dots) \in W \subseteq F_X$. Für eine Gruppe G und $g_1, \dots \in G$ sei $w(g_1, \dots) \in G$ das Element, welches entsteht, indem man x_i in w durch g_i ersetzt (nur endlich viele x_i tauchen in w auf). Man nennt

$$W(G) := \langle w(g_1, \dots) : w \in W, g_1, \dots \in G \rangle$$

die *verbale Untergruppe* bzgl. W .

Beispiel 13.18. Für $W = \{[x, y]\}$ erhält man $W(G) = G'$.

Bemerkung 13.19. Für jeden Homomorphismus $f: G \rightarrow H$ gilt $f(W(G)) \leq W(H)$, d.h. verbale Untergruppen sind vollinvariant.

Satz 13.20 (NEUMANN). *Jede vollinvariante Untergruppe einer freien Gruppe ist verbal.*

Beweis. Sei $F = F_X$ und $H \leq F$ vollinvariant. Sei $w = w(x_1, \dots) \in H$ und $y_1, \dots \in F$ beliebig. Dann existiert ein Endomorphismus $\alpha: F \rightarrow F$ mit $\alpha(x_i) = y_i$. Es gilt $w(y_1, \dots) = \alpha(w) \in H$. Also ist $H = W(H)$ verbal. \square

Definition 13.21. Sei wieder $W \subseteq F = F_X$. Ein Normalteiler N einer Gruppe G heißt *W-marginal*, falls

$$w(g_1, \dots, g_i a, g_{i+1}, \dots) = w(g_1, \dots)$$

für alle $w \in W$, $g_1, \dots \in G$, $i \in \mathbb{N}$ und $a \in N$ gilt. Dies ist äquivalent zu

$$w(g_1, \dots) = w(h_1, \dots)$$

für alle $g_1, h_1, \dots \in G$ mit $g_i \equiv h_i \pmod{N}$ für $i \in \mathbb{N}$. Das Erzeugnis aller W -marginalen Normalteiler nennt man die *W-marginale Untergruppe* $W^*(G)$.

Bemerkung 13.22. Offenbar ist $W^*(G)$ selbst W -marginal. Für $W = \{[x, y]\}$ gilt $W^*(G) = Z(G)$, denn

$$g \in W^*(G) \Rightarrow \forall h \in G : [g, h] = [1g, h] = [1, h] = 1 \Rightarrow g \in Z(G) \Rightarrow g \in W^*(G).$$

Lemma 13.23. Es gilt $W(G) = 1$ genau dann, wenn $W^*(G) = G$.

Beweis. Aus $W(G) = 1$ folgt sicher $W^*(G) = G$. Sei nun $W^*(G) = G$ und $g_1, \dots \in G$. Aus $g_i \equiv 1 \pmod{G}$ folgt $w(g_1, \dots) = w(1, \dots) = 1$. Dies zeigt $W(G) = 1$. \square

Definition 13.24. Eine Gruppenklasse \mathcal{X} heißt *Varietät*, falls $W \subseteq F_X$ existiert mit $\mathcal{X} = \{G : W(G) = 1\}$. Ggf. schreibt man $\mathcal{X} = \mathcal{X}(W)$.

Beispiel 13.25. Die abelschen Gruppen bilden die Varietät $\mathcal{X}([x, y])$. Die elementarabelschen p -Gruppen bilden die Varietät $\mathcal{X}([x, y], x^p)$. Die Gruppen, deren Exponent n teilt, bilden die Varietät $\mathcal{X}(x^n)$ usw. Der nächste Satz impliziert, dass die auflösbaren Gruppen der Stufe $\leq n$ eine Varietät bilden.

Satz 13.26 (BIRKHOFF). Eine Gruppenklasse \mathcal{X} ist genau dann eine Varietät, falls \mathcal{X} abgeschlossen ist unter Bildung von Faktorgruppen und subdirekten Produkten.

Beweis. Jede Varietät ist abgeschlossen bzgl. Untergruppen, Faktorgruppen und (sub)direkten Produkten. Sei nun \mathcal{X} eine Gruppenklasse, die bzgl. Faktorgruppen und subdirekten Produkten abgeschlossen ist. Sei $W \subseteq F_X$ maximal mit $W(G) = 1$ für alle $G \in \mathcal{X}$. Dann ist $\mathcal{X} \subseteq \mathcal{X}(W)$. Sei umgekehrt $G \in \mathcal{X}(W)$. Für jedes $w \in F_X \setminus W$ wählen wir $H(w) \in \mathcal{X}$ mit $w(h_1, \dots) \neq 1$ für gewisse $h_1, \dots \in H(w)$. Sei Y eine Menge, die mindestens so groß wie G und alle $H(w)$ ist (zum Beispiel $Y = G \cup \bigcup_w H(w)$). Dann existieren Isomorphismen $F_Y/N \cong G$ und $F_Y/K(w) \cong H(w) \in \mathcal{X}$ mit $w(y_1, \dots) \notin K(w)$. Für jedes $w \in F_Y \setminus N$ existieren $g_1, \dots \in G$ mit $w(g_1, \dots) \neq 1$. Wegen $G \in \mathcal{X}(W)$ ist also $w \notin W$. Wir setzen

$$K := \bigcap_{w \in F_Y \setminus N} K(w) \trianglelefteq F_Y.$$

Dann ist F_Y/K ein subdirektes Produkt der \mathcal{X} -Gruppen $H(w)$. Nach Voraussetzung ist $F_Y/K \in \mathcal{X}$. Für $w \in F_Y \setminus N$ gilt $w \notin K(w)$, insbesondere $w \notin K$. Also ist $K \subseteq N$ und $G \cong F_Y/N \cong (F_Y/K)/(N/K)$ ist Faktorgruppe einer \mathcal{X} -Gruppe und damit $G \in \mathcal{X}$. Dies zeigt, dass $\mathcal{X} = \mathcal{X}(W)$ eine Varietät ist. \square

Folgerung 13.27. Ist eine Gruppenklasse abgeschlossen unter Bildung von Faktorgruppen und subdirekten Produkten, so auch unter Bildung von Untergruppen.

Definition 13.28. Sei \mathcal{X} eine Varietät. Eine Gruppe $F \in \mathcal{X}$ heißt \mathcal{X} -frei bzgl. $X \subseteq F$, falls für jede \mathcal{X} -Gruppe G und jede Abbildung $\sigma: X \rightarrow G$ genau ein Homomorphismus $\hat{\sigma}: F \rightarrow G$ mit $\hat{\sigma}(x) = \sigma(x)$ für alle $x \in X$ existiert.

Satz 13.29. Sei $F = F_X$ eine freie Gruppe und $\mathcal{X} = \mathcal{X}(W)$ eine Varietät mit $W \subseteq F$. Dann ist $\bar{F} := F/W(F)$ \mathcal{X} -frei bzgl. $\bar{X} := \{xW(F) : x \in X\}$ und jede \mathcal{X} -freie Gruppe bzgl. \bar{X} ist zu \bar{F} isomorph.

Beweis. Sei G eine \mathcal{X} -Gruppe und $\sigma: \bar{X} \rightarrow G$. Wir definieren $\tau: X \rightarrow G$ durch $\tau(x) := \sigma(xW(F))$ für $x \in X$. Dann existiert genau ein Homomorphismus $\hat{\tau}: F \rightarrow G$ mit $\hat{\tau}(x) = \tau(x)$ für $x \in X$. Wegen $G \in \mathcal{X}$ gilt $\hat{\tau}(w) = 1$ für alle $w \in W(F)$. Man erhält einen Homomorphismus $\hat{\sigma}: \bar{F} \rightarrow G$ mit $\hat{\sigma}(xW(F)) = \hat{\tau}(x) = \tau(x) = \sigma(xW(F))$ für $x \in X$. Wegen $\bar{F} = \langle \bar{X} \rangle$ ist $\hat{\sigma}$ durch die Bilder von \bar{X} eindeutig bestimmt.

Sei auch H \mathcal{X} -frei bzgl. \bar{X} . Dann lässt sich $\text{id}_{\bar{X}}$ zu Homomorphismen $\varphi: \bar{F} \rightarrow H$ und $\psi: H \rightarrow \bar{F}$ fortsetzen. Wie üblich folgt, dass φ ein Isomorphismus ist. \square

Bemerkung 13.30. Im Gegensatz zu freien Gruppen, gibt es nicht für jede Menge X eine \mathcal{X} -freie Gruppe bzgl. X . Für $\mathcal{X} = \mathcal{X}(x) = \{1\}$ ist beispielsweise jede \mathcal{X} -freie Gruppe trivial.

Satz 13.31. Sei \mathcal{X} eine Varietät. Dann ist jede \mathcal{X} -Gruppe zu einer Faktorgruppe einer \mathcal{X} -freien Gruppe isomorph.

Beweis. Sei $G \in \mathcal{X} = \mathcal{X}(W)$ mit minimalem Erzeugendensystem X . Sei $F := F_X$ und $\bar{X} := \{xW(F) : x \in X\}$ wie in Satz 13.29. Seien $x, y \in X$ mit $x \equiv y \pmod{W(F)}$. Dann ist $y^{-1}x \in W(F)$. Aus $W(G) = 1$ folgt $x = y$. Daher gilt $|\bar{X}| = |X|$ und es existiert eine Bijektion $\sigma: \bar{X} \rightarrow X \subseteq G$, die sich zu einem Epimorphismus $\bar{F} \rightarrow G$ fortsetzt. Die Behauptung folgt aus Satz 13.29. \square

Satz 13.32 (ENGEL). Seien $x_1, \dots, x_k \in X$ mit $x_{k-1} \neq x_k$. Dann ist jede endliche Gruppe $G \in \mathcal{X}([x_1, \dots, x_k])$ nilpotent.

