# Einführung in die Gruppentheorie, WS 16/17

(Prof. Dr. O. Bogopolski)

## 1 Einige grundlegende Definitionen und Sätze

Sei $G$ eine Gruppe, $H$ eine Untergruppe und $g \in G$. Die Menge

$$gH = \{gh \,|\, h \in H\}$$

heißt *linke Nebenklasse* von $H$ in $G$ mit dem Repräsentant $g$. Die Menge

$$\{gH \,|\, g \in G\}$$

ist die Menge aller linken Nebenklassen von $H$ in $G$. Die rechte Nebenklasse $Hg$ kann man analog definieren. Es gilt:

$$g_1H = g_2H \iff g_1^{-1}g_2 \in H.$$

**Beispiel**
Die Menge aller linken Nebenklassen der Untergruppe $\{e, (12)\}$ in der Gruppe $S_3$ ist:

$$\{e, (12)\},\ \{(13), (123)\},\ \{(23), (132)\}.$$

Die Menge aller rechten Nebenklassen der Untergruppe $\{e, (12)\}$ in der Gruppe $S_3$ ist:

$$\{e, (12)\},\ \{(13), (132)\},\ \{(23), (123)\}.$$

Die Entsprechung $xH \leftrightarrow Hx^{-1}$ ist 1-1, deshalb sind die Kardinalitäten der Mengen von linken und rechten Nebenklassen von $H$ in $G$ gleich. Diese Kardinalität heißt *Index* von $H$ in $G$ und wird als $|G : H|$ bezeichnet.

Eine Untergruppe $H$ von $G$ heißt *normal* (und man schreibt $H \trianglelefteq G$), falls eine von drei äquivalenten Bedingungen erfüllt ist:
1) $gH = Hg \quad \forall g \in G$;
2) $g^{-1}Hg = H \quad \forall g \in G$;
3) $g^{-1}Hg \leqslant H \quad \forall g \in G$.

Sei $H$ normal in $G$. Wir definieren eine Multiplikation auf der Menge von linken Nebenklassen von $H$ in $G$ durch

$$g_1H \cdot g_2H := g_1g_2H.$$

Die Normalität von $H$ in $G$ garantiert, dass diese Definition unabhängig von der Wahl der Repräsentanten in den Nebenklassen ist. Die Menge $\{gH \,|\, g \in G\}$ mit dieser Multiplikation bildet eine Gruppe. Diese Gruppe heißt *Faktorgruppe* von $G$ bezüglich $H$ und wird als $G/H$ bezeichnet. Es ist klar: $|G/H| = |G : H|$.

**Beispiel.** Die Untergruppe $K = \{e, (12)(34), (13)(24), (23)(14)\}$ von $S_4$ ist normal und

$$S_4/K = \{K, (12)K, (13)K, (23)K, (123)K, (132)K\} \cong S_3.$$

Zwei Elemente $a, b \in G$ heißen *konjugiert*, wenn ein $g \in G$ mit $g^{-1}ag = b$ existiert. Wir sagen, dass $a$ zu $b$ *konjugiert ist mit Hilfe von* $g$.

Zum Beispiel (12) ist zu (13) konjugiert mit Hilfe von (123) (in $S_3$).

**Bezeichnung.** Sei $H \leqslant G$. Durch $\mathcal{U}(G, H)$ bezeichnen wir die Menge aller Untergruppen von $G$, die $H$ enthalten. Insbesondere ist $\mathcal{U}(G, 1)$ die Menge aller Untergruppen von $G$.

**Satz 1.1.** Sei $\varphi : G \to G_1$ ein surjektiver Homomorphismus. Dann gilt:

(1) Die Abbildung $\mathcal{U}(G, \ker\varphi) \to \mathcal{U}(G_1, 1)$, $H \mapsto \varphi(H)$, ist eine Bijektion.

(2) Diese Abbildung erhält Indizes: wenn $\ker\varphi \leqslant H_1 \leqslant H_2$ ist, dann ist $|H_2 : H_1| = |\varphi(H_2) : \varphi(H_1)|$.

(3) Diese Abbildung erhält die Normalität: wenn $\ker\varphi \leqslant H_1 \leqslant H_2$ ist, dann ist $H_1 \trianglelefteq H_2 \iff \varphi(H_1) \trianglelefteq \varphi(H_2)$.

**Satz 1.2.** Sei $\varphi : G \to G_1$ ein Homomorphismus. Dann gilt

$$G/\ker\varphi \cong \mathrm{im}\varphi.$$

**Satz 1.3** Sei $A \leqslant B \leqslant G$ und sei $A \trianglelefteq G$, $B \trianglelefteq G$. Dann gilt $B/A \trianglelefteq G/A$ und

$$(G/A)/(B/A) \cong G/B.$$

**Satz 1.4.** Sei $H \trianglelefteq G$ und sei $B \leqslant G$. Dann gilt

$$BH/H \cong B/(B \cap H).$$

**Definition 1.5.** Seien $G_1, \ldots, G_n$ Gruppen. Die Menge

$$\{(g_1, \ldots, g_n) \,|\, g_i \in G_i, i = 1, \ldots, n\}$$

bezüglich der Multiplikation

$$(g_1, \ldots, g_n) \cdot (g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n')$$

bildet eine Gruppe. Diese Gruppe heißt *direktes Produkt* von $G_1, \ldots, G_n$ und wird als $G_1 \times \cdots \times G_n$ bezeichnet.

**Satz 1.6.** Seien $U_1, \ldots, U_n$ Untergruppen einer Gruppe, die die folgenden Bedingungen erfüllen:

(i) $U_i \trianglelefteq G$ für alle $i = 1, \ldots, n$;

(ii) $U_i \cap \langle \bigcup\limits_{j \neq i} U_j \rangle = \{1\}$ für alle $i = 1, \ldots, n$;

(iii) $\langle \bigcup\limits_{i=1}^{n} U_i \rangle = G$.

Dann gilt $G \cong U_1 \times U_2 \times \cdots \times U_n$.

# 2 Die Struktur von endlich erzeugten abelschen Gruppen

**Definition 2.1.** Eine abelsche Gruppe $G$ heißt *frei*, wenn eine Teilmenge $E$ von $G$ existiert, so dass jedes Element $g \in G$ in eindeutiger Form $g = \sum_{e \in E} n_e e$ dargestellt werden kann, wobei $n_i \in \mathbb{Z}$ ist und nur endlich viel $n_e$ ungleich 0 sind. Die Menge $E$ heißt *Basis* der Gruppe $G$.

Man kann beweisen (wie in LA I), dass verschiedene Basen einer freien abelschen Gruppe $G$ gleichmächtig sind. Die Anzahl der Elemente in $E$ heißt *Rang* der Gruppe $G$.

**Beispiel.** Die Gruppe $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ ist eine freie abelsche Gruppe des Ranges 3. Man kann beweisen, dass nur direkte Summen von $\mathbb{Z}$ freie abelsche Gruppen sind.

**Definition 2.2.** Sei $p$ eine Primzahl. Eine Gruppe $G$ heißt *$p$-Gruppe* falls für jedes $g \in G$ ein $k(g)$ existiert, so dass $g^{p^{k(g)}} = 1$ gilt.

**Beispiel.** $\mathbb{Z}_2 \oplus \mathbb{Z}_8$ ist eine 2-Gruppe.

**Satz 2.3.** Sei $F$ eine endlich erzeugte freie abelsche Gruppe mit der Basis $f_1, \ldots, f_n$, und sei $A$ eine Untergruppe von $F$. Dann ist $A$ auch eine freie abelsche Gruppe des Ranges $k \leqslant n$. Außerdem existiert eine Basis $f'_1, \ldots, f'_n$ von $F$, und es existiert eine Basis $a'_1, \ldots, a'_k$ von $A$, so dass $a'_i = m_i f'_i$ für einige $m_i \in \mathbb{Z}$, $i = 1, \ldots, k$, ist.

In dem Fall gilt

$$F/A \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-k}.$$

**Beispiel.** Sei $F$ eine freie abelsche Gruppe mit der Basis $f_1, f_2, f_3$. Sei $A = \langle a_1, a_2 \rangle$ eine Untergruppe von $F$ mit

$$\begin{aligned} a_1 &= 2f_1 - f_2 + 4f_3, \\ a_2 &= 4f_1 + f_2 + 14f_3. \end{aligned}$$

Mit Hilfe von Elementartransformationen über $\mathbb{Z}$ werden wir Basen von $F$ und Erzeuger von $A$ ändern (s. die nächste Seite). Bemerkungen:

- Die Koeffizienten der Elemente aus $A$ bezüglich einer Baseis von $F$ stehen in Zeilen.
- Ersetzen wir $a_i$ durch $a_i + na_j$, dann wird zur $i$-ten Zeile die $n$-fache $j$-te Zeile addiert.
- Ersetzen wir $f_i$ durch $f_i - nf_j$, dann wird zur $j$-ten Spalte die $n$-fache $i$-te Spalte addiert.

  Eine Erklärung dafür ist die Gleichung

  $$\alpha f_i + \beta f_j = \alpha(f_i - nf_j) + (\beta + n\alpha) f_j.$$

  Siehe auch den Übergang von der ersten Tabelle zur zweiten.

- Das Ziel der Transformationen ist, eine "Diagonalmatrix" zu bekommen.

| | $f_1$ | $f_2$ | $f_3$ |
|---|---|---|---|
| $a_1$ | 2 | $-1$ | 4 |
| $a_2$ | 4 | 1 | 14 |

$\downarrow$

| | $f_1$ | $f_2 - f_1$ | $f_3$ |
|---|---|---|---|
| $a_1$ | 1 | $-1$ | 4 |
| $a_2$ | 5 | 1 | 14 |

$\downarrow$

| | $f_1$ | $f_2 - f_1$ | $f_3$ |
|---|---|---|---|
| $a_1$ | 1 | $-1$ | 4 |
| $-5a_1 + a_2$ | 0 | 6 | $-6$ |

$\downarrow$

| | $2f_1 - f_2 + 4f_3$ | $f_2 - f_1$ | $f_3$ |
|---|---|---|---|
| $a_1$ | 1 | 0 | 0 |
| $-5a_1 + a_2$ | 0 | 6 | $-6$ |

$\downarrow$

| | $2f_1 - f_2 + 4f_3$ | $f_2 - f_1 - f_3$ | $f_3$ |
|---|---|---|---|
| $a_1$ | 1 | 0 | 0 |
| $-5a_1 + a_2$ | 0 | 6 | 0 |

Am Ende bekommen wir Basen von $F$ und $A$

$$\begin{aligned} f_1' &= 2f_1 - f_2 + 4f_4, & a_1' &= a_1, \\ f_2' &= -f_1 + f_2 - f_3, & a_2' &= -5a_1 + a_2 \\ f_3' &= f_3 \end{aligned}$$

mit der Eigenschaft $a_1' = f_1'$ und $a_2' = 6f_2'$. Dann gilt nach Satz 2.3

$$\begin{aligned} F/A &\cong \mathbb{Z}_1 \oplus \mathbb{Z}_6 \oplus \mathbb{Z} \\ &\cong \quad \mathbb{Z}_6 \oplus \mathbb{Z}. \end{aligned}$$

**Satz 2.4.** Sei $G$ eine endlich erzeugte abelsche Gruppe. Dann gilt:
(a) Es existiert eine Zerlegung der Form

$$G \cong G_{p_1} \oplus \cdots \oplus G_{p_k} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{t},$$

wobei $G_{p_i}$ endliche abelsche $p_i$-Gruppen sind, $i = 1, \ldots, k$. Dabei gilt $p_i \neq p_j$ für $i \neq j$.

(b) Wenn $G_p$ eine endliche abelsche $p$-Gruppe ist, dann gibt es eine weitere Zerlegung von $G_p$ in $p$-Gruppen, die zyklisch sind:

$$G_p \cong \mathbb{Z}_{p^{l_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{l_s}}.$$

(c) Die Zahlen $t$ und $p^{l_1}, \ldots, p^{l_s}$, wobei $p$ über $\{p_1, \ldots, p_k\}$ läuft, sind eindeutig, d.h. sie hängen nicht von der Zerlegung der Gruppe $G$ ab.

# 3 Semidirektes Produkt, kartesisches Produkt und direktes Produkt, kartesisches Kranzprodukt und direktes Kranzprodukt

**Definition 3.1.** Seien $A, B$ Untergruppen von $G$. Die Gruppe $G$ heißt *semidirektes Produkt* von $A$ und $B$, falls die folgenden Bedingungen erfüllt sind:
1) $A \trianglelefteq G$,
2) $A \cap B = 1$,
3) $G = AB$.

In dem Fall schreibt man $G = A \rtimes B$.

**Beispiele.**
1) Es gilt $S_3 \cong A \rtimes B$, wobei $A = \{id, (123), (132)\}$, $B = \{id, (12)\}$ ist.
2) Seien

$$G = \{ \begin{pmatrix} a & b & x \\ c & d & y \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c, d, x, y \in \mathbb{Z}, ad - bc = 1\},$$

$$A = \{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y \in \mathbb{Z}\},$$

$$B = \{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1\}.$$

Dann ist $G = A \rtimes B$. Merken wir an, dass $A \cong \mathbb{Z} \oplus \mathbb{Z}$ und $B \cong \mathrm{SL}_2(\mathbb{Z})$ ist.

**Definition 3.2.** Sei $I$ eine Menge und seien $G_\alpha$, $\alpha \in I$, Gruppen.
a) Die Menge der Funktionen

$$\overline{\prod_{\alpha\in I}} G_\alpha := \{f : I \to \underset{\alpha\in I}{\cup} G_\alpha \,|\, f(\alpha) \in G_\alpha \text{ für alle } \alpha \in I\}$$

mit der Multiplikation, die durch $fg(\alpha) := f(\alpha)g(\alpha)$, $\alpha \in I$, definiert ist, bildet eine Gruppe. Diese Gruppe heißt *kartesisches Produkt* von $G_\alpha$, $\alpha \in I$.

Das identische Element dieser Gruppe ist die Funktion $id$, so dass $id(\alpha) = e$ für alle $\alpha \in I$ ist.

b) Die Menge

$$\operatorname{supp}(f) := \{\alpha \in I \,|\, f(\alpha) \neq e\}$$

heißt *Träger* der Funktion $f$.

c) Die Teilmenge

$$\prod_{\alpha\in I} G_\alpha := \{f \in \overline{\prod_{\alpha\in I}} G_\alpha \,|\, |\operatorname{supp}(f)| < \infty\}$$

mit der oben definierten Multiplikation bildet eine Gruppe. Diese Gruppe heißt *direktes Produkt* von $G_\alpha$, $\alpha \in I$. Wir haben

$$\prod_{\alpha\in I} G_\alpha \leqslant \overline{\prod_{\alpha\in I}} G_\alpha.$$

**Definition 3.3.** Seien $A, B$ Gruppen. Wir definieren

$$\operatorname{Fun}(B, A) := \{f : B \to A \,|\, f \text{ ist eine Funktion}\}$$

und

$$\operatorname{fun}(B, A) := \{f : B \to A \,|\, \operatorname{supp}(f) < \infty\}.$$

Es ist klar, dass

$$\operatorname{Fun}(B, A) = \overline{\prod_{\alpha\in B}} A_\alpha \quad \text{und} \quad \operatorname{fun}(B, A) = \prod_{\alpha\in B} A_\alpha$$

gilt, wobei $A_\alpha := A$ für alle $\alpha \in B$ ist.