Beweis. Sei G ein minimales Gegenbeispiel. Dann ist jede echte Untergruppe von G nilpotent. Nach Schmidt ist $G = P \rtimes Q$ mit $P \in \text{Syl}_p(G)$ und $Q \in \text{Syl}_q(G)$. Angenommen $\Phi(P) \neq 1$. Dann ist auch $G/\Phi(P)$ nilpotent. Wegen $\Phi(P) \leq \Phi(G)$ wären dann $G/\Phi(G)$ und G nilpotent. Also ist $\Phi(P) = 1$, d. h. P ist elementarabelsch. Für $x \in P$ und $y = y_1 = \dots = y_{k-1} \in Q \setminus \{1\}$ gilt $[y_1, \dots, y_{k-1}, x] = 1$ nach Voraussetzung. Da P abelsch ist, existiert $\alpha \in \text{End}(P)$ mit $\alpha(g) = [y, g]$ für $g \in P$. Induktiv erhält man $\alpha^{k-1}(x) = [y_1, \dots, y_{k-1}, x] = 1$. Ist $\beta \in \text{Aut}(P)$ die Konjugation mit y , so gilt $\alpha = \beta - 1 \in \text{End}(P)$. Sei $m \in \mathbb{N}$ mit $p^m \geq k$. Da P elementarabelsch ist, folgt

$$0 = \alpha^{p^m} = \sum_{i=1}^{p^m} \binom{p^m}{i} (-1)^i \beta^{p^m-i} = \beta^{p^m} - 1$$

(für $p = 2$ ist $-1 = 1$). Also gilt $y^{p^m} \in C_G(P)$ und $y \in C_G(P)$ wegen $p \neq q$. Dann wäre aber G nilpotent. \square

Folgerung 13.33 (ZORN). Sei G eine endliche Gruppe und $k \in \mathbb{N}$ mit $\underbrace{[g, \dots, g, h]}_k = 1$ für alle $g, h \in G$, so ist G nilpotent.

Bemerkung 13.34. Ist sogar $[g_1, \dots, g_k] = 1$ für alle $g_1, \dots, g_k \in G$, so ist G nilpotent mit Nilpotenzklasse $\leq k$. Siehe auch Lemma 12.7.

14 p -Gruppen

Definition 14.1. Sei $X = \{x_1, \dots\}$ und $\mathcal{X} = \mathcal{X}(x^{p^2}, [x, y]^p, [x, y, z] : x, y, z \in F_X)$. Sei G_r die \mathcal{X} -freie Gruppe vom Rang $r \geq 1$ aus Satz 13.29. Wie üblich identifizieren wir x_i mit der entsprechenden Nebenklasse in G_r .

Lemma 14.2. Die Varietät \mathcal{X} besteht aus allen p -Gruppen G mit $\Phi(G) \leq Z(G)$ und $\Phi(\Phi(G)) = 1$.

Beweis. Sei G eine p -Gruppe mit $\Phi(G) \leq Z(G)$ und $\Phi(\Phi(G)) = 1$. Für $x, y, z \in G$ gilt $x^p \in \Phi(G)$ und $x^{p^2} = 1$. Außerdem ist $[x, y] \in G' \leq \Phi(G)$ und $[x, y]^p = 1$ folgt. Schließlich ist $[y, z] \in \Phi(G) \leq Z(G)$ und daher $[x, y, z] = [x, [y, z]] = 1$.

Sei umgekehrt $G \in \mathcal{X}$ und $N := \langle x^p, [x, y] : x, y \in G \rangle$. Dann ist G/N elementarabelsch (möglicherweise unendlich) und $\Phi(G) \leq N$. Wegen $[x^p, y] = [x, y]^p = 1$ und $[x, y, z] = 1$ ist $N \leq Z(G)$ und N ist elementarabelsch, d. h. $\Phi(\Phi(G)) \leq \Phi(N) = 1$. \square

Lemma 14.3. Sei $G \in \mathcal{X}$ und $y_1, \dots, y_r \in G$. Dann existiert ein Homomorphismus $\varphi : G_r \rightarrow G$ mit $\varphi(x_i) = y_i$ für $i = 1, \dots, r$.

Beweis. Folgt aus Satz 13.31 oder Satz 1.15 (da y_1, \dots, y_r nicht unbedingt ein Erzeugendensystem von G ist, erhält man nur einen Homomorphismus anstelle eines Epimorphismus). \square

Lemma 14.4. Es gilt:

- (i) $\Phi(G_r)$ ist elementarabelsch vom Rang $r(r+1)/2$.
- (ii) $G_r/\Phi(G_r)$ ist elementarabelsch vom Rang r .
- (iii) Operiert $\alpha \in \text{Aut}(G_r)$ trivial auf $G_r/\Phi(G_r)$, so auch auf $\Phi(G_r)$.

Beweis.

- (i) Wegen $[x_i, x_j x_k] = [x_i, x_j] \cdot {}^{x_j}[x_i, x_k] = [x_i, x_j][x_i, x_k]$ für $1 \leq i, j, k \leq r$ ist $G'_r = \langle [x_i, x_j] : 1 \leq i < j \leq r \rangle$ elementarabelsch vom Rang höchstens $r(r-1)/2$. Wegen $(x_i x_j)^p \equiv x_i^p x_j^p \pmod{G'_r}$ ist $G_r^p G'_r = \langle x_i^p, [x_i, x_j] \rangle$ elementarabelsch vom Rang höchstens $r(r-1)/2 + r = r(r+1)/2$. Da auch $G/G_r^p G'_r$ elementarabelsch vom Rang höchstens r ist, ist G eine endliche p -Gruppe und $\Phi(G_r) = G_r^p G'_r \leq Z(G_r)$.

Angenommen es gibt eine Relation der Form

$$g := \prod_{i=1}^r x_i^{p a_i} \prod_{1 \leq i < j \leq r} [x_i, x_j]^{b_{ij}} = 1$$

mit $0 \leq a_i, b_{ij} \leq p-1$. Für $\langle h \rangle \cong C_{p^2}$ und $1 \leq i \leq r$ existiert nach Lemma 14.3 ein Homomorphismus $\varphi : G_r \rightarrow \langle h \rangle$ mit $\varphi(x_i) = h$ und $\varphi(x_j) = 1$ für $j \neq i$. Es folgt $1 = \varphi(g) = h^{p a_i}$ und $a_i = 0$ für $i = 1, \dots, r$. Für $1 \leq i < j \leq r$ sei analog $\langle h_i, h_j \rangle \cong p_+^{1+2}$. Wieder existiert ein Homomorphismus $\varphi : G_r \rightarrow \langle h_i, h_j \rangle$ mit $\varphi(x_i) = h_i$, $\varphi(x_j) = h_j$ und $\varphi(x_k) = 1$ für $i \neq k \neq j$. Aus $1 = \varphi(g) = [h_i, h_j]^{b_{ij}}$ folgt $b_{ij} = 0$. Dies zeigt, dass $\Phi(G_r)$ Rang $r(r+1)/2$ hat.

- (ii) Seien $0 \leq a_1, \dots, a_r \leq p-1$ mit $g = x_1^{a_1} \dots x_r^{a_r} \in \Phi(G_r)$. Wie in (i) existiert ein Homomorphismus $\varphi : G_r \rightarrow \langle h \rangle \cong C_{p^2}$ mit $h^{a_i} = \varphi(g) \in \Phi(\langle h \rangle) = \langle h^p \rangle$. Dies zeigt $g = 1$ und die Behauptung folgt.

- (iii) Sei $\alpha \in \text{Aut}(G_r)$ trivial auf $G_r/\Phi(G_r)$. Dann existieren $h_1, \dots, h_r \in \Phi(G_r)$ mit $\alpha(x_i) = x_i h_i$ für $i = 1, \dots, r$. Wegen (i) ist $\alpha(x_i^p) = \alpha(x_i)^p = (x_i h_i)^p = x_i^p$ und $\alpha([x_i, x_j]) = [x_i h_i, x_j h_j] = [x_i, x_j]$ für $1 \leq i < j \leq r$. \square

Lemma 14.5. *Seien $N, M \leq \Phi(G_r)$. Genau dann gilt $G_r/N \cong G_r/M$, falls ein $\alpha \in \text{Aut}(G_r)$ mit $\alpha(N) = M$ existiert.*

Beweis. Jedes $\alpha \in \text{Aut}(G_r)$ mit $\alpha(N) = M$ induziert einen Isomorphismus $G_r/N \cong G_r/M$. Sei umgekehrt ein Isomorphismus $\alpha': G_r/N \rightarrow G_r/M$ gegeben. Wähle $y_1, \dots, y_r \in G_r$ mit $\alpha'(x_i N) = y_i M$ für $i = 1, \dots, r$. Nach Lemma 14.3 und Lemma 14.4 existiert ein Homomorphismus $\alpha: G_r \rightarrow G_r$ mit $\alpha(x_i) = y_i$ für $i = 1, \dots, r$. Bekanntlich gilt

$$G_r = \langle y_1, \dots, y_r \rangle M = \langle y_1, \dots, y_r \rangle \Phi(G_r) = \langle y_1, \dots, y_r \rangle.$$

Daher ist α surjektiv und ein Isomorphismus. Wegen $\alpha(x_i)M = y_i M = \alpha'(x_i N)$ gilt $\alpha(g)M = \alpha'(gN)$ für alle $g \in G_r$. Dabei ist

$$g \in N \iff \alpha'(gN) = 1 \iff \alpha(g)M = 1 \iff \alpha(g) \in M.$$

Dies zeigt $\alpha(N) = M$. \square

Lemma 14.6. *Die Anzahl der d -dimensionalen Unterräume von \mathbb{F}_p^n ist*

$$\binom{n}{d}_p = \frac{(p^n - 1)(p^n - p) \dots (p^n - p^{d-1})}{(p^d - 1)(p^d - p) \dots (p^d - p^{d-1})}$$

und es gilt $p^{d(n-d)} \leq \binom{n}{d}_p \leq p^{d(n-d+1)}$.

Beweis. Die Formel ist aus Kombinatorik bekannt. Die untere Abschätzung folgt aus $p^{n-d} \leq \frac{p^n - p^i}{p^d - p^i}$ für $0 \leq i \leq d-1$. Andererseits ist $p^n + p^{n-d+i+1} \leq 2p^n \leq p^{n+1} + p^i$ und dies liefert $\frac{p^n - p^i}{p^d - p^i} \leq p^{n-d+1}$. \square

Lemma 14.7. *Sei $r, s \in \mathbb{N}$ mit $1 \leq s \leq r(r+1)/2$. Dann existieren mindestens $p^{rs(r+1)/2 - r^2 - s^2}$ nicht-isomorphe Gruppen der Ordnung p^{r+s} .*

Beweis. Sei \mathcal{N} die Menge der Normalteiler $N \leq \Phi(G_r)$ mit $|\Phi(G_r) : N| = p^s$. Nach Lemma 14.4 und Lemma 14.6 gilt $|\mathcal{N}| \geq p^{rs(r+1)/2 - s^2}$. Für $N \in \mathcal{N}$ gilt $|G_r/N| = p^{r+s}$. Nach Lemma 14.5 genügt es die Anzahl der Bahnen von $\text{Aut}(G_r)$ auf \mathcal{N} abzuschätzen. Sei $\Gamma: \text{Aut}(G_r) \rightarrow \text{Aut}(G_r/\Phi(G_r))$ der kanonische Homomorphismus. Nach Lemma 14.4 operieren die Automorphismen in $\text{Ker}(\Gamma)$ trivial auf \mathcal{N} . Andererseits ist

$$|\text{Aut}(G_r/\Phi(G_r))| = |\text{GL}(r, p)| = (p^r - 1)(p^{r-1} - 1) \dots (p - 1) \leq p^{r^2}.$$

Jede Bahn von $\text{Aut}(G_r)$ auf \mathcal{N} hat also höchstens Länge p^{r^2} . Die Anzahl der Bahnen ist somit mindestens $p^{rs(r+1)/2 - r^2 - s^2}$. \square

Satz 14.8 (HIGMAN). *Sei $f(p^n)$ die Anzahl der nicht-isomorphen Gruppen der Ordnung p^n für eine Primzahl p . Dann gilt*

$$p^{\frac{2}{27}n^2(n-6)} \leq f(p^n) \leq p^{\frac{1}{6}(n^3-n)}.$$

Beweis. Für die untere Abschätzung können wir $n \geq 6$ annehmen. Sei

$$s := \begin{cases} n/3 & \text{falls } n \equiv 0 \pmod{3}, \\ (n+2)/3 & \text{falls } n \equiv 1 \pmod{3}, \\ (n+1)/3 & \text{falls } n \equiv 2 \pmod{3} \end{cases}$$

und $r = n - s$. Dann ist $s \leq r \leq r(r+1)/2$ und

$$\begin{aligned} rs(r+1)/2 - r^2 - s^2 &= \begin{cases} \frac{1}{27}n^2(2n+3) - \frac{4}{9}n^2 - \frac{1}{9}n^2 & \text{falls } n \equiv 0 \pmod{3} \\ \frac{1}{27}(n+2)(n-1)(2n+1) - \frac{4}{9}(n-1)^2 - \frac{1}{9}(n+2)^2 & \text{falls } n \equiv 1 \pmod{3} \\ \frac{1}{27}(n+1)(2n-1)(n+1) - \frac{1}{9}(2n-1)^2 - \frac{1}{9}(n+1)^2 & \text{falls } n \equiv 2 \pmod{3} \end{cases} \\ &= \begin{cases} \frac{2}{27}n^2(n-6) & \text{falls } n \equiv 0 \pmod{3} \\ \frac{2}{27}n^2(n-6) + \frac{1}{3}n - \frac{26}{27} & \text{falls } n \equiv 1 \pmod{3} \\ \frac{2}{27}n^2(n-6) + \frac{2}{9}n - \frac{7}{27} & \text{falls } n \equiv 2 \pmod{3} \end{cases} \\ &\geq \frac{2}{27}n^2(n-6). \end{aligned}$$

Nach Lemma 14.7 ist daher $f(p^n) \geq p^{\frac{2}{27}n^2(n-6)}$.

Für die obere Abschätzung sei G eine Gruppe der Ordnung p^n mit Hauptreihe $G = H_0 > H_1 > \dots > H_n = 1$. Wir wählen $g_i \in H_{i-1} \setminus H_i$ für $i = 1, \dots, n$. Jedes Element in G lässt sich dann eindeutig in der Form $g = g_1^{a_1} \dots g_n^{a_n}$ mit $0 \leq a_1, \dots, a_n \leq p-1$ schreiben. Dabei gilt $g \in H_i$ genau dann, wenn $a_1 = \dots = a_i = 0$. Seien $0 \leq b_{ij} \leq p-1$ mit

$$g_i^p = g_{i+1}^{b_{i,i+1}} \dots g_n^{b_{i,n}}. \quad (14.1)$$

Wegen $H_{j-1}/H_j \leq Z(G/H_j)$ gilt $[g_i, g_j] \in H_j$ für $1 \leq i < j \leq n$. Daher existieren $0 \leq c_{ij} \leq p-1$ mit

$$[g_i, g_j] = g_{j+1}^{c_{i,j+1}} \dots g_n^{c_{i,n}} \quad (i < j). \quad (14.2)$$

Wir zeigen nun, dass G durch die Relationen (14.1) und (14.2) eindeutig bestimmt ist. Dafür muss man ein Produkt $g_1^{a_1} \dots g_n^{a_n} g_1^{a'_1} \dots g_n^{a'_n}$ auf die Form $g_1^{a''_1} \dots g_n^{a''_n}$ bringen. Dies ist klar für $n = 1$. Sei $n \geq 2$. Mit (14.2) kann man $g_1^{a'_1}$ nach links schieben, indem man Terme der Form $g_j^{c_{1,j}}$ mit $j \geq 2$ einfügt. Anschließend erhält man $g_1^{a_1+a'_1} h$ mit $h \in H_1$. Mit (14.1) kann man $a_1 + a'_1$ durch a''_1 ersetzen, indem man weitere Terme der Form $g_i^{b_{ij}}$ mit $i \geq 2$ einfügt. Die Behauptung folgt nun durch Induktion. Die Anzahl der nicht-isomorphen Gruppen der Ordnung p^n ist also durch die Wahl der Parameter b_{ij} und c_{ij} beschränkt. Für die Wahl der b_{ij} gibt es $p^{n(n-1)/2}$ Möglichkeiten. Für die Wahl der c_{ij} gibt es p^α Möglichkeiten, wobei

$$\alpha = \sum_{i=1}^{n-2} \binom{n-i}{2} = \binom{n}{3} = \frac{n^3 - 3n^2 + 2n}{6}.$$

(Man zähle die Anzahl der 3-elementigen Teilmengen von $\{1, \dots, n\}$ mit vorgegebenem Maximum.) Insgesamt ergeben sich höchstens $p^{(n^3-n)/6}$ Gruppen der Ordnung p^n . \square

Bemerkung 14.9. Sims-Newman-Seeley haben die stärkere Abschätzung $f(p^n) \leq p^{\frac{2}{27}n^3 + O(n^{5/2})}$ bewiesen. Da wir zum Beweis der unteren Abschätzung nur Faktorgruppen von G_r benutzt haben, folgt: Fast alle p -Gruppen G besitzen einen Normalteiler $N \leq Z(G)$, sodass N und G/N elementarabelsch sind. Insbesondere haben fast alle p -Gruppen Nilpotenzklasse 2.

Definition 14.10. Für endliche Mengen $A, B \subseteq \mathbb{N}$ sei $A \prec B$, falls $|A| < |B|$ oder falls $|A| = |B|$ und A lexikographisch kleiner als B ist (d. h. $\min(A \cup B) \setminus (A \cap B) \in A$).

Bemerkung 14.11. Offenbar ist \prec eine Totalordnung auf der Menge der endlichen Teilmengen von \mathbb{N} . Aus $A \subseteq B$ folgt $A \prec B$.

Lemma 14.12 (HALLS Kollektor-Prozess). Sei $X = \{x_1, \dots, x_n\} = X_1 \dot{\cup} \dots \dot{\cup} X_m$ und $F := F_X$. Für $I \subseteq \{1, \dots, m\}$ sei

$$C_I := F^{[I]} \cap \bigcap_{i \in I} \langle X_i \rangle^F \cap \langle \bigcup_{i \in I} X_i \rangle \leq F.$$

Dann existieren $c_I \in C_I$ mit

$$x_1 \dots x_n = \prod_{I \subseteq \{1, \dots, m\}} c_I,$$

wobei die Teilmengen I gemäß \prec durchlaufen werden.

Beweis. Für $J \subseteq \{1, \dots, m\}$ zeigen wir

$$x_1 \dots x_n = \prod_{I \prec J} c_I \cdot y_1 \dots y_n$$

mit $y_1, \dots, y_n \in C_K$ für ein $J \preceq K$. Die Behauptung folgt dann mit $J = \{1, \dots, m\}$, indem man $c_J = y_1 \dots y_n$ setzt. Für $J = \emptyset$ ist das Produkt über $I \prec J$ leer. Für $x_i \in X_j \leq \langle X_i \rangle = C_{\{j\}}$ kann man $y_i = x_i$ wählen. Sei nun die Behauptung für J bereits bewiesen und sei J' der Nachfolger von J bzgl. \prec . Wir können annehmen, dass mindestens ein y_i in C_J liegt, denn anderenfalls ist $y_i \in C_K$ mit $J' \preceq K$ für alle i . Sei dabei i minimal. Im Fall $i > 1$ schreiben wir $y_{i-1}y_i = y_i y_{i-1} z$ mit $z := [y_{i-1}^{-1}, y_i^{-1}]$ und $y_{i-1} \in C_K \subseteq F^{[K]}$, wobei $J \prec K$. Dann gilt

- $z \in [F^{[K]}, F^{[J]}] \leq F^{[K|+|J|]} \leq F^{[J \cap K]}$.
- $z \in \langle X_j \rangle^F$ für alle $j \in J \cup K$.
- $z \in \langle \bigcup_{j \in J \cup K} X_j \rangle$.

Dies zeigt $z \in C_{J \cup K}$ mit $J \prec J \cup K$. Mit endlich vielen Schritten können wir auf diese Weise alle $y_i \in C_J$ nach links schieben. Das Produkt dieser y_i nennen wir c_J . Für die verbleibenden Faktoren gilt nun $y_j \in C_K$ mit $J' \preceq K$ wie gewünscht. \square

Satz 14.13 (HALL-PETRESCU-Formel). Für jede Gruppe G und $x, y \in G$ existieren eindeutig bestimmte Elemente $c_i \in G^{[i]}$, sodass für alle $n \in \mathbb{N}$ gilt

$$x^n y^n = (xy)^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \dots c_n^{\binom{n}{n}}.$$

Beweis. O. B. d. A. sei $G := \langle x, y \rangle$. Die Eindeutigkeit der c_i folgt induktiv:

$$c_2 = (xy)^{-2} x^2 y^2, \quad c_n = c_{n-1}^{-\binom{n}{n-1}} \dots c_2^{-\binom{n}{2}} (xy)^{-n} x^n y^n.$$

Sei $N \in \mathbb{N}$ beliebig. Wir zeigen, dass die Formel für alle $n \leq N$ gilt. Wegen der Eindeutigkeit gilt sie dann für alle $n \in \mathbb{N}$. Sei $X_i := \{x_i, x_{i+N}\}$ und $X = X_1 \dot{\cup} \dots \dot{\cup} X_N = \{x_1, \dots, x_{2N}\}$. Sei $F := F_X$. Für $I \subseteq \{1, \dots, N\}$ sei $\mu_I: F \rightarrow F$ der Endomorphismus mit

$$\mu_I(x_i) = \begin{cases} x_i & \text{falls } i \in I \vee i - n \in I, \\ 1 & \text{sonst.} \end{cases}$$

Sei $x_1 \dots x_{2N} = \prod c_I$ wie in Lemma 14.12. Für $I \subseteq J$ gilt $\mu_J(c_I) = c_I$, denn $C_I \subseteq \langle \bigcup_{i \in I} X_i \rangle$. Für $I \not\subseteq J$ gilt hingegen $\mu_J(c_I) = 1$, denn für $i \in I \setminus J$ ist $C_I \subseteq \langle X_i \rangle^F = \langle x_i, x_{i+N} \rangle^F \subseteq \text{Ker}(\mu_J)$. Nach Lemma 14.12 gilt also

$$\prod_{j \in J} x_j \prod_{j \in J} x_{j+N} = \mu_J(x_1 \dots x_{2N}) = \prod_{I \subseteq J} c_I,$$

wobei die Mengen I bzgl. \prec angeordnet sind.