**Definition 3.4.**
a) Für $f \in \operatorname{Fun}(B, A)$ und $b \in B$ definieren wir die Funktion $f^b \in \operatorname{Fun}(B, A)$ durch

$$f^b(x) = f(bx), \;\; x \in B.$$

b) Die Menge

$$A \bar{\wr} B := \{bf \,|\, b \in B, f \in \operatorname{Fun}(B, A)\}$$

mit der Multiplikation

$$bf \cdot b'f' := bb' f^{b'} f'$$

bildet eine Gruppe. Diese Gruppe heißt *kartesisches Kranzprodukt*.

c) Die Menge

$$A \wr B := \{bf \mid b \in B, f \in \mathrm{fun}(B, A)\}$$

mit der in b) definierten Multiplikation bildet eine Gruppe. Diese Gruppe heißt *direktes Kranzprodukt*.

Folgendes ist klar:
(i) $A \wr B \leqslant A \bar{\wr} B$,

(ii) $A \wr B = A \bar{\wr} B$ gilt genau dann, wenn $B$ endlich ist.

(iii) $|A \bar{\wr} B| = |B| \cdot |A|^{|B|}$,

**Struktur des Kranzprodukts.**
Wir definieren zwei natürliche Abbildungen:

$$\begin{aligned} i : B &\to A \bar{\wr} B, \quad b \mapsto b\,id, \\ j : \mathrm{Fun}(B, A) &\to A \bar{\wr} B, \quad f \mapsto e f. \end{aligned}$$

Die Bilder dieser Abbildungen werden mit $B'$ und $\mathrm{Fun}(B, A)'$ bezeichnet. Wir setzen auch $\mathrm{fun}(B, A)' := j(\mathrm{fun}(B, A))$. Es ist klar, dass $B \cong B'$, $\mathrm{Fun}(B, A) \cong \mathrm{Fun}(B, A)'$ und $\mathrm{fun}(B, A) \cong \mathrm{fun}(B, A)'$ ist.

**Satz 3.5.** Es gilt:
(a) $A \bar{\wr} B = \mathrm{Fun}(B, A)' \rtimes B'$,
(b) $A \wr B = \mathrm{fun}(B, A)' \rtimes B'$.

# 4 Satz von Schreier

Das folgende Lemma wird im Satz 4.4 benutzt.

**Lemma 4.1.** Sei $A \trianglelefteq B \leqslant G$ und sei $H \trianglelefteq G$. Dann gilt

$$BH/AH \cong B/A(B \cap H).$$

**Definition 4.2.** Sei $G$ eine Gruppe. Eine Reihe $1 = G_0 \leqslant G_1 \leqslant G_2 \leqslant \cdots \leqslant G_n = G$ heißt *subnormal* in $G$, falls $G_i \trianglelefteq G_{i+1}$ für alle $i = 0, \ldots, n-1$ ist. Diese Reihe heißt *normal* in $G$, falls $G_i \trianglelefteq G$ für alle $i = 0, \ldots, n-1$ ist. Die Faktorgruppen $G_{i+1}/G_i$ heißen *Faktoren* dieser Reihe.

**Definition 4.3.** Seien

$$1 = A_0 \leqslant A_1 \leqslant A_2 \leqslant \cdots \leqslant A_n = G \tag{1}$$

und

$$1 = B_0 \leqslant B_1 \leqslant B_2 \leqslant \cdots \leqslant B_m = G \tag{2}$$

zwei subnormale Reihen in $G$. Die zweite Reihe heißt *Dichtung* der ersten, falls

$$\{A_0, A_1, \ldots, A_n\} \subseteq \{B_0, B_1, \ldots, B_m\}$$

gilt. Die Reihe (1) heißt *dicht*, falls es für sie keine *Dichtung* außer sich selbst gibt.

**Satz 4.4.** (Schreier) Zwei subnormale Reihen (1) und (2) besitzen subnormale Dichtungen

$$1 = A'_0 \leqslant A'_1 \leqslant A_2 \leqslant \cdots \leqslant A'_k = G \tag{3}$$

und

$$1 = B'_0 \leqslant B'_1 \leqslant B'_2 \leqslant \cdots \leqslant B'_k = G, \tag{4}$$

die gleiche Faktoren (bis auf Permutation) haben.

**Beispiel.** Die normale Reihen

$$1 \leqslant \mathbb{Z}_3 \leqslant \mathbb{Z}_{12} \qquad \text{und} \qquad 1 \leqslant \mathbb{Z}_2 \leqslant \mathbb{Z}_{12}$$

besitzen folgende Dichtungen:

$$1 \leqslant \mathbb{Z}_3 \leqslant \mathbb{Z}_6 \leqslant \mathbb{Z}_{12} \qquad \text{und} \qquad 1 \leqslant \mathbb{Z}_2 \leqslant \mathbb{Z}_4 \leqslant \mathbb{Z}_{12}.$$

Die Faktoren der Dichtungen (bis auf Permutation) sind $\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3$.

# 5 Kranzprodukte und Erweiterungen von Gruppen

**Definition 5.1.** Seien $K$ und $H$ Gruppen. Eine Gruppe $G$ heißt *Erweiterung* von $K$ mit Hilfe von $H$, falls $G$ eine Untergruppe $A$ besitzt, so dass $A \trianglelefteq G$, $A \cong K$ und $G/A \cong H$ gilt.

**Beispiele.**

(1) $\mathbb{Z}_6$ und $S_3$ sind Erweiterungen von $\mathbb{Z}_3$ mit Hilfe von $\mathbb{Z}_2$.

(2) Wir betrachten die Quaternionen-Gruppe $Quat := \{\pm 1, \pm i, \pm j, \pm k\}$ (sie besteht aus 8 Elementen) mit der Multiplikation, die folgende Regeln erfüllt:

$$\begin{aligned} &ij = k, \quad && jk = i, \quad && ki = j, \\ &ji = -k, \quad && kj = -i, \quad && ik = -j, \\ &i^2 = -1, \quad && j^2 = -1, \quad && k^2 = -1, \quad (-1)^2 = 1. \end{aligned}$$

Das Zentrum von $Quat$ ist $A = \{1, -1\} \cong \mathbb{Z}_2$. Es gilt

$$Quat/A = \{A, iA, jA, kA\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Also ist $Quat$ eine Erweiterung von $\mathbb{Z}_2$ mit Hilfe von $\mathbb{Z}_2 \times \mathbb{Z}_2$.

**Definition 5.2.** Eine *Einbettung* ist ein injektiver Homomorphismus.

**Satz 5.3.** (Frobenius) Jede Erweiterung von $K$ mit Hilfe von $H$ kann in das Kranzprodukt $K \,\bar{\wr}\, H$ eingebettet werden.

# 6 Einfache endliche Gruppen

**Definition 6.1.** Eine Gruppe $G \neq 1$ heißt *einfach*, falls es keine normale Untergruppe $H$ von $G$ gibt, die kleiner als $G$ und größer als 1 ist.

**Bemerkung 6.2.** Wenn $1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$ eine *dichte* subnormale Reihe von $G$ ist, dann sind die Faktoren $G_{i+1}/G_i$ einfache Gruppen. Außerdem ist $G_{i+1}$ eine Erweiterung von $G_i$ mit Hilfe von $G_{i+1}/G_i$. Deswegen ist es wichtig, einfache Gruppen und Erweiterungen mit Hilfe von einfachen Gruppen beschreiben zu können.

**Satz 6.3.** Sei $1 \neq G$ eine endliche Gruppe und sei $1 \neq H$ eine minimale normale Untergruppe von $G$. Dann existiert eine Zerlegung $H = U_1 \times U_2 \times \cdots \times U_k$, wobei $U_1, \ldots, U_k$ paarweise isomorphe *einfache* Gruppen sind.

**Lemma 6.4.** a) Sei $n \geqslant 3$. Dann ist $A_n$ von allen 3-Zyklen $(ijk)$ erzeugt.

b) Sei $n \geqslant 5$. Dann ist $A_n$ von allen Permutationen der Form $(ij)(kl)$ erzeugt, wobei $i, j, k, l$ verschieden sind.

**Lemma 6.5.** (Bertran-Postulat, bewiesen von Tschebyschow). Für jede natürliche Zahl $n > 1$ existiert eine Primzahl $p$, so dass $n < p < 2n$ ist.

**Satz 6.6.** Sei $n \geqslant 5$. Dann gelten:

a) Die Gruppe $A_n$ ist die minimale nichttriviale normale Untergruppe von $S_n$.

b) Die Gruppe $A_n$ ist einfach.

# 7 Cayley-Satz, Poincaré-Satz und die Rotationsgruppe des Ikosaeders

Sei $M$ eine beliebige Menge. Mit $S(M)$ bezeichnen wir die Gruppe aller Bijektionen von $M$ nach $M$. Falls $M = \{1, 2, \ldots, n\}$ ist, haben wir $S(M) = S_n$.

**Satz 7.1.** (Cayley) Sei $G$ eine Gruppe, sei $H$ eine Untergruppe von $G$ und sei $M$ die Menge aller linken Nebenklassen von $H$ in $G$. Dann ist die Abbildung

$$\begin{aligned} \varphi: \ & G \to S(M), \\ & g \mapsto \big(xH \mapsto gxH, \ \ x \in G\big) \end{aligned}$$

ein Homomorphismus mit

$$\ker(\varphi) = \bigcap_{x \in G} xHx^{-1}.$$

**Satz 7.2.** 1) Es existiert ein injektiver Homomorphismus $\varphi : G \to S(G)$, so dass für jedes $1 \neq g \in G$ die Permutation $\varphi(g)$ kein Element aus $G$ fixiert.

2) Sei $G$ eine endliche Gruppe der Ordnung $n$. Dann ist $G$ einer Untergruppe von $S_n$ isomorph.

3) Sei $G$ eine endliche Gruppe der Ordnung $n$ und sei $F$ ein Körper. Dann ist $G$ einer Untergruppe von $\mathrm{GL}_n(F)$ isomorph.

**Behauptung 7.3.** Sei $G$ eine Gruppe mit $|G| = 6$. Dann ist $G \cong \mathbb{Z}_6$ oder $G \cong S_3$.

**Satz 7.4.** (Poincaré) Sei $H$ eine Untergruppe einer Gruppe $G$ und sei $m = |G : H|$. Dann existiert eine Untergruppe $N \leqslant H$, so dass $N \lhd G$ ist und für den Index $n := |G : N|$ gelten: $m|n$ und $n|m!$.

**Satz 7.5.** Die Rotationsgruppe eines Ikosaeders ist zu $A_5$ isomorph.

# 8 Gruppen die auf einer Menge operieren. Burnside-Satz

**Definition 8.1.** Sei $G$ eine Gruppe und sei $M$ eine Menge. Wir sagen, dass $G$ auf $M$ *operiert*, falls für jedes $g \in G$ und jedes $m \in M$ ein Element $gm \in M$ definiert ist, so dass für alle $g_1, g_2 \in G$ und $m \in M$ gelten:

1) $(g_1 g_2)m = g_1(g_2 m)$,
2) $em = m$.

**Beispiel.** 1) Die Rotationsgruppe eines Ikosaeders operiert auf der Menge seiner Eckpunkte (Kanten, Flächen).
2) Die Gruppe $S_n$ operiert auf der Menge $\{1, 2, \ldots, n\}$.

**Definition 8.2.** Operiere eine Gruppe $G$ auf einer Menge $M$.
a) Für $m \in M$ definieren wir *Orbit* von $m$ in $M$:

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

Es ist klar, dass $M$ eine disjunkte Vereinigung verschiedener Orbits ist.

b) Für $m \in M$ definieren wir den *Stabilisator* von $m$ in $G$:

$$\mathrm{St}_G(m) := \{g \in G \,|\, gm = m\}.$$

Es ist leicht zu verstehen, dass $\mathrm{St}_G(m)$ eine Untergruppe von $G$ ist.

c) Für $g \in G$ definieren wir die *Fixpunktmenge* von $g$ in $M$:

$$\mathrm{Fix}(g) := \{m \in M \,|\, gm = m\}.$$

Es ist klar, dass $\mathrm{Fix}(g)$ eine Teilmenge von $M$ ist.

**Beispiel.**
Die Gruppe $G = \langle id, (12)\rangle$ operiert auf der Menge $M = \{1, 2, 3, 4\}$.
Die Orbits sind: $\{1, 2\}, \{3\}, \{4\}$.
Die Stabilisatoren sind: $\mathrm{St}_G(1) = \mathrm{St}_G(2) = \{id\}$, $\mathrm{St}_G(3) = \mathrm{St}_G(4) = \{id, (12)\}$.
Die Fixpunktmengen sind: $\mathrm{Fix}(id) = \{1, 2, 3, 4\}$, $\mathrm{Fix}((12)) = \{3, 4\}$.

**Satz 8.3.** Operiere eine Gruppe $G$ auf einer Menge $M$. Dann gilt für jedes $m \in M$:

$$|Gm| = |G : \mathrm{St}_G(m)|.$$

**Satz 8.4.** (Burnside) Operiere eine endliche Gruppe $G$ auf einer endlichen Menge $M$. Dann ist die Anzahl von Orbits von $G$ in $M$ gleich

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|.$$

**Beispiel 8.5.** Die Gruppe $\mathbb{Z}_n^*$ ist die multiplikative Gruppe aller invertierbaren Elemente des Ringes $(\mathbb{Z}_n, +_n, \cdot_n)$. Sei $G$ die Untergruppe von $\mathbb{Z}_{30}^*$, die von 7 erzeugt ist. Dann ist

$$\mathbb{Z}_{30} = \{0, 1, 2, 3, \ldots, 29\},$$

$$\mathbb{Z}_{30}^* = \{1, 7, 11, 13, 17, 19, 23, 29\},$$

und

$$G = \{1, 7, 19, 13\}.$$

(a) Die Gruppe $G$ operiert auf der Menge $\mathbb{Z}_{30}^*$ durch Multiplikation. Die Orbits dieser Operierung sind

$$\{1, 7, 19, 13\} \quad \text{und} \quad \{11, 17, 29, 23\}.$$

(b) Die Gruppe $G$ operiert auf der Menge $\mathbb{Z}_{30}$ durch Multiplikation. Diese Operierung hat 12 Orbits:

$$\begin{array}{l}\{0\},\\ \{1, 7, 19, 13\},\\ \{2, 14, 8, 26\},\\ \{3, 21, 27, 9\},\\ \{4, 28, 16, 22\},\\ \{5\},\\ \{6, 12, 24, 18\},\\ \{10\},\\ \{11, 17, 29, 23\},\\ \{15\},\\ \{20\},\\ \{25\}.\end{array}$$

Die Fixpunkte der Elemente aus der Gruppe $G$ in der Menge $\mathbb{Z}_{30}$ sind

$$\begin{array}{l}\mathrm{Fix}(1) = \{0, 1, 2, 3, \ldots, 29\},\\ \mathrm{Fix}(7) = \{0, 5, 10, 15, 20, 25\},\\ \mathrm{Fix}(19) = \{0, 5, 10, 15, 20, 25\},\\ \mathrm{Fix}(13) = \{0, 5, 10, 15, 20, 25\}.\end{array}$$

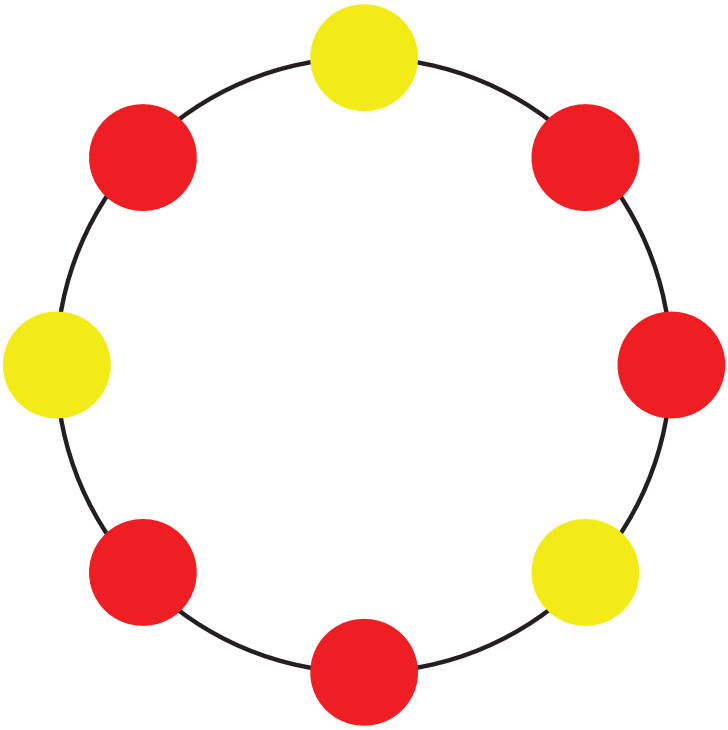
Die Anzahl von Orbits ist

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)| = \frac{1}{4}(30 + 6 + 6 + 6) = 12.$$

**Satz 8.6.** Es gibt genau 57 Färbungen eines Würfels in 3 Farben (jede Fläche soll einfarbig sein). Wir betrachten zwei Färbungen als gleiche, falls eine in die andere mit Hilfe einer Rotation überführt werden kann.

**Aufgabe**. Man hat unbeschränkte Mengen von roten und gelben Perlen. Wie viele Halsketten können aus 8 Perlen gemacht werden?

*Hinweis.* Die Halsketten werden in $\mathbb{R}^3$ betrachtet. Daher sind zwei Halsketten äquivalent, wenn sich die zweite Kette aus der ersten mit Hilfe von Spiegelungen und Rotationen transformiern läßt. Wenden Sie den Burnside-Satz an.



# 9 Projektive spezielle lineare Gruppen

**Definition 9.1.** Sei $K$ ein Körper.

(a) Die *allgemeine lineare Gruppe* $\mathrm{GL}_n(K)$ ist die Gruppe aller Matrizen der Größe $n \times n$ über $K$ mit der Determinante ungleich 0.

(b) Die *spezielle lineare Gruppe* $\mathrm{SL}_n(K)$ ist die Gruppe aller Matrizen der Größe $n \times n$ über $K$ mit der Determinante gleich 1.

(c) Die *projektive spezielle lineare Gruppe* $\mathrm{PSL}_n(K)$ ist die Faktorgruppe von $\mathrm{SL}_n(K)$ bezüglich ihres Zentrums:

$$\mathrm{PSL}_n(K) := \mathrm{SL}_n(K)/Z(\mathrm{SL}_n(K)).$$

**Bemerkung.** Das Zentrum von $\mathrm{SL}_n(K)$ betsteht aus Skalarmatrizen $aE_n$, wobei $E_n$ die Einheitsmatrix und $a \in K$ ein Element mit der Eigenschaft $a^n = 1$ ist:

$$Z(\mathrm{SL}_n(K)) = \{aE_n \mid a \in K, a^n = 1\}.$$

Mit $\mathbb{F}_q$ bezeichnen wir einen Körper der Ordnung $q$. Statt $\mathrm{PSL}_n(\mathbb{F}_q)$ schreibt man auch $\mathrm{PSL}_n(q)$.

**Satz 9.2.**
(a) Die Ordnung von $\mathrm{GL}_n(q)$ ist

$$\prod_{i=0}^{n-1}(q^n - q^i).$$

(b) Die Ordnung von $\mathrm{SL}_n(q)$ ist

$$\frac{1}{(q-1)}\prod_{i=0}^{n-1}(q^n - q^i).$$

(c) Die Ordnung von $\mathrm{PSL}_n(q)$ ist

$$\frac{1}{\mathrm{ggT}(q-1,n)\cdot(q-1)}\prod_{i=0}^{n-1}(q^n - q^i).$$

**Satz 9.3.** $\mathrm{PSL}_2(5) \cong \mathrm{PSL}_2(4) \cong A_5$.

# 10 Doppelte Nebenklassen. Sylow-Satz

**Definition 10.1.** Sei $K, H \leqslant G$ und sei $g \in G$. Die Teilmenge $KgH \subseteq G$ heißt *doppelte Nebenklasse bezüglich $K$ und $H$*. Also ist $\{KgH \mid g \in G\}$ die Menge aller doppelten Nebenklassen bezüglich $K$ und $H$.

**Satz 10.2.** Seien $K, H \leqslant G$. Dann gilt:
1) Jedes Element $g \in G$ liegt in einer einzigen doppelten Nebenklassse bez. $K, H$.
2) Die Gruppe $G$ ist die disjunkte Vereinigung verschiedener doppelter Nebenklassen bez. $K, H$.
3) Die Nebenklasse $KgH$ zerfällt in $|K : K \cap gHg^{-1}|$ linke Nebenklassen von $H$.

**Satz 10.3.** Seien $K, H \in G$ und sei $X$ eine Menge von Repräsentanten von doppelten Nebenklassen bez. $K, H$ (also wählen wir ein Element aus jeder doppelten Nebenklasse). Dann gilt:

$$|G : H| = \sum_{x \in X} |K : K \cap xHx^{-1}|.$$

**Definition 10.4.** Sei $G$ eine endliche Gruppe und sei $|G| = p^k m$, wobei $p$ eine Primzahl, $k \geqslant 1$ und $\mathrm{ggT}(p, m) = 1$ ist. Jede Untergruppe $H \leqslant G$ mit $|H| = p^k$ heißt *$p$-Sylow* Untergruppe von $G$. Die Menge aller *$p$-Sylow* Untergruppen von $G$ wird mit $Syl_p(G)$ bezeichnet.

**Lemma 10.5.** Sei $H$ eine $p$-Sylow Untergruppe von $G$ und sei $K$ eine Untergruppe von $G$. Dann existiert $x \in G$, so dass $K \cap xHx^{-1}$ eine $p$-Sylow Untergruppe von $K$ ist.

**Satz 10.6. (Sylow)** Sei $G$ eine endliche Gruppe und sei $|G| = p^k m$, wobei $p$ eine Primzahl, $k \geqslant 1$ und $\mathrm{ggT}(p, m) = 1$ ist. Dann gilt:

(1) Es existiert eine $p$-Sylow Untergruppe in $G$.

(2) Sei $K \leqslant G$ mit $|K| = p^l$ für einen $l \leqslant k$. Dann existiert eine $p$-Sylow Untergruppe $H$ in $G$, so dass $K \leqslant H$ ist.

(3) Je zwei $p$-Sylow Untergruppen in $G$ sind konjugiert.

(4) Sei $s_p$ die Anzahl von $p$-Sylow Untergruppen in $G$. Dann ist

$$s_p | m \quad \text{und} \quad s_p \equiv 1 \,(\mathrm{mod}\ p).$$

**Behauptung 10.7.** In $S_4$ existieren genau drei 2-Sylow Untergruppen. Sie sind:

$$K \cup K(12), \;\; K \cup K(13), \;\; K \cup K(23),$$

wobei $K = \{id, (12)(34), (13)(24), (14)(23)\}$ ist.

# 11 Normalisator und Zentralisator

**Definition 11.1.** Sei $H \leqslant G$. Der *Normalisator* von $H$ in $G$ ist

$$N_G(H) := \{g \in G \,|\, gHg^{-1} = H\}.$$

**Behauptung 11.2.** Es gilt: $H \trianglelefteq N_G(H) \leqslant G$. Außerdem ist $N_G(H)$ die größte Untergruppe von $G$, die $H$ als normale Untergruppe enthält.

**Beispiel.**
1) $N_{S_3}(\{id, (123), (132)\}) = S_3$.

2) $N_{S_3}(\{id, (12)\}) = \{id, (12)\}$.

**Satz 11.3.** Sei $H$ eine Untergruppe einer Gruppe $G$. Dann ist die Anzahl von Untergruppen von $G$, die mit $H$ konjugiert sind, gleich $|G : N_G(H)|$.

**Folgerung 11.4.** Sei $G$ eine endliche Gruppe und $H$ eine $p$-Sylow Untergruppe in $G$. Dann ist die Anzahl der $p$-Sylow Untergruppen in $G$ gleich dem Index $|G : N_G(H)|$.

**Definition 11.5.** Sei $g \in G$ ein Element. Der *Zentralisator* von $g$ in $G$ ist

$$C_G(g) := \{x \in G \,|\, xgx^{-1} = g\}.$$

**Behauptung 11.6.** Es gilt $\langle g \rangle \trianglelefteq C_G(g) \trianglelefteq N_G(\langle g \rangle) \leqslant G$.

**Satz 11.7.** Sei $g$ ein Element einer Gruppe $G$. Dann ist die Anzahl der Elemente von $G$, die mit $g$ konjugiert sind, gleich $|G : C_G(g)|$.

# 12 Gruppe $A \rtimes_\varphi B$. Gruppen der kleinen Ordnung

**Definition 12.1.** Sei $G$ eine Gruppe. Die Gruppe $Aut(G)$ ist die Gruppe aller Isomorphismen von $G$ nach $G$ bezüglich der Komposition von Abbildungen:

$$Aut(G) := \{\varphi : G \to G \,|\, \varphi \text{ ist bijektiv und } \varphi(xy) = \varphi(x)\varphi(y) \text{ für alle } x, y \in G\}.$$

Das identische Element von $Aut(G)$ ist die Abbildung $id : G \to G$, so dass $id(g) = g$ für alle $g \in G$ ist.

**Beispiel.**
1) $Aut(\mathbb{Z}_5) = \{(1 \mapsto 1), (1 \mapsto 2), (1 \mapsto 3), (1 \mapsto 4)\} \cong \mathbb{Z}_4$.
2) $Aut(\mathbb{Z}_6) = \{(1 \mapsto 1), (1 \mapsto 4)\} \cong \mathbb{Z}_2$.
3) $Aut(\mathbb{Z}) = \{(1 \mapsto 1), (1 \mapsto -1)\} \cong \mathbb{Z}_2$.

**Definition 12.2.** (Gruppe $A \rtimes_\varphi B$)
Seien $A$ und $B$ Gruppen und sei $\varphi : B \to Aut(A)$ ein Homomorphismus. Sei $G$ die Menge aller formalen Elemente $ab$ mit $a \in A$ und $b \in B$, also sei $G := \{ab \,|\, a \in A, b \in B\}$. Wir definieren eine Multiplikation auf $G$ durch

$$ab \cdot a_1 b_1 := a\,\underbrace{\varphi(b)(a_1)}\, bb_1.$$

Man kann beweisen, dass $G$ bezüglich dieser Multiplikation eine Gruppe ist. Diese Gruppe wird als $A \rtimes_\varphi B$ bezeichnet.

**Bezeichnung.** Seien $A = \langle a \rangle$ und $B = \langle b \rangle$ zwei (möglicherweise endliche) zyklische Gruppen. Sei $G = A \rtimes_\varphi B$. Dann ist $\varphi(b)(a) = a^k$ für ein $k \in \mathbb{Z}$. In dem Fall schreiben wir

$$G = A \rtimes_k B.$$

Also, im Fall $G = \mathbb{Z}_n \rtimes_k \mathbb{Z}_m$ meinen wir $\varphi(1)(1) = k$.

**Beispiel 12.3.** (wichtig)

1) Die Gruppe $\mathbb{Z}_6 \rtimes_3 \mathbb{Z}_4$ existiert nicht, weil $1 \mapsto 3$ kein Automorphismus von $\mathbb{Z}_6$ definiert.

2) Die Gruppe $\mathbb{Z}_6 \rtimes_{-1} \mathbb{Z}_2$ existiert.

3) Die Gruppe $\mathbb{Z}_6 \rtimes_{-1} \mathbb{Z}_5$ existiert nicht, obwohl $1 \mapsto -1$ einen Automorphismus von $\mathbb{Z}_6$ definiert (wir bezeichnen ihn durch $inv$). Die Ursache ist, dass es keinen Homomorphismus $\varphi : \mathbb{Z}_5 \to Aut(\mathbb{Z}_6)$, mit $1 \mapsto inv$ gibt.

4) Die Gruppe $\mathbb{Z}_6 \rtimes_{-1} \mathbb{Z}_4$ existiert.

**Definition 12.4.** (Diedergruppen)

(1) Die Gruppe $\mathbb{Z}_n \rtimes_{-1} \mathbb{Z}_2$ heißt *Diedergruppe der Ordnung 2n* und wird mit $D_n$ bezeichnet.

(2) Die Gruppe $\mathbb{Z} \rtimes_{-1} \mathbb{Z}_2$ heißt *unendliche Diedergruppe* und wird mit $D_\infty$ bezeichnet.

**Behauptung 12.5.** Die Symmetriegruppe eines regulären $n$-Ecks besteht aus $n$ Rotationen und $n$ Spiegelungen. Sie ist isomorph der Diedergruppe $D_n$.

**Satz 12.6.** (nützlich)

1) Sei $\varphi : B \to Aut(A)$ der triviale Homomorphismus, also sei $\varphi(b) = id$ für alle $b \in B$. Dann gilt $A \rtimes_\varphi B \cong A \times B$.

2) Die Gruppe $A \rtimes_\varphi B$ enthält isomorphe Kopien von $A$ und $B$:

$$A' := \{ae_B \mid a \in A\} \text{ und } B' := \{e_A b \mid b \in B\}.$$

3) Es gilt $A \rtimes_\varphi B = A' \rtimes B'$. Mit anderen Worten, es gilt:

   a) $A' \trianglelefteq A \rtimes_\varphi B$;

   b) $A' \cap B' = 1$;

   c) $\langle A', B' \rangle = A \rtimes_\varphi B$.

4) Sei $G = A \rtimes B$ ein semidirektes Produkt.

   a) Für jedes $b \in B$ definieren wir eine Abbildung $\widehat{b} : A \to A$ durch $\widehat{b}(a) := bab^{-1}$, $a \in A$. Dann gilt $\widehat{b} \in Aut(A)$.

   b) Jetzt definieren wir eine Abbildung $\varphi : B \to Aut(A)$ durch $\varphi(b) := \widehat{b}$. Dann ist $\varphi$ ein Homomorphismus.

   c) Für dieses $\varphi$ gilt $G \cong A \rtimes_\varphi B$.