Sei $\varphi: F \rightarrow G$ ein Homomorphismus mit $\varphi(x_i) = x$ und $\varphi(x_{i+N}) = y$ für $i = 1, \dots, N$. Für $|J| = n$ erhalten wir

$$x^n y^n = \varphi(\mu_J(x_1 \dots x_{2N})) = \prod_{I \subseteq J} \varphi(c_I).$$

Wir behaupten, dass $\varphi(c_I)$ nur von $|I|$ abhängt. Dies ist klar für $n = 0$ mit $c_\emptyset = 1$. Für $n = 1$ erhält man $\varphi(c_I) = xy$ für alle einelementigen Mengen I . Sei nun $n := |J| = |J'|$ und

$$\left(\prod_{I \subseteq J} \varphi(c_I) \right) \varphi(c_J) = \prod_{I \subseteq J} \varphi(c_I) = x^n y^n = \prod_{I' \subseteq J'} \varphi(c_{I'}) = \left(\prod_{I' \subseteq J'} \varphi(c_{I'}) \right) \varphi(c_{J'}).$$

Auf beiden Seiten sind die I der Größe nach aufsteigend sortiert. Für $l := |I| = |I'| < n$ gilt bereits $\varphi(c_I) = \varphi(c_{I'})$ nach Induktion. Die Anzahl dieser Faktoren ist auf beiden Seiten $\binom{n}{l}$. Daher ist $\varphi(c_J) = \varphi(c_{J'})$.

Wir setzen $c_l := \varphi(c_{\{1, \dots, l\}})$ für $l = 1, \dots, N$. Dann gilt $c_l \in \varphi(F^{[l]}) \subseteq G^{[l]}$ und

$$x^n y^n = \prod_{l=1}^n c_l^{\binom{n}{l}} = c_1^n \prod_{l=2}^n c_l^{\binom{n}{l}} = (xy)^n \prod_{l=1}^n c_l^{\binom{n}{l}}. \quad \square$$

Beispiel 14.14. Es gilt $c_2 = (xy)^{-2} x^2 y^2 = y^{-1} x^{-1} y^{-1} x y^2 = [y^{-1} x^{-1}, y^{-1}]$. Im Fall $\langle x, y \rangle^{[3]} = 1$ erhält man die aus GT-Aufgabe 16 bekannte Formel $(xy)^n = x^n y^n [y, x]^{\binom{n}{2}}$.

Lemma 14.15. Sei p eine Primzahl und G nilpotent mit Klasse $k < p$. Für alle $x, y \in G$ und $q = p^n$ gilt:

- (i) Es existiert ein $z \in G'$ mit $x^q y^q = (xy)^q z^q$.
- (ii) $x^q = y^q \iff (xy^{-1})^q = 1$.
- (iii) $\Omega_q(G) := \{x \in G : x^q = 1\} \trianglelefteq G$.
- (iv) $\mathcal{U}_q(G) := \{x^q : x \in G\} \trianglelefteq G$.
- (v) $|G| = |\Omega_q(G)| |\mathcal{U}_q(G)|$.
- (vi) $\mathcal{U}_q(G)' \in \mathcal{U}_{q^2}(G')$.

Beweis. Induktion nach k : Im Fall $k \leq 1$ ist G abelsch und alle Aussagen folgen leicht. Sei $k \geq 2$ und o. B. d. A. $G = \langle x, y \rangle$.

- (i) Nach Voraussetzung gilt $G^{[p]} \leq G^{[k+1]} = 1$. Nach der Hall-Petrescu-Formel existieren $c_i \in G^{[i]} \leq G'$ mit

$$x^q y^q = (xy)^q c_2^{\binom{q}{2}} \dots c_{p-1}^{\binom{q}{p-1}}.$$

Man sieht leicht, dass $\binom{q}{i}$ für $0 < i < p$ durch q teilbar. Nach Induktion gilt (iv) für G' . Dies zeigt $c_2^{\binom{q}{2}} \dots c_{p-1}^{\binom{q}{p-1}} \in \mathcal{U}_q(G')$.

(ii) Sei $x^q = y^q$. Dann gilt

$$x^q = yx^qy^{-1} = (yxy^{-1})^q.$$

Sei $H := \langle x, yxy^{-1} \rangle \leq G$. Wegen

$$[x, yxy^{-1}] = [x, yxy^{-1}x^{-1}] = [x, y, x] \in G^{[3]}$$

gilt $H' = \langle [x, yxy^{-1}] \rangle^H \leq G^{[3]}$. Daher hat H Nilpotenzklasse $< k$. Nach Induktion gilt $[x, y]^q = (x(yxy^{-1})^{-1})^q = 1$. Da auch G' Nilpotenzklasse $< k$ hat, gilt

$$G' = \langle [x, y] \rangle^G = \langle g[x, y]g^{-1} : g \in G \rangle \leq \Omega_q(G') = G',$$

d. h. $\exp(G') \leq q$. Aus (i) folgt $(xy^{-1})^q = x^qy^{-q} = 1$.

Sei umgekehrt $(xy^{-1})^q = 1$. Dann ist auch $(y^{-1}x)^q = x^{-1}(xy^{-1})^qx = 1$. Nach dem ersten Teil der Äquivalenz ergibt sich $[x, y^{-1}]^q = (xy^{-1}x^{-1}y)^q = 1$. Wie zuvor erhält man $\exp(G') \leq q$. Nach (i) ist $x^qy^{-q} = (xy^{-1})^q = 1$ und $x^q = y^q$.

- (iii) Für $x, y \in \Omega_q(G)$ gilt $x^q = 1 = y^q$ und $(xy^{-1})^q = 1$ nach (ii). Dies zeigt $xy^{-1} \in \Omega_q(G)$ und $\Omega_q(G) \leq G$. Offensichtlich ist $\Omega_q(G)$ ein Normalteiler von G .
- (iv) Für $x^q, y^q \in \mathcal{U}_q(G)$ existiert nach (i) ein $z \in G'$ mit $x^qy^{-q} = (xy^{-1})^qz^q$. Für $H := \langle xy^{-1}, z \rangle$ gilt $[xy^{-1}, z] \in G^{[3]}$ und $H' = \langle [xy^{-1}, z] \rangle^H \leq G^{[3]}$. Insbesondere hat H Nilpotenzklasse $< k$. Nach Induktion gilt $(xy^{-1})^qz^q \in \mathcal{U}_q(H) \leq \mathcal{U}_q(G)$ und $\mathcal{U}_q(G) \leq G$. Offensichtlich ist $\mathcal{U}_q(G)$ normal in G .
- (v) Die Abbildung $f : G \rightarrow \mathcal{U}_q(G)$, $x \mapsto x^q$ ist surjektiv (aber im Allgemeinen kein Homomorphismus). Nach (ii) gilt $f(x) = f(y)$ genau dann, wenn $xy^{-1} \in \Omega_q(G)$. Daher ist $f^{-1}(x^q) = x\Omega_q(G)$ und $|f^{-1}(x)| = |\Omega_q(G)|$ für alle $x \in G$. Ist $\Omega_q(G)$ unendlich, so auch G . Anderenfalls ist $|G : \Omega_q(G)| = |\mathcal{U}_q(G)|$.
- (vi) Seien $x^q, y^q \in \mathcal{U}_q(G)$. Wir wenden (ii) auf $\overline{G'} := G'/\mathcal{U}_{q^2}(G')$ an:

$$[x^q, y^q] = x^q(y^qxy^{-q})^{-q} \in \mathcal{U}_{q^2}(G') \iff (xy^qx^{-1}y^{-q})^q \in \mathcal{U}_{q^2}(G') \iff xy^qx^{-1}y^{-q} \in \Omega_q(\overline{G'}).$$

Nun wenden wir (ii) auf $\overline{G'}/\Omega_q(\overline{G'})$ an:

$$xy^qx^{-1}y^{-q} = (xyx^{-1})^qy^{-q} \in \Omega_q(\overline{G'}) \iff [x, y]^q \in \Omega_q(\overline{G'}) \iff [x, y]^{q^2} \in \mathcal{U}_{q^2}(G').$$

Die Aussage auf der rechten Seite ist offensichtlich wahr. □

Beispiel 14.16. Die Aussagen in Lemma 14.15 gelten in Allgemeinen nicht für Gruppen mit Nilpotenzklasse $\geq p$. Zum Beispiel kann $\Omega_2(D_8)$ wegen $|\Omega_2(D_8)| = 6$ keine Untergruppe von D_8 sein. Für

$$G := \langle x, y \mid x^4 = y^4 = 1, yxy^{-1} = x^{-1} \rangle \cong C_4 \rtimes C_4.$$

ist $\mathcal{U}_2(G) = \{1, x^2, y^2\}$ keine Untergruppe von G .

Bemerkung 14.17. p -Gruppen, die Lemma 14.15(i) (und damit auch alle anderen Aussagen) erfüllen, nennt man *regulär*. Nach Aufgabe 40 ist die Nilpotenzklasse einer regulären p -Gruppen nicht durch p beschränkt. Der nächste Satz zeigt, dass sich p -Gruppen mit „kleiner“ Nilpotenzklasse annähernd wie abelsche Gruppen verhalten.

Satz 14.18 (GROVES). *Sei P eine p -Gruppe mit Nilpotenzklasse $< p$. Dann existiert eine Verknüpfung $P \times P \rightarrow P$, $(x, y) \mapsto x + y$ mit folgenden Eigenschaften:*

- (i) $P_+ := (P, +)$ ist eine abelsche Gruppe.
- (ii) Die Ordnungen von x in P und P_+ sind gleich.
- (iii) Für alle $x, y \in P$ gilt $x + y \in \langle x, y \rangle$.
- (iv) Jeder Automorphismus von P ist auch ein Automorphismus von P_+ .
- (v) Jede Untergruppe von P ist auch eine Untergruppe von P_+ .

Beweis. Sei $P = \langle x_1, \dots, x_n \rangle$ und $F := F_n/F_n^{[p]}$ die freie nilpotente Gruppe mit Rang n und Nilpotenzklasse $p - 1$. Dann existiert ein Epimorphismus $f: F \rightarrow P$, $x \mapsto \bar{x}$. Sei $q = \exp(P')$. Für alle $x, y \in F$ existiert nach Lemma 14.15 (angewendet auf $\langle x, y \rangle$) ein $s = s(x, y) \in \langle x, y \rangle$ mit $x^q y^q = s^q$. Sei auch $t \in F$ mit $s^q = t^q$. Dann folgt $(st^{-1})^q = 1$ aus Lemma 14.15. Da F torsionsfrei ist (Folgerung 12.34), folgt $s = t$, d. h. s ist durch x, y eindeutig bestimmt. Wir definieren $\bar{x} + \bar{y} := \bar{s}$.

- (i) Für $x, y, z \in F$ gilt

$$s(s(x, y), z)^q = s(x, y)^q z^q = (x^q y^q) z^q = x^q (y^q z^q) = x^q s(y, z)^q = s(x, s(y, z))^q.$$

Wie oben folgt $s(s(x, y), z) = s(x, s(y, z))$. Dies zeigt, dass $+$ auf P assoziativ ist. Wegen $s(x, 1) = 1 = s(1, x)$ ist $\bar{1}$ neutral bzgl. $+$. Wegen $s(x, x^{-1}) = 1$ ist \bar{x}^{-1} invers zu \bar{x} bzgl. $+$.

Nach Lemma 14.15 ist $s(x, y)^q s(y, s)^{-q} = [x^q, y^q] \in \mathcal{U}_{q^2}(F')$ und $(s(x, y)s(y, x)^{-1})^q \in \mathcal{U}_{q^2}(F')$. Sei $z \in F'$ mit $(s(x, y)s(y, x)^{-1})^q = z^{q^2} = (z^q)^q$. Aus Lemma 14.15 folgt $(s(x, y)s(y, x)^{-1}z^{-q})^q = 1$. Da F torsionsfrei ist, erhält man $s(x, y)s(y, x)^{-1} = z^p \in \mathcal{U}_q(F')$. Wegen $\mathcal{U}_q(P') = 1$ folgt

$$\bar{x} + \bar{y} = \overline{s(x, y)} = \overline{s(y, s)} = \bar{y} + \bar{x}$$

für alle $x, y \in P$, d. h. P_+ ist eine abelsche Gruppe.

- (ii) Offenbar ist $\bar{x} + \bar{x} = \overline{s(x, x)} = \overline{x^2}$ und induktiv $k \cdot \bar{x} = \overline{x^k}$ für alle $k \in \mathbb{N}$.
- (iii) Folgt aus $s(x, y) \in \langle x, y \rangle$.
- (iv) Sei $\alpha \in \text{Aut}(P)$. Nach (iii) ist $\bar{x} + \bar{y}$ ein Wort in \bar{x} und \bar{y} . Daher ist $\alpha(\bar{x} + \bar{y})$ das entsprechende Wort in $\alpha(\bar{x})$ und $\alpha(\bar{y})$. Dies zeigt $\alpha(\bar{x} + \bar{y}) = \alpha(\bar{x}) + \alpha(\bar{y})$.
- (v) Sei $Q \leq P$, $H := f^{-1}(Q) \leq F$ und $\bar{x}, \bar{y} \in Q$. Dann gilt $s(x, y^{-1}) \in \langle x, y^{-1} \rangle \leq H$ und $\bar{x} - \bar{y} \in Q$. Dies zeigt $Q \leq P_+$. \square

Bemerkung 14.19.

- (i) Der Isomorphietyp von P_+ lässt sich leicht aus $|\Omega_q(P)| = |\Omega_q(P_+)|$ für $q = p, p^2, \dots$ bestimmen.
- (ii) Sei $p > 2$ und P eine p -Gruppe mit Nilpotenzklasse 2. Sei $q := \exp(P')$. In der freien Gruppe mit Nilpotenzklasse 2 gilt

$$x^q y^q = (xy)^q [y, x]^{-\binom{q}{2}} = (xy[y, x]^{\frac{1-q}{2}})^q.$$

nach Beispiel 14.14. Da die Abbildung $P \rightarrow P$, $x \mapsto x^2$ bijektiv ist, besitzt jedes $x \in P$ genau eine „Wurzel“ $\sqrt{x} \in P$ mit $\sqrt{x}^2 = x$. Wie im Beweis von Satz 14.18 erhält man durch

$$x + y := xy[y, x]^{\frac{1-q}{2}} = xy\sqrt{[y, x]}$$

eine abelsche Gruppenstruktur auf P . Dieser Spezialfall wurde zuerst von Baer konstruiert.

- (iii) Für p -Gruppen mit Nilpotenzklasse $3 < p$ lautet die Formel

$$x + y := xy \sqrt{[y^{-1}, x^{-1}]}^{12} \sqrt{[x, y, x]}^{12} \sqrt{[y, x, y]}^{12}$$

(ohne Beweis). Im Allgemeinen erhält man diese Terme aus der *Baker-Campbell-Hausdorff-Formel*.

- (iv) Satz 14.18 gilt bereits, wenn jede von drei Elementen erzeugte Untergruppe von G Nilpotenzklasse $< p$ hat (drei Erzeuger sind notwendig, um das Assoziativgesetz zu beweisen).
- (v) Die *Lazard-Korrespondenz* liefert eine Lie-Ring-Struktur auf p -Gruppen mit Nilpotenzklasse $< p$. Dabei ist P_+ die additive Gruppe dieses Lie-Rings.

Beispiel 14.20.

- (i) Alle p -Gruppen P mit $|P| \leq p^p$ haben Nilpotenzklasse $< p$ und erfüllen daher die Voraussetzung von Satz 14.18. Für $P = \text{SmallGroup}(5^5, 21)$ gilt $|\Omega_5(P)| = 5^3$ und $|\Omega_{25}(P)| = 5^4$. Daher ist $P_+ \cong C_{5^3} \times C_5^2$. Man kann zeigen, dass P_+ genau 56 Untergruppen der Ordnung 25 besitzt. Nach Satz 14.18 besitzt P höchstens so viele Untergruppen (tatsächlich sind es nur 16).
- (ii) Satz 14.18 ist für reguläre p -Gruppen im Allgemeinen falsch: $P := \text{SmallGroup}(3^5, 22)$ ist wegen $P' \cong C_9$ nach Aufgabe 40 regulär mit Nilpotenzklasse 3. Existiert P_+ , so ist $P_+ \cong C_{27} \times C_9$ und $(P^2)_+ \cong C_{27}^2 \times C_9^2$. Allerdings hat P^2 mehr Untergruppen der Ordnung 27 als $(P^2)_+$. Wielandt hat bewiesen, dass P^2 nicht regulär ist.

15 Entscheidbarkeitsprobleme

Bemerkung 15.1 (DEHNs Probleme).

- (i) Sei G eine Gruppe mit Erzeugendensystem X . In der „Praxis“ möchte man folgende Aufgaben algorithmisch lösen:
- (Wortproblem) Wann repräsentiert ein Wort in X das neutrale Element in G ?
 - (Konjugationsproblem) Wann sind zwei Wörter in X als Elemente von G konjugiert?
 - (Isomorphieproblem) Wann ist G zu einer weiteren gegebenen Gruppe H isomorph?
- (ii) Eine Lösung des Wortproblems bedeutet, dass man jedes Element in G auf eine „Normalform“ bringen kann. Nach Lemma 1.7 ist das Wortproblem daher für freie Gruppen lösbar (vorausgesetzt man weiß bereits, dass G frei ist).
- (iii) Ist das Konjugationsproblem für G lösbar, so auch das Wortproblem, denn $g = 1$ genau dann, wenn g und 1 konjugiert sind.
- (iv) NOVIKOV und BOONE haben gezeigt alle drei Probleme selbst für endlich präsentierte Gruppen unlösbar sind, d. h. es gibt keinen allgemeinen Algorithmus, der eines der drei Probleme in endlicher Zeit löst. Selbst die Frage, ob eine gegebene Gruppe endlich oder trivial ist, lässt sich nicht entscheiden!
- (v) Im Allgemeinen hängt die Lösbarkeit der Probleme von der gewählten Darstellung ab. Für endlich erzeugte Gruppen ist die Situation besser.

Satz 15.2. *Sei $G = \langle X \mid R \rangle$ endlich erzeugt. Ist das Wortproblem (bzw. Konjugationsproblem) bzgl. dieser Präsentation von G lösbar, so ist das Wortproblem (bzw. Konjugationsproblem) auch für jede andere endliche erzeugte Präsentation von G lösbar.*

Beweis. Sei $F := F_X$ und $\varphi: F \rightarrow G$ der kanonische Epimorphismus. Sei $F_1 := F_{X_1}$ und $\varphi_1: F_1 \rightarrow G$ eine weitere Präsentation mit $|X_1| < \infty$. Dann existiert eine Funktion $\psi: X_1 \rightarrow F$ mit $(\varphi\psi)(x) = \varphi_1(x)$ für alle $x \in X_1$. Nach der universellen Eigenschaft setzt sich ψ nach F_1 fort. Diese Fortsetzung lässt sich explizit anhand der endlich vielen Werte $\varphi(x)$ mit $x \in X_1$ berechnen. Sei nun $w \in F_1$. Ist das Wortproblem für $\langle X \mid R \rangle$ lösbar, so lässt sich $\varphi(\psi(w)) = 1$ entscheiden. Also lässt sich auch $\varphi_1(w) = 1$ entscheiden, d. h. das Wortproblem für $\langle X_1 \mid R_1 \rangle$ ist lösbar. Analog für das Konjugationsproblem. \square