**Bezeichnungen.** Weiterhin werden wir die Kopien $A'$ und $B'$ wieder mit $A$ und $B$ bezeichnen.

**Beispiel 12.7.** Wir betrachten die Gruppen
$G_1 = \mathbb{Z}_5 \rtimes_1 \mathbb{Z}_4 = \langle a, b \mid a^5 = 1, b^4 = 1, bab^{-1} = a \rangle \cong \mathbb{Z}_{20}$,
$G_2 = \mathbb{Z}_5 \rtimes_2 \mathbb{Z}_4 = \langle a, b \mid a^5 = 1, b^4 = 1, bab^{-1} = a^2 \rangle$,
$G_3 = \mathbb{Z}_5 \rtimes_3 \mathbb{Z}_4 = \langle a, b \mid a^5 = 1, b^4 = 1, bab^{-1} = a^3 \rangle$,
$G_4 = \mathbb{Z}_5 \rtimes_4 \mathbb{Z}_4 = \langle a, b \mid a^5 = 1, b^4 = 1, bab^{-1} = a^4 \rangle$.

Man kann beweisen, dass nur $G_2$ und $G_3$ isomorph sind.

**Satz 12.8.** Die folgende Liste enthält alle (bis auf Isomorphie) Gruppen der Ordnungen bis 15:

$\mathbb{Z}_1$
$\mathbb{Z}_2$
$\mathbb{Z}_3$
$\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$
$\mathbb{Z}_5$
$\mathbb{Z}_6,\ S_3$
$\mathbb{Z}_7$
$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ Quat,\ D_4$
$\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$
$\mathbb{Z}_{10},\ D_5$
$\mathbb{Z}_{11}$

$\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, $A_4$, $\mathbb{Z}_3 \rtimes_{-1} \mathbb{Z}_4$, $\mathbb{Z}_6 \rtimes_{-1} \mathbb{Z}_2$
$\mathbb{Z}_{13}$
$\mathbb{Z}_{14}$, $D_7$
$\mathbb{Z}_{15}$

*Beweis.* Wir klassifizieren nur die Gruppen der Ordnung 12 (schwerster Fall). Sei $G$ eine Gruppe der Ordnung 12. Nach Sylow-Satz existieren Untergruppen $A$ und $B$ von $G$ mit $|A| = 4$ und $|B| = 3$. Es gilt $A \cong \mathbb{Z}_4$ oder $A \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ und es gilt $B \cong \mathbb{Z}_3$. Sei $B = \langle b \,|\, b^3 = 1 \rangle$.

*Fall 1.* Sei $A \trianglelefteq G$. Dann haben wir $G = A \rtimes B$ und somit ist $G = A \rtimes_\varphi B$ für einen Homomorphismus $\varphi : B \to Aut(A)$.

*Fall 1.1.* Sei $A \cong \mathbb{Z}_4$. Dann ist $A = \langle a \,|\, a^4 = 1 \rangle$. Es gilt

$$Aut(A) = \{id, \theta\} \cong \mathbb{Z}_2,$$

wobei $id : a \mapsto a$ und $\theta : a \mapsto a^{-1}$ ist. Da $|B| = 3$ und $|Aut(A)| = 2$ ist, existiert nur ein Homomorphismus $\varphi : B \to Aut(A)$, nämlich $\varphi(b) = id$. Dann haben wir

$$G = A \rtimes_\varphi B \cong A \times B \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}.$$

*Fall 1.2.* Sei $A \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Dann ist

$$A = \{e, x_1, x_2, x_3 \,|\, x_i^2 = e \text{ und } x_i x_j = x_k \text{ für verschiedene } i, j, k\}.$$

Es gilt $Aut(A) \cong S_3$, weil jede Abbildung $A \to A$, die $e$ nach $e$ abbildet und die Elemente $x_1, x_2, x_3$ beliebig permutiert, ein Automorphismus von $A$ ist. Nun bestimmen wir alle Homomorphismen $\varphi : B \to Aut(A)$.

Da $\mathrm{Ord}(b) = 3$ ist, ist $\mathrm{Ord}(\varphi(b)) = 1$ oder $\mathrm{Ord}(\varphi(b)) = 3$. So gibt es drei Varianten:

a) $\varphi(b) = id$; b) $\varphi(b) = \begin{pmatrix} e & x_1 & x_2 & x_3 \\ e & x_2 & x_3 & x_1 \end{pmatrix}$; c) $\varphi(b) = \begin{pmatrix} e & x_1 & x_2 & x_3 \\ e & x_3 & x_1 & x_2 \end{pmatrix}$.

Wenn wir im Fall c) das Element $b$ nach $b^{-1}$ ersetzen, bekommmen wir den Fall b). Diese Ersetzung entspricht der anderen Wahl der Erzeuger von $B = \langle b \rangle = \langle b^{-1} \rangle$. So haben wir nur zwei Varianten für $G$:

1) $G = A \rtimes_\varphi B$ mit $\varphi$ aus a) oben. Dann ist $G \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_6$.

2) $G = A \rtimes_\varphi B$ mit $\varphi$ aus b) oben. Dann ist $G \cong A_4$.

Um das zu beweisen, betrachten wir in $A_4$ die Untergruppen

$A = \{id, \underbrace{(12)(34)}_{x_1}, \underbrace{(14)(23)}_{x_2}, \underbrace{(13)(24)}_{x_3}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ und $B = \{id, \underbrace{(123)}_{b}, \underbrace{(132)}_{b^2}\} \cong \mathbb{Z}_3$.

Dann ist $A_4 = A \rtimes B$. Wir berechnen, wie $B$ auf der normalen Untergruppe $A$ durch Konjugation operiert:

$$bx_1b^{-1} = x_2,\ bx_2b^{-1} = x_3,\ bx_3b^{-1} = x_1.$$

Wir sehen, dass $\widehat{b} = \varphi(b)$ ist. Nach Satz 12.6.4) gilt: $A_4 \cong A \rtimes_\varphi B$.

*Fall 2.* $A$ ist nicht normal in $G$.

Wir haben $|G : A| = 3$. Nach Poincaré-Satz existiert eine Untergruppe $A_1 \leqslant A$, so dass $A_1 \trianglelefteq G$ ist und für $k = |G : A_1|$ gilt $3|k$ und $k|3!$. Also ist $k = 3$ oder 6. Es kann nicht sein, dass $k = 3$ ist, sonst wäre $|G : A_1| = 3 = |G : A|$ und somit $A_1 = A$, was unmöglich ist.

Also ist $|G : A_1| = 6$. Dann ist $|A_1| = 2$. Da $A_1 \trianglelefteq G$ und $|B| = 3$ ist, haben wir $\langle A_1, B\rangle = A_1 \rtimes B$. Diese Untergruppe hat die Ordnung 6 und den Index 2 in $G$. So ist $\langle A_1, B\rangle \trianglelefteq G$.

Insbesondere ist $gBg^{-1}$ eine Untergruppe von $\langle A_1, B\rangle$ für jedes $g \in G$. Da jede Gruppe der Ordnung 6 eine einzige Untergruppe der Ordnung 3 hat, haben wir $gBg^{-1} = B$. Also ist $B \trianglelefteq G$. Dann ist $G = B \rtimes A$.
Wir bereiten uns vor, um dieses semidirekte Produkt zu beschreiben. Für $B = \langle b \,|\, b^3 = 1\rangle$ gilt:

$$Aut(B) = \{id, \tau\} \cong \mathbb{Z}_2,$$

wobei $id(b) = b$ und $\tau(b) = b^{-1}$ ist.

*Fall 2.1.* Sei $A \cong \mathbb{Z}_4$. Dann ist $A = \langle a \,|\, a^4 = 1\rangle$.

Wir haben $G = B \rtimes_\varphi A$ für einen Homomorphismus $\varphi : A \to Aut(B)$. Es gibt zwei Varianten: $\varphi(a) = id$ und $\varphi(a) = \tau$. Die erste Variante gibt $G = B \times A \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$.

Die zweite Variante gibt eine nichtabelsche Gruppe $G = B \rtimes_\varphi A$ mit $\varphi(a)(b) = b^{-1}$. Wir schreiben kurz $G = \mathbb{Z}_3 \rtimes_{-1} \mathbb{Z}_4$.

*Fall 2.2.* Sei $A \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Dann ist

$$A = \{e, x_1, x_2, x_3 \,|\, x_i^2 = e \text{ und } x_i x_j = x_k \text{ für verschiedene } i, j, k\}.$$

Wir haben $G = B \rtimes_\varphi A$ für einen Homomorphismus $\varphi : A \to Aut(B)$. Es gibt zwei Varianten (bis zum Umbenennen von $x_i$):

1) $\varphi(x_i) = id$ für alle $x_i \in A$,

2) $\varphi(x_1) = id$, $\varphi(x_2) = \tau$, $\varphi(x_3) = \tau$.

Die erste Variante gibt $G = B \times A \cong \mathbb{Z}_3 \times (\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathbb{Z}_6 \times \mathbb{Z}_2$. Die zweite Variante gibt $G = B \rtimes_\varphi A$ mit dem entsprechenden $\varphi$. Wir schreiben kurz $G \cong \mathbb{Z}_3 \rtimes_{\{1,-1\}} (\mathbb{Z}_2 \times \mathbb{Z}_2)$. Es ist leicht zu verstehen, dass die letzte Gruppe isomorph zu $\mathbb{Z}_6 \rtimes_{-1} \mathbb{Z}_2$ ist. □

**Fortsetzung nächste Seite**

# 13 $k$-transitive Operierung

**Definition 13.1.** Sei $k$ eine natürliche Zahl. Eine Gruppe $G$ operiert auf einer Menge $M$ *$k$-transitiv*, falls das Folgende gilt:

für je zwei $k$-Tupel $(m_1, \ldots, m_k)$ und $(m'_1, \ldots, m'_k)$ von Elementen aus $M$,
wobei $m_i \neq m_j$ und $m'_i \neq m'_j$ für $i \neq j$ sind,
existiert ein $g \in G$ mit $gm_i = m'_i$ für alle $i = 1, \ldots, k$,

**Beispiel 13.2.**

1) Die Rotationsgruppe eines Würfels operiert auf der Menge der Eckpunkte des Würfels 1-transitiv, aber nicht 2-transitiv.
2) $S_n$ operiert auf $\{1, 2, \ldots, n\}$ $n$-transitiv.
3) $A_n$ operiert auf $\{1, 2, \ldots, n\}$ $(n-2)$-transitiv für $n \geqslant 3$.

**Bemerkung.** Man sagt "transitiv" anstatt "1-transitiv". Eine Gruppe $G$ operiert auf einer Menge $M$ transitiv genau dann, wenn es nur einen Orbit gibt – $M$ selbst.

**Definition 13.3.** Eine Gruppe $G$ operiert auf einer Menge $M$ *treu*, falls für jedes nicht-triviale Element $g \in G$ ein $m \in M$ mit $gm \neq m$ existiert.

**Beispiel 13.4.**

1) Alle Operierungen aus dem Beispiel 13.2 sind treu.

2) Sei $G$ eine nicht-triviale Gruppe und sei $M$ eine Menge. Wir definieren eine Operierung von $G$ auf $M$ durch $gm = m$ für alle $g \in G$, $m \in M$. Diese Operierung ist untreu.

**Satz 13.5.** Operiert eine Gruppe $G$ auf einer Menge $M$ treu und 2-transitiv, dann operiert jede nicht-triviale normale Untergruppe $N$ von $G$ auf der Menge $M$ transitiv.

# 14 Ein Kriterium der Einfachheit. Satz von Dickson

**Definition. 14.1.** Sei $G$ eine Gruppe. Für $a, b \in G$ heißt das Element $[a, b] := aba^{-1}b^{-1}$ *Kommutator* von $a$ und $b$. Die Untergruppe, die von allen Kommutatoren erzeugt ist, heißt *Kommutator-Untergruppe* und wird mit $[G, G]$ oder $G'$ bezeichnet.

**Satz 14.2.** Gegeben ist: Eine Gruppe $G$ operiert treu und 2-transitiv auf einer Menge $M$, so dass folgende zwei Bedingungen erfüllt sind:

(1) $G = G'$.

(2) Es existiert ein $m \in M$, so dass $\mathrm{St}_G(m)$ eine Untergruppe $A$ enthält, für welche gilt:

   (a) $A$ ist abelsch;

   (b) $A$ ist normal in $\mathrm{St}_G(m)$;

   (c) $G = \langle gAg^{-1} \mid g \in G \rangle$.

Dann ist $G$ einfach.

**Satz 14.3. (Dickson)** Sei $K$ ein Körper. Dann ist die Gruppe $\mathrm{PSL}_n(K)$ einfach mit zwei Ausnahmen: $\mathrm{PSL}_2(2)$ und $\mathrm{PSL}_2(3)$.

# 15 Nilpotente Gruppen (Teil I)

**Definition 15.1.**

(a) Für zwei Untergruppen $A, B$ einer Gruppe $G$ definieren wir ihre *Kommutator-Untergruppe*:

$$[A, B] := \langle [a, b] \mid a \in A, b \in B \rangle.$$

(b) Sei $\gamma_1(G) = G$ und $\gamma_{i+1}(G) := [G, \gamma_i(G)]$ für $i \geqslant 1$.

Man erhält dadurch *absteigende Zentralreihe* von $G$:

$$G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \dots$$

(c) Eine Gruppe $G$ heißt *nilpotent*, falls $\gamma_{n+1}(G) = 1$ für einen $n \in \mathbb{N} \cup \{0\}$ ist. Die minimale $n$ mit $\gamma_{n+1}(G) = 1$ heißt *Nilpotenzgrad* von $G$.

**Beispiel.**

1) Die triviale Gruppe ist nilpotent des Grades 0.

2) Alle nichttrivialen abelschen Gruppen sind nilpotente Gruppen des Grades 1.

3) Die Heisenberg-Gruppe

$$H_3 = \{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \}$$

ist nilpotent des Grades 2.

4) Die Heisenberg-Gruppe $H_n$ ist nilpotent des Grades $n - 1$.

**Bezeichnung.** Seien $a, b, c$ drei Elemente einer Gruppe. Wir bezeichnen:

$$[a, b] := a^{-1}b^{-1}ab \quad \text{und} \quad a^c := c^{-1}ac.$$

**Behauptung 15.2.** Seien $a, b, c$ drei Elemente einer Gruppe. Dann gilt:

a) $[a, b] = [b, a]^{-1}$,

b) $[ab, c] = [a, c]^b [b, c]$,

c) $[a, bc] = [a, c][a, b]^c$,

d) $[a^{-1}, b] = [b, a]^{a^{-1}}$,

e) $[a, b]^c = [a^c, b^c]$.

**Behauptung 15.3.** Seien $A, B$ zwei Untergruppen einer Gruppe $G$. Dann gilt $[A, B] = [B, A]$.

# 16 Nilpotente Gruppen (Teil II)

**Definition 16.1.** Im Fogenden definieren wir die Reihe der *Hyperzentren* von $G$ (oder *aufsteigende Zentralreihe* von $G$)

$$1 = \Gamma_0(G) \leqslant \Gamma_1(G) \leqslant \Gamma_2(G) \leqslant \dots.$$

a) Sei $\Gamma_0(G) = 1$. Nehmen wir an, dass $\Gamma_i(G)$ schon definiert ist und $\Gamma_i(G) \trianglelefteq G$ ist. Dann definieren wir $\Gamma_{i+1}(G)$ als Urbild des Zentrums $Z(G/\Gamma_i(G))$ unter dem kanonischen Homomorphismus $G \to G/\Gamma_i(G)$.

$$\begin{array}{ccc} G & \longrightarrow & G/\Gamma_i(G) \\ \mathbb{V} & & \mathbb{V} \\ \Gamma_{i+1}(G) & \longrightarrow & Z(G/\Gamma_i(G)) \end{array}$$

Da Urbilder normaler Untergruppen normal sind, gilt $\Gamma_{i+1}(G) \trianglelefteq G$. Deshalb können wir $\Gamma_{i+2}(G)$ definieren u.s.w.

b) Eine äquivalente Definition: $\Gamma_0(G) = 1$,

$$\begin{aligned} \Gamma_{i+1}(G) &= \{x \in G \mid x\Gamma_i(G) \cdot g\Gamma_i(G) = g\Gamma_i(G) \cdot x\Gamma_i(G) \text{ für alle } g \in G\} \\ &= \{x \in G \mid [x, g] \in \Gamma_i(G) \text{ für alle } g \in G\}. \end{aligned}$$

Daraus folgt

$$[\Gamma_{i+1}(G), G] \leqslant \Gamma_i(G).$$

c) Noch eine äquivalente Definition: $\Gamma_0(G) = 1$ und $\Gamma_{i+1}(G)$ ist die maximale Untergruppe $X$ von $G$ mit der Eigenschaft $[X, G] \leqslant \Gamma_i(G)$.

**Bemerkung.** $\Gamma_1(G) = Z(G)$.

**Satz 16.2.** Für jede Gruppe $G$ sind folgende drei Bedingungen äquivalent:

1) $\gamma_{n+1}(G) = 1$.

2) $\Gamma_n(G) = G$.

3)
$$\begin{array}{ccccccccc} 1 = & \Gamma_0(G) & \leqslant & \Gamma_1(G) & \leqslant \dots \leqslant & \Gamma_{n-1}(G) & \leqslant & \Gamma_n(G) = G & (\mathbf{o}) \\ & \mathbb{V} & & \mathbb{V} & & \mathbb{V} & & \mathbb{V} & \\ 1 = & \gamma_{n+1}(G) & \leqslant & \gamma_n(G) & \leqslant \dots \leqslant & \gamma_2(G) & \leqslant & \gamma_1(G) = G & (\mathbf{u}) \end{array}$$

**Skizze des Beweises.** Es reicht zu beweisen, dass für jedes $i = 0, \dots, n$ die folgende Äquivalenz gilt:

$$\gamma_i(G) \leqslant \Gamma_{n+1-i} \iff \gamma_{i+1}(G) \leqslant \Gamma_{n-i}.$$

Das sieht man leicht aus $\gamma_{i+1}(G) = [G, \gamma_i(G)]$ und Definition 16.1 c). □

**Bemerkung.** Das rechtfertigt die folgende Terminologie:

(a) Die aufsteigende Zentralreihe

$$1 = \Gamma_0(G) \leqslant \Gamma_1(G) \leqslant \Gamma_2(G) \leqslant \dots.$$

heißt *obere Zentralreihe* von $G$.

(b) Die absteigende Zentralreihe

$$G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \gamma_3(G) \geqslant \dots$$

heißt *untere Zentralreihe* von $G$.

**Satz 16.3.** Alle Untergruppen und Faktorgruppen einer nilpotenten Gruppe sind nilpotent.

**Bemerkung.** Sei $F \trianglelefteq G$ und $G/F = B$. Wenn $F$ und $B$ nilpotent sind, dann ist $G$ nicht unbedingt nilpotent. Mit anderen Worten sind die Erweiterungen von nilpotenten Gruppen nicht unbedingt nilpotent. Um das zu zeigen, nehmen wir

$$G = \mathbb{Z}_3 \wr \mathbb{Z}_2, \qquad F := \mathrm{fun}(\mathbb{Z}_2, \mathbb{Z}_3), \qquad B := \mathbb{Z}_2.$$

Nach Satz 3.5 b), ist $G = F \rtimes B$ und so ist $G/F = B$. Die Gruppen $F$ und $B$ sind abelsch und so nilpotent. Die Gruppe $G$ ist aber nicht nilpotent, weil sie $S_3$ enthält.

**Lemma 16.4.** Sei $G$ eine nilpotente Gruppe des Nilpotenzgrades $n$ und sei $a \in G$. Dann hat die Untergruppe $\langle [G, G], a\rangle$ den Nilpotenzgrad $\leqslant n - 1$.

**Terminologie.** Sei $G$ eine Gruppe. Ein Element $g \in G$ heißt *periodisch*, wenn es eine endliche Ordnung hat.

**Satz 16.5.** Periodische Elemente einer nilpotenten Gruppe bilden eine Untergruppe.

# 17 Nilpotente Gruppen (Teil III)

**Definition 17.1.** Sei $p$ eine Primzahl. Eine nichttriviale Gruppe $G$ heißt *$p$-Gruppe*, falls für jedes $g \in G \setminus \{e\}$ die Ordnung von $g$ eine Potenz von $p$ ist:

$$\mathrm{Ord}(g) = p^{n(g)}.$$

**Bemerkung 17.2.** Sei $G$ eine endliche Gruppe und $p \in \mathrm{Prim}$. Dann ist äquivalent:
(a) $G$ ist eine $p$-Gruppe.
(b) $|G| = p^k$ für ein $k \geqslant 1$.

**Satz 17.3.** Sei $G$ eine endliche $p$-Gruppe. Dann gilt $Z(G) \neq 1$. Insbesondere ist $G$ nilpotent.

**Korollar 17.4.** Sei $p$ eine Primzahl. Jede Gruppe $G$ der Ordnung $p^2$ ist abelsch, deshalb gilt

$$G \cong \mathbb{Z}_{p^2} \quad \text{oder} \quad G \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

**Lemma 17.5.** Sei $P$ eine Sylow-Untergruppe einer endlichen Gruppe $G$ und sei $N_G(P) \leqslant H \leqslant G$. Dann gilt: $H = N_G(H)$.

**Korollar 17.6.** Sei $P$ eine Sylow-Untergruppe einer endlichen Gruppe $G$. Dann gilt

$$N_G(N_G(P)) = N_G(P).$$

**Satz 17.7.** Sei $G$ eine nilpotente Gruppe und sei $H < G$. Dann gelten:

(1) Die Reihe von Normalisatoren $H \leqslant N_G(H) \leqslant N_G(N_G(H)) \leqslant \ldots$ erreicht $G$ nicht später als in $n$ Schritten, wobei $n$ der Nilpotenzgrad von $G$ ist.
(2) $H \lneqq N_G(H)$.

**Satz 17.8. (Burnside-Wielandt)**. Sei $G$ eine endliche Gruppe. Dann sind die folgenden Bedingungen äquivalent:

(1) $G$ ist nilpotent.
(2) Für alle Untergruppen $H \lneqq G$ gilt $H \lneqq N_G(H)$.
(3) Sei $|G| = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$ eine Primzahlzerlegung von $|G|$. Dann gilt

$$G \cong G_{p_1} \times \ldots \times G_{p_s},$$

wobei $G_{p_i}$ eine (und somit auch die einzige) $p_i$-Sylow Untergruppe von $G$ ist.

**Fortsetzung nächste Seite**

# 18 Burnside-Problem

Es gibt drei Variationen des Burnside-Problems: klassisch, schwach und eingeschränkt.

**KLASSISCHES BURNSIDE-PROBLEM (Burnside, 1902):**
Sei $n$ eine natürliche Zahl und sei $G$ eine endlich erzeugte Gruppe, so dass für alle $g \in G$ gilt: $g^n = 1$. Ist $G$ endlich?

Die Antwort ist `positiv` für
$n = 2$ (leicht),
$n = 3$ (Levi und van der Waerden, 1933),
$n = 4$ (Sanow, 1940)
$n = 6$ (M. Hall, 1976).

Die Antwort ist `negativ` für
alle ungerade $n > 4381$ (P.S. Novikov und S.I. Adian, 1968)
alle ungerade $n > 665$ (S.I. Adian, 1975)

Das Problem für $n = 5, 7$ und $n = 8$ ist bis jetzt offen.

**Satz (Ol'shanski, 1982).** Sei $p$ eine Primzahl größer als $10^{75}$. Es existiert eine unendliche Gruppe $G$, so dass jede echte Untergruppe von $G$ isomorph $\mathbb{Z}_p$ ist.

Diese Gruppe heißt Tarski-Monster.

**SCHWACHES BURNSIDE-PROBLEM:** Sei $G$ endlich erzeugt und für alle $g \in G$ existiert $n(g) \in \mathbb{N}$, so dass $g^{n(g)} = 1$ ist. Ist $G$ endlich?

Die Antwort ist `negativ` nach folgendem Satz:

**Satz (Golod, 1964).** Für jede Primzahl $p$ existiert eine 2-erzeugte unendliche $p$-Gruppe.

**Satz (Grigorchuk, Gupta-Sidki).** Für jede ungerade Primzahl $p$ existiert ein Baum $X$, so dass $\mathrm{Aut}(X)$ eine Untergruppe $G$ enthält, für die folgendes gilt:

(1) $G$ ist von 2 Elementen erzeugt.
(2) $G$ ist eine $p$-Gruppe.
(3) $G$ ist unendlich.

Eine Gruppe $G$ heißt *periodisch*, wenn jedes Element von $G$ eine endliche Ordnung hat.

**Satz (Schur, 1911).** Jede endlich erzeugte periodische Untergruppe von $\mathrm{GL}_n(\mathbb{C})$ ist endlich.

**EINGESCHRÄNKTES BURNSIDE-PROBLEM:** Seien $n, m \in \mathbb{N}$. Gibt es eine natürliche Zahl $f(n, m)$, so dass die Ordnung jeder endlichen $m$-erzeugten Gruppe mit dem Gesetz $g^n = 1$ nicht größer als $f(n, m)$ ist?

Die Antwort ist `positiv` (Zelmanov, Fields-Prämie 1994; Nowosibirsk).

# 19 Freie Gruppen

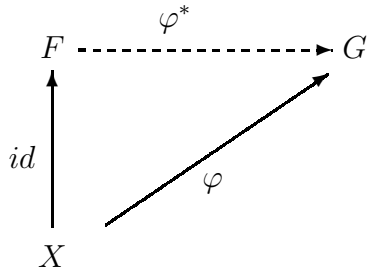
Literatur: Seiten 52-56 des Buches von O. Bogopolski "Introduction to Group Theory".

**Definition 19.1.** Eine Gruppe $F$ heißt *frei*, wenn eine Teilmenge $X \subseteq F$ existiert, so dass $X \cap X^{-1} = \emptyset$ ist und jedes Element $f \in F$ auf genau eine Weise in der Form $f = x_1 x_2 \dots x_n$ geschrieben werden kann, wobei $x_i \in X \cup X^{-1}$ und $x_i x_{i+1} \neq 1$ für $i = 1, \dots, n-1$ ist. Diese Form heißt *irreduzibel*. Die Menge $X$ heißt *Basis* von $F$.

Die *Länge des Elements $f$ bezüglich $X$* ist $n$ und wird als $|f|$ bezeichnet.

**Satz 19.2.** Für jede Menge $X$ existiert eine freie Gruppe mit der Basis $X$. Alle freien Gruppen mit der Basis $X$ sind isomorph. (Wir bezeichnen eine als $F(X)$.)

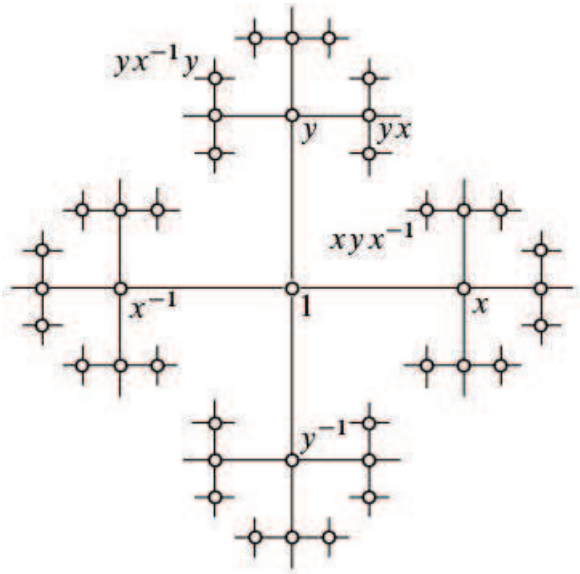
**Satz 19.3.** Eine Gruppe $F$ ist frei mit der Basis $X$ genau dann, wenn für jede Gruppe $G$ und jede Abbildung $X \xrightarrow{\varphi} G$ ein einziger Homomorphismus $F \xrightarrow{\varphi^*} G$ mit $\varphi^*|_X = \varphi$ existiert.




**Satz 19.4.** Alle Basen einer freien Gruppe haben dieselbe Kardinalität.[1]

Diese Kardinalität heißt *Rang* der freien Gruppe.

Folgender (unendlicher!) Graph stellt die freie Gruppe $F(x, y)$ dar:




[1]Wir benutzten folgender Fakt: Für jede unendliche Menge $X$ gilt $|X \times X| = |X|$. Das ist richtig im Rahmen der Zermelo-Frenkel Axiomatik, wenn man noch die Auswahlaxiom voraussetzt.

# 20 Nielsen-Methode

Literatur: Seiten 123-124 des Buches von O. Bogopolski "Introduction to Group Theory". Auch siehe die ersten 10 Seiten des Buches von R. Lyndon, P. Schupp "Combinatorial group theory".

**Behauptung 20.1.** Sei $F$ eine freie Gruppe vom Rang 2 und $(u, v)$ eine Basis von $F$. Dann gelten:
1) $(u, vu^{\varepsilon})$ und $(u, u^{\varepsilon}v)$, $\varepsilon = \pm 1$ sind die Basen von $F$,
2) $(v, u)$ ist eine Basis von $F$,
3) $(u, v^{-1})$ ist eine Basis von $F$.

**Beispiel.** $(ababa^{-1}, ab)$ ist eine Basis der freien Gruppe $F(a, b)$:

$$(ababa^{-1}, ab) \to (aba^{-1}, ab) \to (a^{-1}, ab) \to (a^{-1}, b) \to (a, b).$$

**Frage.** Wie kann man algorithmisch erkennen, ob eine Teilmenge $U$ einer freien Gruppe $F(X)$ eine Basis von $F(X)$ ist?

**Definition 20.2.** Sei $U = (u_1, \dots, u_m)$ ein Tupel von Elementen einer freien Gruppe $F(X)$. Wir bezeichnen $U^{\pm} := \{u_1, \dots, u_m\} \cup \{u_1^{-1}, \dots, u_m^{-1}\}$. Also ist $U$ ein Tupel und $U^{\pm}$ eine Menge. Ferner bezeichnen wir $\langle U \rangle := \langle u_1, \dots, u_m \rangle$. Das ist eine Untergruppe von $F(X)$.

• *Nielsen-Transformationen* sind:

(T1) ein $u_i$ nach $u_i^{-1}$ ersetzen,
(T2) ein $u_i$ nach $u_i u_j$ ersetzen, wobei $i \neq j$ ist,
(T3) $u_i$ ausstreichen, wenn $u_i = 1$ ist.