Satz 15.3. *Das Konjugationsproblem ist für alle freie Gruppen lösbar.*

Beweis. Offenbar ist jedes $g \in F_X$ zu einem zyklisch reduzierten Wort \check{g} konjugiert. Unterscheiden sich \check{g} und \check{h} nur durch Shifts, so sind g und h in F_X konjugiert. Nehmen wir umgekehrt an, dass g und h konjugiert sind. Dann sind auch \check{g} und \check{h} konjugiert. Sei $a \in F_X$ reduziert mit $a\check{g}a^{-1} = \check{h}$. Da \check{h} zyklisch reduziert ist, muss sich a^{-1} vollständig mit \check{g} kürzen. Also ist \check{g} ein Shift von \check{h} . Auf diese Weise kann man entscheiden, ob g und h konjugiert sind. \square

Satz 15.4. *Sei G endlich präsentiert und residual endlich. Dann ist das Wortproblem für G lösbar.*

Beweis. Sei $G = \langle X \mid R \rangle$ eine endliche Präsentation und w ein Wort in X . Wir führen folgende Algorithmen parallel (oder im Wechsel) aus:

- Man konstruiere alle (abzählbar viele) Wörter in R (zum Beispiel in lexikographischer Reihenfolge). Ist $w = 1$ in G , so muss w irgendwann als ein solches Wort auftreten.
- Man konstruiere alle (abzählbar viele) endlichen Gruppen H . Da X endlich ist, gibt es nur endlich viele Homomorphismen $\varphi: G \rightarrow H$. Man prüfe $\varphi(w) \neq 1$. Ist $w \neq 1$, so existiert H und φ mit $\varphi(w) \neq 1$, da G residual endlich ist. \square

Satz 15.5. *Das Wortproblem ist für Coxetergruppen lösbar.*

Beweis. Sei $G = \langle x_1, \dots, x_n \rangle$ eine Coxetergruppe vom Rang n und $w = x_{i_1} \dots x_{i_l} \in G$. Sei $\sigma: G \rightarrow \text{GL}(n, \mathbb{R})$ der Monomorphismus aus Satz 10.14. Dann lässt sich $\sigma(w) = \sigma_{i_1} \dots \sigma_{i_l}$ allein aus den Zahlen m_{ij} berechnen. (Auf dem Computer könnte man die Matriceinträge $\cos(\pi/m_{ij})$ diskret in einem Kreisteilungskörper realisieren anstatt mit rundungsanfälligen Fließkommazahlen zu arbeiten.) Es gilt $w = 1$ genau dann, wenn $\sigma(w) = 1$. \square

Bemerkung 15.6.

- (i) TITS hat einen effizienten Algorithmus für Satz 15.5 gegeben: Sei $G = \langle x_1, \dots, x_n \rangle$ eine Coxetergruppe und $\pi: F_X \rightarrow G$ der kanonische Epimorphismus mit $X = \{x_1, \dots, x_n\}$. Für $w = x_{i_1} \dots x_{i_k} \in F_X$ sei $R(w) \subseteq F_X$ die Menge aller Wörter, die man aus w mittels der folgenden Operationen erhalten kann:

- Ersetze $x_i x_j x_i \dots$ (m_{ij} Buchstaben) durch $x_j x_i x_j \dots$ (m_{ij} Buchstaben).
- Ist $x_i = x_{i+1}$, so entferne $x_i x_{i+1}$.

Da die Länge der Wörter in $R(w)$ beschränkt ist, ist $R(w)$ endlich. Offenbar gilt $\pi(r) = \pi(w)$ für alle $r \in R(w)$. Man kann zeigen, dass $\pi(w) = 1$ genau dann gilt, wenn $1 \in R(w)$ (ohne Beweis).

- (ii) Das Isomorphieproblem für Coxetergruppen wurde noch nicht vollständig gelöst.
- (iii) Die Schwierigkeit der Dehnschen Probleme nutzt man in der Kryptographie aus. Wir beschreiben beispielhaft das ANSHEL-ANSHEL-GOLDFELD-Protokoll zur Bestimmung eines gemeinsamen geheimen Schlüssels zwischen Personen A und B . Gegeben sei eine Gruppe G für die das Wortproblem „effizient“ lösbar ist, das Konjugationsproblem aber nicht. Der öffentliche Schlüssel von A bzw. B besteht aus zufälligen Elementen a_1, \dots, a_n bzw. b_1, \dots, b_n . Die privaten Schlüssel bestehen jeweils aus Wörtern w_A bzw. w_B in a_1, \dots, a_n bzw. b_1, \dots, b_n . Der Schlüsselaustausch basiert auf folgenden Prinzip:

(i) A sendet $(w_A b_1 w_A^{-1}, \dots, w_A b_n w_A^{-1})$ an B .

(ii) B sendet $(w_B a_1 w_B^{-1}, \dots, w_B a_n w_B^{-1})$ an A .

(iii) Beide können nun

$$w_A w_A (w_B a_1 w_B^{-1}, \dots, w_B a_n w_B^{-1}) = [w_A, w_B] = w_B (w_A b_1 w_A^{-1}, \dots, w_A b_n w_A^{-1}) w_B^{-1}$$

berechnen und als gemeinsamen Schlüssel benutzen. In der Praxis setzt man für G Zopfgruppen oder polyzyklische Gruppen ein. Diese kryptographischen Verfahren werden interessant, wenn mit leistungsfähigen Quantencomputern bisherige Verfahren wie RSA unbrauchbar werden.

Aufgaben

Aufgabe 1. Sei F eine freie Gruppe vom Rang > 1 . Zeigen Sie $Z(F) = 1$.

Aufgabe 2. Zeigen Sie:

(a) $Q_{2^n} \cong \langle x, y \mid x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle$ für $n \geq 3$ (siehe GT-Satz 8.15)

(b) $A_4 \cong \langle x, y \mid x^2 = y^3 = (xy)^3 = 1 \rangle$.

Aufgabe 3. Eine Gruppe G heißt *metazyklisch*, falls ein zyklischer Normalteiler N mit zyklischer Faktorgruppe G/N existiert (Beispiel: GT-Satz 7.24). Sei P eine endliche metazyklische p -Gruppe. Zeigen Sie, dass $a, b, c, k \geq 0$ mit $k^{p^b} - 1 \equiv 0 \equiv p^c(k - 1) \pmod{p^a}$ und

$$P \cong \langle x, y \mid x^{p^a} = 1, y^{p^b} = x^{p^c}, yxy^{-1} = x^k \rangle$$

existieren.

Bemerkung: Verschiedene Parameter können zu isomorphen Gruppen gehören. Eine exakte Klassifikation wurde von Liedahl gegeben.

Aufgabe 4. Sei p eine Primzahl, $a \geq 2$ und $b \geq 1$. Sei

$$P(a, b) := P = \langle x, y \mid x^{p^a} = y^{p^b} = 1, yxy^{-1} = x^{1+p^{a-1}} \rangle.$$

Zeigen Sie:

(a) $|P| = p^{a+b}$.

- (b) $P' = \langle x^{p^{a-1}} \rangle \cong C_p$.
(c) $\Phi(P) = Z(P) = \langle x^p, y^p \rangle \cong C_{p^{a-1}} \times C_{p^{b-1}}$.

Aufgabe 5. Eine nicht-abelsche Gruppe G heißt *minimal nicht-abelsch*, falls jede echte Untergruppe von G abelsch ist. Zeigen Sie, dass für eine endliche p -Gruppe P die folgenden Aussagen äquivalent sind:

- (a) P ist minimal nicht-abelsch.
(b) $|P : \Phi(P)| = |P : Z(P)| = p^2$.
(c) $|P : \Phi(P)| = p^2$ und $|P'| = p$.

Hinweis: GT-Kapitel 4.

Aufgabe 6. Sei p eine Primzahl und $a, b \in \mathbb{N}$. Sei

$$Q(a, b) := Q = \langle x, y \mid x^{p^a} = y^{p^b} = [x, y]^p = [x, x, y] = [y, x, y] = 1 \rangle$$

(Erinnerung: $[x, y, z] := [x, [y, z]]$). Zeigen Sie:

- (a) $|Q| = p^{a+b+1}$.
(b) $Q' = \langle [x, y] \rangle \cong C_p$.
(c) $\Phi(Q) = Z(Q) = \langle x^p, y^p, [x, y] \rangle \cong C_{p^{a-1}} \times C_{p^{b-1}} \times C_2$.

Bemerkung: Rédei hat gezeigt, dass jede minimal nicht-abelsche p -Gruppe zu $P(a, b)$, $Q(a, b)$ oder zu Q_8 isomorph ist.

Aufgabe 7. Entscheiden Sie, ob der Petersen-Graph der Cayley-Graph einer Gruppe ist.

Aufgabe 8. Sei F die freie Gruppe über dem Alphabet $\{x, y\}$ und $G \leq F$ die Untergruppe aller Wörter mit gerader Länge. Zeigen Sie, dass G frei durch x^2 , y^2 und xy erzeugt wird.

Aufgabe 9. Sei $G = \langle X \mid R \rangle$ eine einfache Gruppe, wobei jeder Relator in R gerade Länge hat. Zeigen Sie: $G \cong C_2$.

Aufgabe 10. Sei F eine freie Gruppe und $w \in F \setminus \{1\}$. Zeigen Sie $C_F(w) \cong C_\infty$. Folgern Sie, dass F unzerlegbar ist.

Aufgabe 11. Zeigen Sie, dass eine Gruppe H genau dann frei ist, wenn jede Erweiterung von H zerfällt.

Aufgabe 12. Das Koproduct

$$A := \prod_{n \in \mathbb{Z}} \mathbb{F}_2 \leq \prod_{n \in \mathbb{Z}} \mathbb{F}_2$$

besteht aus allen Folgen $(a_n)_{n \in \mathbb{Z}}$ mit $|\{n \in \mathbb{Z} : a_n = 1\}| < \infty$. Offenbar existiert $\gamma \in \text{Aut}(A)$ mit $\gamma((a_n)_n) := (a_{n+1})_n$ für alle $n \in \mathbb{Z}$. Sei $G := A \rtimes \langle \gamma \rangle$. Zeigen Sie, dass G endlich erzeugt und metabelsch ist, aber die Untergruppe $A \leq G$ nicht endlich erzeugt ist.

Aufgabe 13. Bestimmen Sie alle Erweiterungen von C_2 mit C_n bis auf Äquivalenz ($n \in \mathbb{N}$).

Aufgabe 14. Sei

$$D_\infty := \langle x, y \mid x^2 = y^2 = 1 \rangle \cong C_\infty \rtimes C_2$$

(GT-Aufgabe 58(b)). Zeigen Sie, dass $G := \langle x, y \mid x^2 = y^2 \rangle$ eine Erweiterung von D_∞ mit $Z(G) \cong C_\infty$ ist. Folgern Sie, dass G überauflösbar und G' zyklisch ist.