• Das Tupel $U = (u_1, \dots, u_m)$ heißt *Nielsen-irreduzibel*, wenn $u_i \neq u_j$ und $u_i \neq u_j^{-1}$ für alle $i \neq j$ ist und für alle $v_1, v_3, v_3 \in U^{\pm}$ gilt

(N1) $v_1 \neq 1$,
(N2) aus $v_1 v_2 \neq 1$ folgt $|v_1 v_2| \geqslant |v_1|, |v_2|$,
(N3) aus $v_1 v_2 \neq 1$ und $v_2 v_3 \neq 1$ folgt $|v_1 v_2 v_3| > |v_1| - |v_2| + |v_3|$,

**Behauptung 20.3.** Transformieren wir ein Tupel $U$ in ein anderes Tupel $U'$ mit Hilfe der Nielsen-Transformationen (T1)-(T3). Dann gilt $\langle U \rangle = \langle U' \rangle$.

**Behauptung 20.4.** Sei $U = (u_1, \dots, u_m)$ ein Nielsen-irreduzibles Tupel in $F(X)$. Sei $v = v_1 v_2 \dots v_k$ ein Produkt, wobei $k \geqslant 0$, $v_i \in U^{\pm}$ und $v_i v_{i+1} \neq 1$ ist. Dann ist $|v| \geqslant k$. Insbesondere ist $\langle U \rangle$ eine freie Gruppe mit der Basis $U$.

**Satz 20.5.** Man kann jedes Tupel $U = (u_1, \dots, u_m)$ von Elementen einer freien Gruppe $F$ in ein Nielsen-irreduzibles Tupel $U_{Nirr}$ mit Hilfe der Nielsen-Transformationen transformieren.

**Folgerung 20.6.** Die Gruppe $\langle U \rangle$ ist frei mit der Basis $U_{Nirr}$. Insbesondere ist jede endlich erzeugte Untergruppe einer freien Gruppe frei.

**Folgerung 20.7.** Ein Tupel $U$ von Elementen aus $F(X)$ ist eine Basis von $F(X)$ nur dann, wenn $|U| = |X|$ ist und $U_{Nirr} = X$ bis auf Permutationen und Inversionen der Elemente in $X$ gilt.

# 21 Präsentationen von Gruppen

**Definition 21.1.** Sei $R \subseteq F$ eine Teilmenge einer Gruppe $F$. Der *normale Abschluss* von $R$ in $F$ ist die Menge

$$R^F = \{\prod_{i=1}^{k} f_i^{-1} r_i^{\varepsilon_i} f_i \mid f_i \in F, r_i \in R, \varepsilon_i = \pm 1, k = 0, 1, \dots\}.$$

Es ist leicht zu verstehen, dass $R^F$ eine normale Untergruppe von $F$ ist. Außerdem ist $R^F$ die kleinste normale Untergruppe von $F$, die $R$ enthält.

**Lemma 21.2.** Sei $r \in R \subseteq F$ und $u, v \in F$. Dann gilt:

$$urv \in R^F \Leftrightarrow uv \in R^F.$$

**Definition 21.3.** Sei $G$ eine Gruppe. Dann existiert eine freie Gruppe $F(X)$ und ein surjektiver Homomorphismus $\varphi : F(X) \to G$. Somit gilt

$$G \cong F(X)/\mathrm{Ker}\,\varphi.$$

Sei $R$ eine beliebige Teilmenge von $F(X)$ mit $R^{F(X)} = \mathrm{Ker}\,\varphi$. Dann heißt

$$\langle X \mid R \rangle$$

*Präsentation* von $G$. Diese Präsentation heißt *endlich*, wenn $X$ und $R$ endlich sind.

Eine Gruppe kann mehrere Präsentationen haben.

**Beispiel 21.4.**

1) $S_3$ hat die Präsentation $\langle x, y \mid x^2, y^2, (xy)^3 \rangle$.

2) $\mathbb{Z}_3$ hat folgende Präsentationen: $\langle x \mid x^3 \rangle$ und $\langle x, y \mid x^{-5}y^2,\ x^6y^{-3} \rangle$.

3) Sei $n \geqslant 2$ eine natürliche Zahl und sei $G$ die Untergruppe von $\mathrm{GL}_2(\mathbb{Q})$, die von

$$A = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

erzeugt ist. Dann hat $G$ die Präsentation $\langle a, b \mid a^{-1}bab^{-n} \rangle$.

**Satz 21.5** Sei $\varphi : F(X) \to G$ ein Epimorphismus und sei $R \subseteq F(X)$ eine Teilmenge. Wenn $\varphi(r) = 1$ für alle $r \in R$ gilt, dann ist die Abbildung

$$\begin{aligned} F(X)/R^{F(X)} &\to G \\ w \cdot R^{F(X)} &\mapsto \varphi(w) \end{aligned}$$

ein korrekt definierter Epimorphismus.

**Satz 21.6.** Die Gruppe $S_n$ hat die Präsentation.

$$\langle t_1, t_2, \ldots, t_{n-1} \mid t_i^2,\ \ t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1},\ \ t_i t_j = t_j t_i \,(|i-j|>1)\rangle.$$

Dabei entspricht das Symbol $t_i$ der Transposition $(i, i+1)$.

Eine Gruppe kann verschiedene Präsentationen haben. Aber von einer Präsentation zur anderen kann man mit Hilfe der Tietze-Transformationen gehen.

**Definition 21.7.**

(1) Tietze-Transformation des Typs 1:

$$\langle X \mid R\rangle \to \langle X \mid R \cup \{r\}\rangle,$$

wobei $r \in R^{F(X)}$ ist.

(2) Tietze-Transformation des Typs 2:

$$\langle X \mid R\rangle \to \langle X \cup \{y\} \mid R \cup \{y^{-1}w\}\rangle,$$

wobei $y \notin X^{\pm}$ und $w \in F(X)$ ist.

**Satz 21.8. (Tietze)** Seien $\langle X_1 \mid R_1\rangle$ und $\langle X_2 \mid R_2\rangle$ zwei endliche Präsentationen einer Gruppe $G$. Dann kann man die zweite Präsentation aus der ersten mit Hilfe endlicher Anwendungen der Tietze-Transformationen (1) und (2) und ihrer Inversen bekommen.

**Beispiel 21.9.**

1) $\langle x, y \mid xyx = yxy\rangle$ und $\langle a, b \mid a^2 = b^3\rangle$ präsentieren dieselbe Gruppe.
2) $\langle a, b \mid a^{-1}b^2a = b^3,\ b^{-1}a^2b = a^3\rangle$ und $\langle a, b \mid a, b\rangle$ sind zwei Präsentationen der trivialen Gruppe.

**Verabredung.** Wenn eine Gruppe $G$ eine Präsentation $\langle X \mid R\rangle$ hat, dann schreiben wir einfach $G = \langle X \mid R\rangle$.

# 22 Fundamentalgruppe eines topologischen Raumes

**Definition 22.1.**

Sei $X$ ein topologischer Raum. Ein *Weg* in $X$ ist eine stetige Abbildung $p : [0,1] \to X$. Die Punkte $p_- := p(0)$ und $p_+ := p(1)$ heißen *Anfangspunkt* und *Endpunkt* von $p$. Der *inverse* zu $p$ Weg $\overline{p}$ wird mit der Formel $\overline{p}(t) := p(1-t)$ für $t \in [0,1]$ definiert. Für $x \in X$ definieren wir den *trivialen* Weg $id_x$ mit der Formel $id_x(t) = x$ für $t \in [0,1]$.

Der Raum $X$ heißt *zusammenhängend*, falls keine Zerlegung $X = X_1 \coprod X_2$ mit offenen Mengen $X_1, X_2$ und $X_1 \cap X_2 = \varnothing$ existiert. Der Raum $X$ heißt *wegzusammenhängend*, falls für je zwei Punkte $x_1, x_2 \in X$ ein Weg $p$ in $X$ mit $p_- = x_1$ und $p_+ = x_2$ existiert. Der wegzusammenhängender Raum ist zusammenhängend. Es existieren zusammenhängende Räume, die nicht wegzusammenhängend sind.

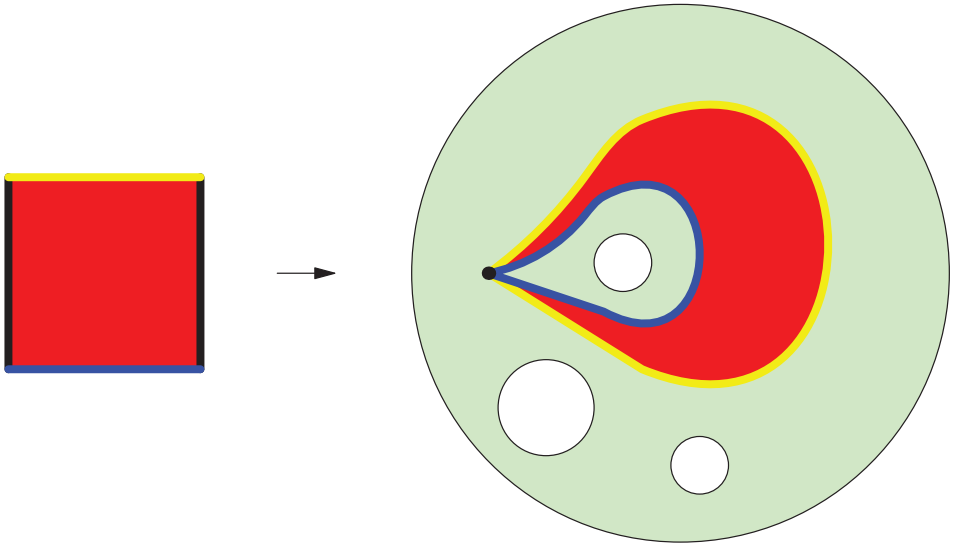
Seien $p$ und $q$ zwei Wege in $X$ mit $p_+ = q_-$. Dann wird ihr Produkt $p \cdot q$ mit der folgenden Formel definiert:

$$(p \cdot q)(t) = \begin{cases} p(2t), & \text{falls } 0 \leqslant t \leqslant \frac{1}{2}, \\ q(2t-1), & \text{falls } \frac{1}{2} \leqslant t \leqslant 1. \end{cases}$$

Zwei Wege $p, q$ in $X$ mit $p_- = q_-$ und $p_+ = q_+$ heißen *homotop*, falls eine stetige Abbildung $F : [0,1] \times [0,1] \to X$ existiert, so dass

$$F_{|[0,1]\times\{0\}}((t,0)) = p(t), \qquad F_{|[0,1]\times\{1\}}((t,1)) = q(t),$$
$$F_{|\{0\}\times[0,1]}((0,s)) = p_-, \qquad F_{|\{1\}\times[0,1]}((0,t)) = p_+$$

für alle $s, t \in [0,1]$ gilt. Die Äquivalenzklasse der Wege, die dem Weg $p$ homotop sind, wird mit $[p]$ bezeichnet.



**Definizion 22.2.** Sei $X$ ein wegzusammehängender topologischer Raum und sei $x$ ein ausgewählter Punkt in $X$. Die Menge

$$\pi_1(X,x) := \{[p] \,|\, p \text{ ist ein Weg in } X \text{ mit } p_- = p_+ = x\}$$

mit der Multiplikation $[p] \cdot [q] := [pq]$ ist eine Gruppe. Das zu $[p]$ inverse Element ist $[\overline{p}]$ und das neutrale Element ist $[id_x]$. Diese Gruppe heißt *Fundamentalgruppe* des Raumes $X$ bezüglich $x$.

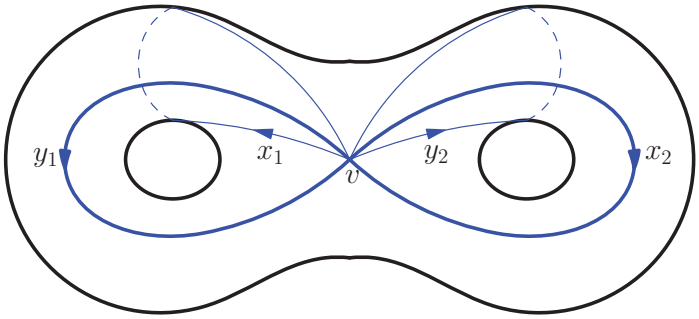
Zur Erinnerung: Wir benutzen die Bezeichnung $[a,b] := a^{-1}b^{-1}ab$.

**Beispiel 22.3.**

1) Sei $\mathcal{D}_n$ ein Disk mit $n$ "Disklöchern" und $v \in \mathcal{D}_n$ ein Punkt. Dann ist $\pi_1(\mathcal{D}_n, v) = F_n$, wobei $F_n$ eine freie Gruppe des Ranges $n$ ist.

2) Sei $T$ ein Torus und $v \in T$ ein Punkt. Dann ist $\pi_1(T, v) = \langle a, b \,|\, [a,b] \rangle$.

3) Sei $S_2$ die orientierbare Fläche des Geschlechts 2:




Dann ist $\pi_1(S_2, v) = \langle x_1, y_1, x_2, y_2 \,|\, [x_1, y_1][x_2, y_2] \rangle$.

4) Sei $S_g$ die orientierbare Fläche des Geschlechts $g$ und $v \in S_g$. Dann ist

$$\pi_1(S_g, v) = \langle x_1, y_1, \ldots, x_g, y_g \,|\, \prod_{i=1}^{g} [x_i, y_i] \rangle.$$

**Definition 22.4.** Seien $X$ und $Y$ topologische Räume. Eine Abbildung $f : X \to Y$ heißt *Homöomorphismus*, wenn $f$ ist bijektiv ist und beide Abbildungen $f$ und $f^{-1}$ stetig sind. Die Räume $X$ und $Y$ heißen *homöomorph*, wenn ein Homöomorphismus $f : X \to Y$ existiert.

**Satz 22.5.**

(a) Sei $X$ ein wegzusammenhängender topologischer Raum, seien $x, y \in X$ und sei $\ell$ ein Weg in $X$ mit $\ell_- = x$ und $\ell_+ = y$. Dann ist die Abbildung

$$\begin{aligned} \pi_1(X, x) &\to \pi_1(X, y) \\ [p] &\mapsto [\overline{\ell} p \ell] \end{aligned}$$

ein Isomorphismus.

(b) Seien $X, Y$ zwei wegzusammenhängende topologische Räume, sei $x \in X$. Jede stetige Abbildung $f : X \to Y$ induziert einen Homomorphismus

$$\begin{aligned} f_* : \ & \pi_1(X, x) \to \pi_1(Y, f(x)) \\ & [p] \mapsto [f \circ p]. \end{aligned}$$

Ist $f$ ein Homöomorphismus, dann ist $f_*$ ein Isomorphismus. Insbesondere haben homöomorphe topologische Räume isomorphe Fundamentalgruppen.

# 23 Fox-Calculus

**Definition 23.1.** Sei $G$ eine Gruppe. Wir betrachten die Menge aller endlichen formalen Summen $\sum'_{g\in G} n_g g$, wobei $n_g \in \mathbb{Z}$ ist. Die Endlichkeit bedeutet, dass alle Koeffizienten $n_g$ außer einer endlichen Anzahl gleich 0 sind.

Man kann zwei solcher Summen addieren und multiplizieren. Daraus entsteht ein Ring, der *Gruppenring* von $G$ heißt. Der Ring wird als $\mathbb{Z}G$ bezeichnet.

**Definition 23.2.** Sei $F = F(X)$ eine freie Gruppe mit der Basis $X$. Für jedes $x \in X$ definieren wir eine Fox-Ableitung

$$\frac{\partial}{\partial x} : F \to \mathbb{Z}F$$

nach der folgenden Regel:

$$\frac{\partial w}{\partial x} = u_1 + \cdots + u_k - x^{-1}v_1 - \cdots - x^{-1}v_s,$$

wobei $u_1, \ldots, u_k$ die Unterworte von $w$ sind, die nach Auftreten von $x$ in $w$ stehen, und $v_1, \ldots, v_s$ die Unterworte von $w$ sind, die nach Auftreten von $x^{-1}$ in $w$ stehen. Das leere Unterwort wird mit $e$ identifiziert. Wenn $w$ keinen der Buchstaben $x$ und $x^{-1}$ enthält, dann ist $\dfrac{\partial w}{\partial x} = 0$.

**Beispiel 23.3.**

1) $\frac{\partial}{\partial x}(x^{-1}y^{-1}xy) = y - x^{-1}y^{-1}xy$,

2) $\frac{\partial}{\partial y}(x^{-1}y^{-1}xy) = e - y^{-1}xy$,

3) $\frac{\partial}{\partial x}(x^n) = e + x + \cdots + x^{n-1}$.

**Behauptung 23.4.** Seien $x, y \in X$ und $u, v \in F$. Dann gelten die Formeln

1)
$$\frac{\partial y}{\partial x} = \begin{cases} e, & \text{wenn } x = y \text{ ist,} \\ 0, & \text{wenn } x \neq y \text{ ist,} \end{cases}$$

2)
$$\frac{\partial}{\partial x}(x^{-1}) = -x^{-1},$$

3)
$$\frac{\partial}{\partial x}(uv) = \frac{\partial u}{\partial x}v + \frac{\partial v}{\partial x},$$

4)
$$\frac{\partial}{\partial x}(u^{-1}) = -\frac{\partial u}{\partial x} \cdot u^{-1}.$$

**Satz 23.5. (Kettenregel)** Seien $v_1, \ldots, v_k \in F(X)$ und sei $w = w(v_1, \ldots, v_k)$ ein Wort von $v_1, \ldots, v_k$. Dann gilt

$$\frac{\partial w}{\partial x} = \sum_{i=1}^{k} \frac{\partial v_i}{\partial x} \cdot \frac{\partial w}{\partial v_i}$$

für alle $x \in X$.

**Satz 23.6. (Taylor-Formel)** Für alle $w \in F(x_1, \ldots, x_n)$ gilt

$$w - e = \sum_{i=1}^{n} (x_i - e) \cdot \frac{\partial w}{\partial x_i}.$$

# 24 Fundamentalgruppe eines Knotens. Wirtinger-Präsentation

**Definition 24.1.**

1) Ein zahmer *Knoten* in $\mathbb{R}^3$ ist das Bild einer injektiven und unendlich differenzierbaren Abbildung von dem Kreis $\{e^{i\varphi} \mid 0 \leqslant \varphi < 2\pi\}$ in $\mathbb{R}^3$.
2) Die *Fundamentalgruppe des Knotens* $K \subset \mathbb{R}^3$ ist $\pi_1(\mathbb{R}^3 \setminus K, x)$.
3) Zwei Knoten $K_1, K_2$ heißen *äquivalent*, falls ein Homöomorphismus $\varphi : (\mathbb{R}^3 \setminus K_1) \to (\mathbb{R}^3 \setminus K_2)$ existiert.

**Folgerung 24.2.** Äquivalente Knoten haben isomorphe Fundamentalgruppen.

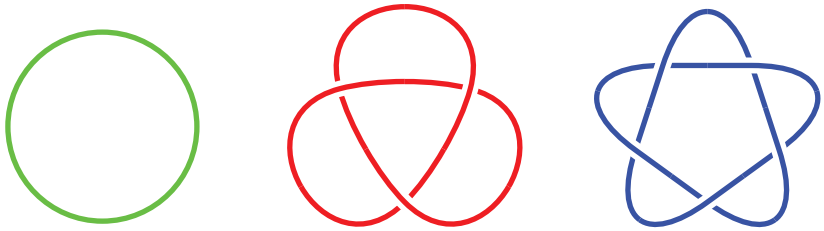
Beginnend mit den Abschnitten 25 und 26 wird eine Methode entwickelt, die oft ermöglicht zu zeigen, dass zwei Präsentationen nicht isomorphe Gruppen bestimmen.

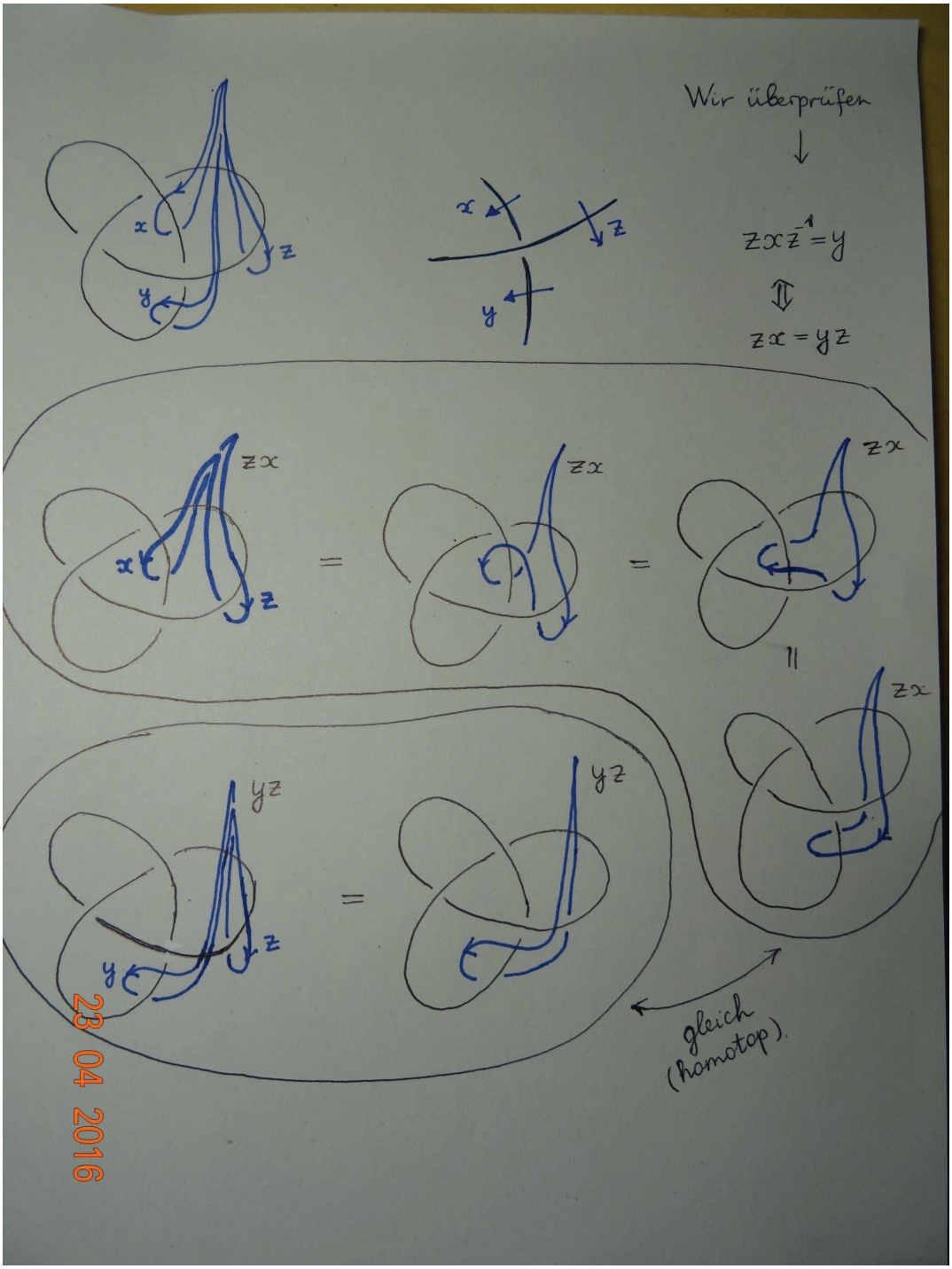
**Satz 24.3. (Wirtinger)**

1) Gegeben ein zahmer Knoten $K$ durch seine Projektion, dann kann man eine Präsentation seiner Fundamentalgruppe $G = \pi_1(\mathbb{R}^3 \setminus K, x)$ algorithmisch aufschreiben.
2) Es gilt $G/[G, G] \cong \mathbb{Z}$.

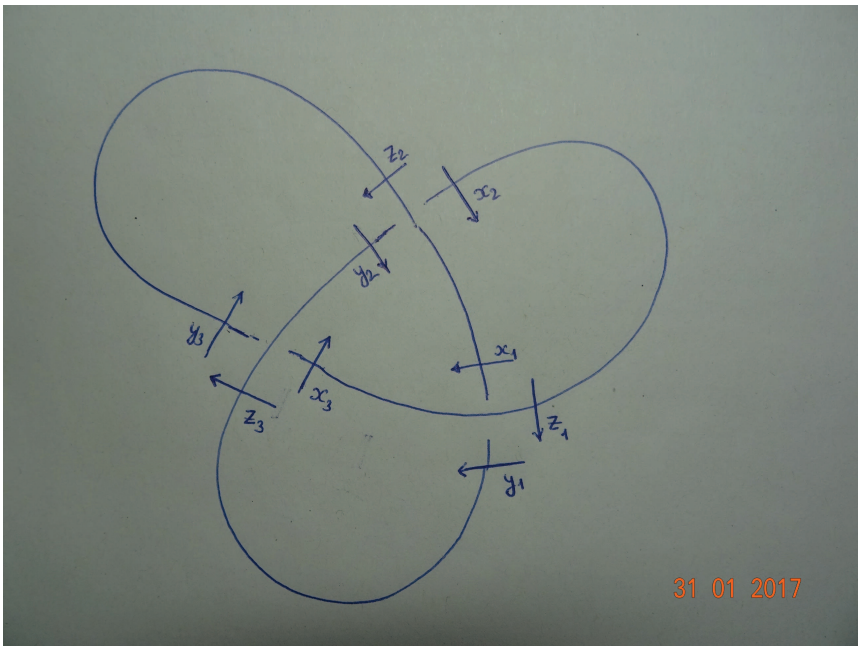
**Beispiel.** Der Kleeblattknoten (Mitte unten) kann folgendermaßen parameterisiert werden:

$$x = (2 + \cos(3t))\cos(2t), \quad y = (2 + \cos(3t))\sin(2t), \quad z = \sin(3t), \qquad t \in [0, 2\pi).$$






Diese Abbildung zeigt, dass die Homotopieklassen von Wegen $zxz^{-1}$ und $y$ gleich sind.




Erzeuger von $\pi_1(\mathbb{R}^3 \setminus K)$: $\{x_i, y_i, z_i \,|\, i = 1, 2, 3\}$.
Relationen:

$$\begin{aligned} x_3 &= z_1^{-1} &&= x_2, \\ y_1 &= z_3^{-1} &&= y_2, \\ x_1 &= z_2 &&= y_2, \end{aligned}$$

und

$$\begin{aligned} z_1 x_1 z_1^{-1} &= y_1, \\ z_2 x_2 z_2^{-1} &= y_2, \\ z_3 x_3 z_3^{-1} &= y_3. \end{aligned}$$

Tietze-Transformationen ermöglichen, $x_i, y_i, z_i$ mit $i \geqslant 2$ und danach noch $z_1$ zu eliminieren und die Relationen zu vereinfachen:

$$\pi_1(\mathbb{R}^3 \setminus K) = \langle x_1, y_1 \,|\, x_1 y_1 x_1 = y_1 x_1 y_1 \rangle.$$

Diese Gruppe ist nicht abelsch, weil es folgenden Epimorphismus gibt:

$$\begin{aligned} \pi_1(\mathbb{R}^3 \setminus K) &\to S_3 \\ x_1 &\mapsto (12), \\ y_1 &\mapsto (13). \end{aligned}$$

Die Fundamentalgruppe des trivialen Knotens (links auf Seite 32) ist aber $\mathbb{Z}$. Deswegen ist $K$ nicht zu dem trivialen Knoten äquivalent.

# 25 Matrizen von Präsentationen

**Definition 25.1.** Sei $\mathcal{P} = \langle x_1, \dots, x_n \,|\, r_1, \dots, r_m \rangle$ eine Präsentation. Sei $H = F/R^F$, wobei $F := F(x_1, \dots, x_n)$ und $R := \{r_1, \dots, r_m\}$ ist. Der natürliche Gruppenhomomorphismus $\theta_{\mathcal{P}} : F \to H$ kann bis zum Ringhomomorphismus $\theta^*_{\mathcal{P}} : \mathbb{Z}F \to \mathbb{Z}H$ fortgesetzt werden. Die *Matrix* der Präsentation $\mathcal{P}$ ist dann die Matrix

$$M(\mathcal{P}) = \begin{pmatrix} \theta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_1}) & \dots & \theta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_1}) \\ \vdots & & \vdots \\ \theta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_n}) & \dots & \theta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_n}) \end{pmatrix}.$$

Somit ist

$$M(\mathcal{P}) \in \mathrm{Mat}(n, m, \mathbb{Z}H).$$

Wir wissen, dass eine Gruppe $G$ verschiedene Präsentationen haben kann. Wenn $G$ endlich präsentierbar ist, dann sind endliche Präsentationen von $G$ miteinander durch endliche Ketten von Tietze-Transformationen verbunden. In den nächsten zwei Sätzen untersuchen wir, wie die Tietze-Transformationen auf die Matrizen von Präsentationen wirken.

**Satz 25.2.** Sei $\mathcal{P} = \langle x_1, \dots, x_n \,|\, r_1, \dots, r_m \rangle$ eine Präsentation und $H = F/R^F$ wie oben. Wir betrachten eine Tietze-Transformation des Typs (1):

$$\mathcal{P} = \langle x_1, \dots, x_n \,|\, r_1, \dots, r_m \rangle \to \mathcal{P}' = \langle x_1, \dots, x_n \,|\, r_1, \dots, r_m, r \rangle$$

und die entsprechende Transformation von assoziierten Matrizen:

$$M(\mathcal{P}) = \begin{pmatrix} \theta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_1}) & \dots & \theta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_1}) \\ \vdots & & \vdots \\ \theta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_n}) & \dots & \theta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_n}) \end{pmatrix} \to M(\mathcal{P}') = \begin{pmatrix} \theta^*_{\mathcal{P}'}(\frac{\partial r_1}{\partial x_1}) & \dots & \theta^*_{\mathcal{P}'}(\frac{\partial r_m}{\partial x_1}) & \theta^*_{\mathcal{P}'}(\frac{\partial r}{\partial x_1}) \\ \vdots & & & \vdots \\ \theta^*_{\mathcal{P}'}(\frac{\partial r_1}{\partial x_n}) & \dots & \theta^*_{\mathcal{P}'}(\frac{\partial r_m}{\partial x_n}) & \theta^*_{\mathcal{P}'}(\frac{\partial r}{\partial x_n}) \end{pmatrix}.$$

Dann gelten:

- $\theta_{\mathcal{P}} = \theta_{\mathcal{P}'}$. Insbesondere gilt $\theta^*_{\mathcal{P}} = \theta^*_{\mathcal{P}'}$.
- Die ersten $m$ Spalten von $M(\mathcal{P})$ und $M(\mathcal{P}')$ sind gleich.
- Die letzte Spalte der Matrix $M(\mathcal{P}')$ ist eine lineare Kombination der Spalten von Matrix $M(\mathcal{P})$ mit Koeffizienten aus $\mathbb{Z}H$.