Aufgabe 15. Sei $A := \langle a \rangle \cong C_4$, $S := \text{SL}(2, 3)$ und $G := (S \times A) / \langle (-1_2, a^2) \rangle \cong S * A$ (Zentralprodukt). Zeigen Sie:

- (a) $S \cong Q_8 \rtimes C_3$.
- (b) $Q_8 \trianglelefteq G$ besitzt ein Komplement in $H := Q_8 * A \in \text{Syl}_2(G)$.
- (c) Q_8 besitzt kein Komplement in G .

Bemerkung: Für nicht-abelsche Gruppen N ist der Satz 4.23 von Gaschütz also falsch.

Aufgabe 16. Sei $N := D_8$ und $H \cong C_2$.

- (a) Zeigen Sie $\text{Aut}(N) \cong D_8$.
- (b) Bestimmen Sie alle Erweiterungen von H mit N bis auf Äquivalenz. Welche davon sind isomorph?

Aufgabe 17. Sei $N = \langle a, b \mid a^8 = b^2 = 1, bab^{-1} = a^{-1} \rangle \cong D_{16}$ und $H = \langle x \rangle \cong C_2$. Zeigen Sie:

- (a) Es existiert ein Automorphismus $\beta \in \text{Aut}(N)$ mit $\beta(a) = a^3$ und $\beta(b) = ab$.
- (b) Es existiert ein Homomorphismus $\omega: H \rightarrow \text{Out}(N)$ mit $\omega(x) = \beta \text{Inn}(N)$.
- (c) Es gibt kein Parametersystem von H mit N zur Paarung ω .

Hinweis: Satz 4.16.

Aufgabe 18. Wir betrachten die einfache Gruppe $N := \text{PSL}(2, 9)$ der Ordnung 360. Wir identifizieren die Elemente in N mit ihren Urbildern in $\text{SL}(2, 9)$ (beachte: $Z(\text{SL}(2, 9)) = \langle -1_2 \rangle$). Sei $\mathbb{F}_9^\times = \langle \zeta \rangle$ und $d := \text{diag}(\zeta, 1) \in \text{GL}(2, 9)$. Zeigen Sie:

- (a) Die Abbildung $\sigma: N \rightarrow N$, $x \mapsto dxd^{-1}$ ist ein äußerer Automorphismus mit $\sigma^2 \in \text{Inn}(N)$.
- (b) Die Abbildung $\tau: N \rightarrow N$, $(x_{ij}) \mapsto (x_{ij}^3)$ ist ein äußerer Automorphismus der Ordnung 2.
- (c) Sei $H = \langle x \rangle \cong C_2$. Nach Folgerung 4.28 gibt es je ein Parametersystem (α, κ) von H mit N und $\alpha_x \in \{1, \sigma, \tau, \sigma\tau\}$. Untersuchen Sie, welche der Erweiterungen zerfallen und welche isomorph sind.

Bemerkung: Es gilt $N \cong A_6$.

Aufgabe 19. Sei N abelsch und $\alpha: H \rightarrow \text{Aut}(N)$ ein Gruppenhomomorphismus. Eine Abbildung $\delta: H \rightarrow N$ mit

$$\boxed{\delta(xy) = \delta(x)\alpha_x(\delta(y))}$$

für alle $x, y \in H$ heißt *verschränkter Homomorphismus* bzgl. α . Zeigen Sie:

- (a) Die verschränkten Homomorphismen bilden eine Gruppe $\text{Hom}_\alpha(H, N) \leq C^1(H, N)$.
- (b) Die Abbildung $\Gamma: N \rightarrow \text{Hom}_\alpha(H, N)$, $a \mapsto \delta_a$ mit $\delta_a(x) := \alpha_x(a)a^{-1}$ ist ein Homomorphismus. Man setzt $H_\alpha^1(H, N) := \text{Hom}_\alpha(H, N)/\Gamma(N)$.
- (c) Sei K ein Komplement von N in $G := N \rtimes_\alpha H$. Für $x \in H$ existiert genau ein $y \in K$ mit $\delta_K(x) := xy^{-1} \in N$. Es gilt $\delta_K \in \text{Hom}_\alpha(H, N)$.
- (d) Jedes $\delta \in \text{Hom}_\alpha(H, N)$ definiert ein Komplement $K_\delta := \{\delta(x)^{-1}x : x \in H\}$ von N in G mit $\delta_{K_\delta} = \delta$.
- (e) Zwei Komplemente K_1, K_2 von N in G sind genau dann konjugiert, wenn $\delta_{K_1}\delta_{K_2}^{-1} \in \Gamma(N)$ gilt.
- (f) Die Abbildung $K \rightarrow \delta_K$ induziert eine Bijektion zwischen den Konjugationsklassen von Komplementen von N in G und $H_\alpha^1(H, N)$.

Aufgabe 20 (GASCHÜTZ). Sei N ein abelscher Normalteiler einer endlichen Gruppe G und $N \leq H \leq G$ mit $\text{ggT}(|N|, |G:H|) = 1$. Zeigen Sie: Sind alle Komplemente von N in H konjugiert, so sind alle Komplemente von N in G konjugiert.

Aufgabe 21.

- (a) Zeigen Sie $\text{Aut}(S_n) \cong \text{Aut}(A_n)$ für $n \geq 4$.
- (b) Zeigen Sie, dass $\varphi \in \text{Aut}(S_6)$ mit

$$\begin{aligned}\varphi((1, 2)) &= (1, 5)(2, 3)(4, 6), & \varphi((1, 3)) &= (1, 4)(2, 6)(3, 5), \\ \varphi((1, 4)) &= (1, 3)(2, 4)(5, 6), & \varphi((1, 5)) &= (1, 2)(3, 6)(4, 5), \\ \varphi((1, 6)) &= (1, 6)(2, 5)(3, 4)\end{aligned}$$

ein äußerer Automorphismus der Ordnung 2 ist.

Aufgabe 22. Sei $P = P(a, 1) = M_{p^{a+1}}$ die minimal nicht-abelsche Gruppe aus Aufgabe 4 (oder GT-Satz 8.15) mit $a \geq 2$. Im Fall $p = 2$ sei $a \geq 3$. Zeigen Sie $M(P) = 1$.
Hinweis: Satz 5.25.

Aufgabe 23. Seien $G_i \approx H_i$ isokline Gruppen für $i = 1, 2$. Zeigen Sie $G_1 \times G_2 \approx H_1 \times H_2$.

Aufgabe 24. Zeigen Sie, dass man mindestens 82 Lotto-Scheine (6 aus 49) ausfüllen muss, um zwei „Richtige“ (auf einem Schein) zu haben.

Aufgabe 25. Sei $S = (\Omega, \mathcal{B})$ ein $(2, k, v)$ -Steinersystem. Zeigen, dass die folgenden Aussagen äquivalent sind:

- (1) $v = k^2$.
- (2) $|\mathcal{B}| = k^2 + k$.
- (3) Für $B \in \mathcal{B}$ und $\omega \in \Omega \setminus B$ existiert genau ein Block $B' \in \mathcal{B}$ mit $\omega \in B'$ und $B \cap B' = \emptyset$.

Bemerkung: In der affinen Ebene \mathbb{F}_q^2 ist (3) das *Parallelenpostulat*: Zu jedem Punkt x und jeder Gerade g existiert genau eine Parallele von g , die durch x verläuft.

Aufgabe 26. Zeigen Sie, dass der Higman-Sims-Graph 22-regulär ist, d. h. jede Ecke ist zu genau 22 weiteren Ecken verbunden.

Aufgabe 27. Ein *Gitter* ist eine freie abelsche Untergruppe von \mathbb{R}^n vom Rang n . Jedes Gitter hat also die Form $L = \mathbb{Z}b_1 + \dots + \mathbb{Z}b_n$, wobei $b_1, \dots, b_n \in \mathbb{R}^n$ eine Basis von \mathbb{R}^n ist. Zeigen Sie, dass

$$\text{Aut}(L) = \{f \in \text{O}(\mathbb{R}^n) : f(L) = L\}$$

eine endliche Gruppe ist. Bestimmen Sie $\text{Aut}(\mathbb{Z}^n)$.

Aufgabe 28. Zeigen Sie, dass eine Operation von G auf Ω genau dann 2-transitiv ist, wenn $G = G_\omega \cup G_\omega x G_\omega$ für $\omega \in \Omega$ und ein $x \in G$ gilt.

Aufgabe 29. Zeigen Sie, dass die einfache Gruppe $\text{PSp}(4, 3)$ zu keiner alternierenden Gruppe und keiner projektiven speziellen linearen Gruppe isomorph ist.

Bemerkung: Nach Beispiel 8.13 gilt $\text{PSp}(4, 3) \cong \text{PSU}(4, 2)$. Mit Hilfe von *Zsigmondy-Primzahlen* kann man zeigen, dass $\text{PSp}(2n, q)$ für $n \geq 2$ zu keiner alternierenden Gruppe und keiner projektiven speziellen linearen Gruppe isomorph ist.

Aufgabe 30. Sei V ein unitärer Raum. Zeigen Sie, dass V eine Basis aus Elementen in V_0 besitzt.

Aufgabe 31. Sei V ein unitärer Raum der Dimension n und $U \leq V$ mit $U \subseteq U^\perp$. Zeigen Sie $\dim U \leq \lfloor n/2 \rfloor$. Geben Sie ein Beispiel, in dem Gleichheit gilt.

Bemerkung: Im Allgemeinen (d. h. für beliebige „Skalarprodukte“ auf V) nennt man

$$\max\{\dim U : U \leq V, U \subseteq U^\perp\}$$

den *Witt-Index* von V .

Aufgabe 32. Zeigen Sie $\text{Sp}(2n, q) \leq \text{SU}(2n, q)$ für alle $n \in \mathbb{N}$ und Primzahlpotenzen $q \neq 1$.

Aufgabe 33. Beweisen Sie $\text{PSU}(3, 2) \cong M_9$.

Hinweis: GT-Satz 6.21.

Aufgabe 34. Sei $q \neq 1$ eine ungerade Primzahlpotenz und V ein n -dimensionaler \mathbb{F}_q -Vektorraum. Sei $\beta: V \times V \rightarrow \mathbb{F}_q$ eine nicht-ausgeartete symmetrische Bilinearform. Sei $\lambda \in K^\times \setminus (K^\times)^2$ ein Nicht-Quadrat.

- (a) Konstruieren Sie eine Basis b_1, \dots, b_n von V mit $\beta(b_1, b_1) \in \{1, \lambda\}$, $\beta(b_i, b_i) = 1$ für $i = 2, \dots, n$ und $\beta(b_i, b_j) = 0$ für $i \neq j$.
- (b) Seien β_1 und β_2 Bilinearformen, die die beiden Möglichkeiten in (a) repräsentieren. Sei n ungerade. Zeigen Sie $\text{GO}(n, q, \beta_1) \cong \text{GO}(n, q, \beta_2)$ mit den Bezeichnungen aus Bemerkung 8.28.
- (c) Sei $n = 2$. Zeigen Sie, dass für genau eine der beiden Bilinearformen ein $v \in V \setminus \{0\}$ mit $\beta(v, v) = 0$ existiert. Diese Form bezeichnen wir mit β_+ (Witt-Index 1) und die anderen mit β_- (Witt-Index 0). Für $\epsilon = \pm 1$ sei $\text{GO}^\epsilon(2, q) := \text{GO}(2, q, \beta_\epsilon)$. Zeigen Sie $\text{GO}^\epsilon(2, q) \cong D_{2(q-\epsilon)}$.

Bemerkung: Nach Sylvesters Trägheitssatz gibt es genau $n + 1$ nicht-äquivalente nicht-ausgeartete symmetrische Bilinearformen auf \mathbb{R}^n .

Aufgabe 35. Sei $p > 2$ eine Primzahl und $G := \langle x, y \mid x^p = y^p = (xy)^p = 1 \rangle$. Zeigen Sie $|G| = \infty$.
Hinweis: Realisieren Sie G als Untergruppe von $\text{Sym}(\mathbb{Z})$.

Aufgabe 36. Zeigen Sie:

- (a) Jede Hurwitz-Gruppe G ist perfekt und 84 teilt $|G|$.
- (b) $\text{GL}(3, 2)$ ist eine Hurwitz-Gruppe.

Aufgabe 37. Sei $G = \text{Fr}_{i \in I} G_i$ und $H = \bigoplus_{i \in I} G_i$.

- (a) Konstruieren Sie einen natürlichen Epimorphismus $G \rightarrow H$ und beschreiben Sie seinen Kern.
- (b) Zeigen Sie $G/G' \cong H/H'$.
- (c) Sei $N_i \trianglelefteq G_i$ für $i \in I$. Sei N der normale Abschluss von $\bigcup_{i \in I} N_i$ in G . Zeigen Sie $G/N \cong \text{Fr}_{i \in I} G_i/N_i$.

Aufgabe 38. Sei G ein Amalgam von G_I bzgl. H mit $H < G_i$ für alle $i \in I$. Zeigen Sie: $Z(G) = \bigcap_{i \in I} Z(G_i)$.

Aufgabe 39. Zeigen Sie, dass jede endlich erzeugte periodische auflösbare Gruppe endlich ist.

Aufgabe 40.

- (a) Sei P eine p -Gruppe mit $p > 2$ und P' zyklisch. Zeigen Sie, dass P regulär ist (Bemerkung 14.17).
- (b) Folgern Sie, dass es reguläre p -Gruppen mit beliebig hoher Nilpotenzklasse gibt (für alle $p > 2$).
Bemerkung: Für $p \geq 5$ ist auch die Auflösbarkeitsstufe einer regulären p -Gruppe nicht beschränkt.

Stichwortverzeichnis

Symbole

A^* , 34
 $B^2(H, N)$, 32
 Co_1 , 76
 Co_2 , 76
 Co_3 , 76
 $\delta_n(k)$, 109
 D_∞ , 133
 $\text{Fr}_{i \in I} G_i$, 97
 $G * H$, 97
 $G \approx H$, 44
 $GO(n, q, \rho)$, 67
 $GU(V)$, 59
 $GU(n, q)$, 59
 $H^2(H, N)$, 32
 $H_s^2(H, A)$, 32
 HS , 75
 J_1 , 77
 $k_n(G)$, 45
 $l(g)$, 79
 $M(G)$, 34
 McL , 76
 M_d , 72
 $\Omega_q(G)$, 126
 $\mathcal{U}_q(G)$, 126
 $\omega(c_i)$, 109
 $P\Omega$, 67
 $PSU(V)$, 59
 $PSU(n, q)$, 59
 $P\text{Sp}(V)$, 53
 Φ , 80
 Π , 80
 $SU(V)$, 59
 $SU(n, q)$, 59
 σ_v , 80
 $\text{Sp}(V)$, 53
 $\text{Sz}(q)$, 58
 $W^*(G)$, 120
 $W(G)$, 119
 x_v , 80
 $Z^2(H, N)$, 32
 $Z_s^2(H, A)$, 32
 $Z^*(G)$, 42
 $\partial\varphi$, 32

A

affine Ebene, 73
 Alphabet, 4
 Anshel-Anshel-Goldfeld-Protokoll, 131
 Antisymmetrie, 53
 Artingruppe, 78
 Austauschbedingung, 85
 Automorphismensystem, 22

B

Baer, 43, 128
 Baker-Campbell-Hausdorff-Formel, 129
 Basiskommutator, 109
 Baumslag, 117
 Beyl-Felgner-Schmid, 43
 Birkhoff, 120
 Buchstabe, 4
 Burnside-Gruppe, 104

C

Cayley-Graph, 9
 CFSG, 68
 Chapman, 72
 Coextergraph, 85
 Conway-Gruppe, 76
 Coxeter, 90
 Coxeter-Todd-Algorithmus, 15
 Coxetergruppe, 77
 alternierende Untergruppe, 79
 irreduzible, 85
 universelle, 78

D

Dehns Probleme, 129
 Dynkin-Diagramm, 90

E

Engel, 121
 Epizentrum, 42
 Erweiterung, 20
 zentrale, 32
 zerfallende, 21
 äquivalente, 21

F

Faktorensystem, 22
 triviale, 22
 Fano-Ebene, 73
 Fishers Ungleichung, 74
 freie Algebra, 112
 freies Produkt, 97
 Frucht, 9

G

GAP, 7, 11, 13, 15, 16, 18, 20, 21, 27, 31, 36, 46, 49,
 51, 52, 61, 75, 94
 Gaschütz, 29, 41, 134
 Gewicht
 Basiskommutator, 109
 Gitter, 135
 Golay-Code, 75
 Golod, 103
 Groves, 128

Gruppe

- endlich präsentierte, 6
- hopfsche, 117
- isoklin, 44
- metazyklische, 131
- minimal nicht-abelsche, 132
- polyzyklische, 27
- reguäre, 127
- symplektische, 53
- unitäre, 59
- vollständige, 31
- zentral erweiterbare, 42

Gruppenklasse, 115

Gupta, 103

Guralnick-Kantor-Kassabov-Lubotzky, 17

H

Hall, 45, 116, 117

Hall-Higman-Lemma, 109

Hall-Petrescu-Formel, 125

Halls Kollektor-Prozess, 125

Higman, 123

Higman-Neumann-Neumann, 102

Higman-Sims-Graph, 75

Higman-Sims-Gruppe, 75

HNN-Erweiterung, 102

Hölder, 48

Hopf-Formel, 40

Hurwitz-Gruppe, 96

hyperbolisches Paar, 53

I

inverses Galois-Problem, 76

Isoklinismus, 44

Isometrie, 59

Isomorphieproblem, 129

Iwasawa, 116

J

Jacobi-Identität, 94

Johnson-Zassenhaus, 31

K

Keevash, 77

Kohomologiegruppe, 32

Kommutator

freie Algebra, 112

Konjugationsproblem, 129

Koprodukt, 133

Kozyklus, 32

Kurosch, 100

L

Lazard-Korrespondenz, 129

Leech-Gitter, 76

Levi, 105, 106

Lie-Algebra, 94

Liedahl, 131

Länge, 4, 79

Löschbedingung, 85

M

Magnus, 116

Magnus' Freiheitssatz, 17

Mal'cev, 117

Mathieu, 69, 71

Mathieugruppen, 72

McLaughlin-Gruppe, 76

Mendelsohn, 75

Miller, 96

Monstergruppe, 96

Moore, 16

N

Neumann, 119

Newman, 20

Nielsen-Schreier, 12

Nielsen-Transformationen, 18

Novikov-Ajan, 103

Novikov-Boone, 129

O

Olschanski, 106

Orthogonale Gruppen, 67

P

Paarung, 29

Parallelenpostulat, 135

Parametersystem, 22

normalisiertes, 22

äquivalente, 23

Petersen-Graph, 132

Ping-Pong-Lemma, 6

projektive Darstellung, 42

projektive Ebene, 73

Präsentation

balancierte, 8

Q

quadratische Form, 67

R

Rang, 5

Coxetergruppe, 77

Read, 41

Rédei, 132

Reidemeister-Schreier, 14

Relation, 6

Relator, 6

S

Sanov, 107

Schreier, 25

Schreier-Transversale, 11

Schreiers Formel, 12
 Schur, 35, 41
 Schur-Erweiterung, 34
 maximale, 35
 universelle, 39
 Schur-Multiplikator, 34
 Shephard-Todd, 95
 Sims-Newman-Seeley, 124
 Spiegelung, 78
 komplexe, 95
 Spiegelungsgruppe, 78
 Spinornorm, 67
 Stammgruppe, 45
 Steinberg, 11
 Steinersystem, 73
 Stirling-Zahl, 73
 subdirektes Produkt, 115
 Suzuki-Gruppen, 58
 symplektische Basis, 53
 Symplektischer Raum, 53

T

Tarski-Monster, 106
 Tietze-Transformation, 17
 Tits, 84, 130
 Transvektion
 symplektische, 55
 unitäre, 63

U

unitärer Raum, 58
 Universeller Koeffizientensatz, 37
 Untergruppe
 W -marginale, 120
 verbale, 119

V

Valentiner-Gruppe, 52
 Van der Waerden, 106
 Varietät, 120
 verschränkter Homomorphismus, 134
 Verzweigungsfaktor, 44
 von Dyck, 7
 von-Dyck-Gruppe, 95

W

Wall, 66
 Wielandt, 129
 Witt, 62, 69
 Witt-Index, 135
 Witts Formel, 112
 Wort, 4
 leeres, 4
 reduziert
 Coxetergruppe, 79
 reduziertes, 4
 zyklisch reduziert, 17

 äquivalente, 4
 Wortproblem, 129
 Wurzel, 80
 positive/negative, 80
 Wurzelsystem, 80

Z

Zelmanov, 103
 Zopfgruppe, 78
 Zorn, 121
 Zsigmondy-Primzahlen, 135