Genauer: es existieren $c_1, \dots, c_m \in \mathbb{Z}H$, so dass das Folgende gilt:

$$\begin{pmatrix} \theta^*_{\mathcal{P}'}(\frac{\partial r}{\partial x_1}) \\ \vdots \\ \theta^*_{\mathcal{P}'}(\frac{\partial r}{\partial x_n}) \end{pmatrix} = \begin{pmatrix} \theta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_1}) \\ \vdots \\ \theta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_n}) \end{pmatrix} \cdot c_1 + \dots + \begin{pmatrix} \theta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_1}) \\ \vdots \\ \theta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_n}) \end{pmatrix} \cdot c_m.$$

Bevor wir die zweite Tietze-Transformation analysieren, formulieren wir eine Behauptung, um zu verstehen, wie $\theta_{\mathcal{P}'}$ und $\theta_{\mathcal{P}}$ miteinander verbunden sind, wenn $\mathcal{P}'$ eine Erweiterung von $\mathcal{P}$ ist.

**Behauptung.** Seien $\mathcal{P} = \langle X \,|\, R\rangle$ und $\mathcal{P}' = \langle X' \,|\, R'\rangle$ zwei Präsentationen von (möglicherweise verschiedenen) Gruppen, so dass $X \subseteq X'$ und $R \subseteq R'$ gilt. Wir betrachten folgende Kette von Homomorphismen:

$$\begin{array}{ccccc} F(X) & \overset{\theta_{\mathcal{P}}}{\to} & F(X)/R^{F(X)} & \overset{i_{\mathcal{P},\mathcal{P}'}}{\to} & F(X')/R'^{F(X')} \\ f & \mapsto & f \cdot R^{F(X)} & \mapsto & f \cdot R'^{F(X')}. \end{array}$$

Daraus folgt $\theta_{\mathcal{P}'}(f) = (i_{\mathcal{P},\mathcal{P}'} \circ \theta_{\mathcal{P}})(f)$ für $f \in F(X)$.

**Satz 25.3.** Sei $G$ eine Gruppe mit der Präsentation $\mathcal{P} = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m\rangle$. Wir betrachten eine Tietze-Transformation des Typs (2):

$$\mathcal{P} = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m\rangle \to \mathcal{P}' = \langle x_1, \ldots, x_n, y \,|\, r_1, \ldots, r_m, y^{-1}w\rangle.$$

Dann sieht die entsprechende Transformation von assoziierten Matrizen so aus:

$$M(\mathcal{P}) = \begin{pmatrix} \theta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_1}) & \ldots & \theta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_1}) \\ \vdots & & \vdots \\ \theta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_n}) & \ldots & \theta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_n}) \end{pmatrix} \to M(\mathcal{P}') = \begin{pmatrix} \theta^*_{\mathcal{P}'}(\frac{\partial r_1}{\partial x_1}) & \ldots & \theta^*_{\mathcal{P}'}(\frac{\partial r_m}{\partial x_1}) & \star \\ \vdots & & & \vdots \\ \theta^*_{\mathcal{P}'}(\frac{\partial r_1}{\partial x_n}) & \ldots & \theta^*_{\mathcal{P}'}(\frac{\partial r_m}{\partial x_n}) & \star \\ 0 & & 0 & -e \end{pmatrix}.$$

# 26 Laurent-Polynome

**Definition 26.1.** Der Ring von *Laurent-Polynomen* von $t, t^{-1}$ ist der Ring

$$\mathbb{Z}[t, t^{-1}] := \{\sum_{i=n}^{m} a_i t^i \,|\, a_i \in \mathbb{Z}; n, m \in \mathbb{Z}, n \leqslant m\}.$$

bezüglich der natürlichen Addition und Multiplikation.

Jedes nichtnullsche Element $f$ aus $\mathbb{Z}[t, t^{-1}]$ kann eindeutig in der Form $f = f_1/t^p$ mit $p \in \mathbb{Z}$ geschrieben werden, wobei $f_1 = a_s t^s + a_{s-1}t^{s-1} + \cdots + a_0$ ein Polynom aus $\mathbb{Z}[t]$ mit $a_0 \neq 0$ ist. Diese Form heißt *kanonische Form* von $f$.

**Definition 26.2.** Seien $f, g$ zwei nichtnullsche Elemente aus $\mathbb{Z}[t, t^{-1}]$. Wir schreiben sie in der kanonischen Form: $f = f_1/t^p$ und $g = g_1/t^q$ und setzen

$$\mathrm{ggT}(f, g) := \mathrm{ggT}(f_1, g_1).$$

Wenn $f = 0$ und $g \neq 0$ ist, dann setzen wir

$$\mathrm{ggT}(f, g) := \mathrm{ggT}(0, g_1) := g_1.$$

**Bezeichnung $\mathcal{Z}$.** In Weiterem benutzen wir auch die multiplikative Schreibweise für die Gruppe $(\mathbb{Z}, +)$. Also benutzen wir die Gruppe $\mathcal{Z} := \{t^i \,|\, i \in \mathbb{Z}\}$ mit der Multiplikation $t^i \cdot t^j = t^{i+j}$. Es ist klar, dass $(\mathcal{Z}, \cdot) \cong (\mathbb{Z}, +)$ gilt. Wir bezeichnen $\mathbf{1} := t^0$. Die Gruppe $\mathcal{Z}$ besitzt einen nichttrivialen Automorphismus

$$\begin{array}{rl} \mathbf{Inv} : \mathcal{Z} & \to \mathcal{Z} \\ t & \mapsto t^{-1}. \end{array}$$

**Bemerkung 26.3.** Der Gruppenring $\mathbb{Z}\mathcal{Z}$ ist gleich dem Ring $\mathbb{Z}[t, t^{-1}]$.
Der Gruppenautomorphismus $\mathbf{Inv} : \mathcal{Z} \to \mathcal{Z}$ kann bis zum Ringautomorphismus

$$\mathbf{Inv}^* : \mathbb{Z}[t, t^{-1}] \to \mathbb{Z}[t, t^{-1}]$$

fortgesetzt werden.

**Definition 26.4.** Sei $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$ ein Polynom aus $\mathbb{Z}[t]$.

(a) Das Polynom $g(t) = a_0 t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n$ heißt *gespiegeltes* zu $f(t)$. In diesem Fall schreiben wir $g(t) = \mathbf{Sp}(f(t))$.

(b) Ein Polynom $f(x)$ heißt *palindromisch*, wenn $f(t) = \mathbf{Sp}(f(t))$ ist.

**Lemma 26.5.** Für $f, g \in \mathbb{Z}[t, t^{-1}]$ gilt:

$$\mathrm{ggT}(\mathbf{Inv}^*(f), \mathbf{Inv}^*(g)) = \mathbf{Sp}(\mathrm{ggT}(f, g)).$$

**Beispiel.** Seien $f = 3t^5 + 2t^3$ und $g = -3t^2 + 3t - 2 + 2t^{-1}$.

(a) Die kanonischen Formen von $f$ und $g$ sind

$$f = \frac{3t^2 + 2}{t^{-3}}, \quad g = \frac{-3t^3 + 3t^2 - 2t + 2}{t}.$$

Deswegen gilt

$$\begin{aligned} ggT(f, g) &= ggT(3t^2 + 2, -3t^3 + 3t^2 - 2t + 2) \\ &= ggT(3t^2 + 2, (3t^2 + 2)(t - 1)) \\ &= 3t^2 + 2. \end{aligned}$$

(b) Wir haben $\mathbf{Inv}^*(f) = 3t^{-2} + 2$ und $\mathbf{Inv}^*(g) = -3t^{-2} + 3t^{-1} - 2 + 2t$.
Die entsprechenden kanonischen Formen sind:

$$\mathbf{Inv}^*(f) = \frac{3 + 2t^2}{t^2}, \quad \mathbf{Inv}^*(g) = \frac{-3 + 3t - 2t^2 + 2t^3}{t^2}.$$

Deswegen gilt

$$\begin{aligned} ggt(\mathbf{Inv}^*(f), \mathbf{Inv}^*(g)) &= ggT(3 + 2t^2, -3 + 3t - 2t^2 + 2t^3) \\ &= ggT(3 + 2t^2, (3 + 2t^2)(-1 + t)) \\ &= 3 + 2t^2. \end{aligned}$$

# 27 Alexander-Polynome von Gruppen $G$ mit der Eigenschaft $G/[G,G] \cong \mathbb{Z}$

**Lemma 27.1.** Jedes Epimorphismus $\theta : \mathcal{Z} \to \mathcal{Z}$ ist ein Isomorphismus. Insbesondere gilt $\theta \in \{id, \mathbf{Inv}\}$.

**Lemma 27.2.** Sei $G$ eine beliebige Gruppe mit der Präsentation $\mathcal{P} = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m \rangle$. Dann gilt:

(a) Die Gruppe $G/[G,G]$ hat die Präsentation

$$\mathcal{P}_{ab} = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m, [x_i, x_j],\ \ i,j \in \{1, \ldots, n\} \rangle.$$

(b) Angenommen $G/[G,G] \cong \mathcal{Z}$. Dann existieren genau zwei Epimorphismen

$$\delta : F(x_1, \ldots, x_n) \to \mathcal{Z} \quad \text{mit der Eigenschaft} \quad \delta(r_1) = \cdots = \delta(r_m) = \mathbf{1}.$$

Wir bezeichnen diese Epimorphismen mit $\delta_{\mathcal{P}_{ab},1}$ und $\delta_{\mathcal{P},2}$. Dann gilt

$$\delta_{\mathcal{P},2} = \mathbf{Inv} \circ \delta_{\mathcal{P},1}.$$

*Beweis.* (a) ist klar.

(b) Wir schreiben kurz $\mathcal{P}_{ab} = \langle X \,|\, R \rangle$ und benutzen der kanonische Epimorphismus

$$\pi : F \to F/R^F.$$

Nach (a) ist $\mathcal{P}_{ab}$ eine Präsentation von $\mathcal{Z}$. Dann existiert ein Isomorphismus

$$\varphi : F/R^F \to \mathcal{Z}.$$

Dann gilt die Komposition $\varphi \circ \pi$ als $\delta$. Als zweites $\delta$ gilt die Komposition $\mathbf{Inv} \circ \delta$.

Nun sei $\delta : F \to \mathcal{Z}$ ein beliebiger Epimorphismus mit der Eigenschaft $\delta(r) = 1$ für alle $r \in R$. Nach Satz 21.5 existiert ein Epimorphismus

$$\psi : F/R^F \to \mathcal{Z},$$

so dass $\delta = \psi \circ \pi$ ist. Merken wir an, dass $\psi \circ \varphi^{-1} : \mathcal{Z} \to \mathcal{Z}$ ein Epimorphismus ist. Dann ist $\psi = \varphi$ oder $\psi = \mathbf{Inv} \circ \varphi$ nach Lemma 26.3. Das gibt zwei Varianten für $\delta$, die wir schon oben hatten. □

**Beispiel 27.3.** Sei $G$ eine Gruppe mit der Präsentation

$$\mathcal{P} = \langle x_1, x_2 \,|\, x_1^{-1} x_2^2 x_1 x_2^{-3} \rangle.$$

Man kann überprüfen, dass $G/[G,G] \cong \mathcal{Z}$ ist. Wir suchen einen Epimorphismus $\delta : F(x_1, x_2) \to \mathcal{Z}$, so dass gilt:

$$\delta(x_1^{-1} x_2^2 x_1 x_2^{-3}) = \mathbf{1}.$$

Sei $\delta(x_i) = t^{k_i}$, $i = 1, 2$. Dann erhalten wir $k_2 = 0$. Da $\delta$ ein Epimorphismus sein soll, gilt

$$\mathbb{Z} = \langle k_1, k_2 \rangle = \langle k_1 \rangle.$$

Also haben wir zwei Lösungen: $(k_1, k_2) = (1, 0)$ und $(k_1, k_2) = (-1, 0)$. Entsprechend ist

$$\delta_{\mathcal{P},1}(x_1) = t, \quad \delta_{\mathcal{P},1}(x_2) = \mathbf{1}$$

oder

$$\delta_{\mathcal{P},2}(x_1) = t^{-1}, \quad \delta_{\mathcal{P},2}(x_2) = \mathbf{1}.$$

**Lemma 27.4.** Sei $G$ eine Gruppe und sei $\mathcal{P} = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m \rangle$ eine Präsentation von $G$. Dann ist die minimale Anzahl der Erzeuger von $G/[G, G]$ mindestens $n - m$. Insbesondere gilt: Ist $G/[G, G] \cong \mathcal{Z}$, dann ist $m \geqslant n - 1$.

**Definition 27.5. (Alexander-Matrix und Alexander-Polynom)**
Sei $G$ eine Gruppe mit der Eigenschaft $G/[G, G] \cong \mathcal{Z}$. Sei $\mathcal{P} = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m \rangle$ eine Präsentation von $G$. Wir wählen einen von zwei Gruppenhomomorphismen $\delta_{\mathcal{P}} : F \to \mathcal{Z}$ (siehe Lemma 26.4 (b)). Der Gruppenhomomorphismus $\delta_{\mathcal{P}}$ kann bis zum Ringhomomorphismus $\delta^*_{\mathcal{P}} : \mathbb{Z}F \to \mathbb{Z}\mathcal{Z}$ fortgesetzt werden. Die *Alexander-Matrix* der Präsentation $\mathcal{P}$ ist dann die Matrix

$$AlexMat(\mathcal{P}) = \begin{pmatrix} \delta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_1}) & \ldots & \delta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_1}) \\ \vdots & & \vdots \\ \delta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_n}) & \ldots & \delta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_n}) \end{pmatrix} \in \mathrm{Mat}(n, m, \mathbb{Z}\mathcal{Z}).$$

Das Alexander-Polynom $AlexPol(\mathcal{P})$ der Präsentation $\mathcal{P}$ ist dann gleich dem ggT der Determinanten aller $(n-1) \times (n-1)$-Untermatrizen dieser Matrix.

**Fortsetzung des Beispiels 27.3.** Wir haben $r_1 = x_1^{-1} x_2^2 x_1 x_2^{-3}$. Dann gilt

$$\begin{aligned} \tfrac{\partial r_1}{\partial x_1} &= -x_1^{-1} x_2^2 x_1 x_2^{-3} + x_2^{-3}, \\ \tfrac{\partial r_1}{\partial x_2} &= x_2 x_1 x_2^{-3} + x_1 x_2^{-3} - x_2^{-3} - x_2^{-2} - x_2^{-1}. \end{aligned}$$

Wir wählen

$$\delta_{\mathcal{P}}(x_1) = t, \quad \delta_{\mathcal{P}}(x_2) = \mathbf{1}.$$

Dann gilt

$$AlexMat(\mathcal{P}) = \begin{pmatrix} 0 \\ \\ 2t - 3 \end{pmatrix} \in \mathrm{Mat}\ (2, 1, \mathbb{Z}\mathcal{Z}).$$

Hier ist $n = 2$. Deswegen ist das *Alexander-Polynom* von $\mathcal{P}$ gleich dem ggT der Determinanten aller $1 \times 1$-Untermatrizen dieser Matrix:

$$AlexPol(\mathcal{P}) = \mathrm{ggT}(0, 2t - 3) = 2t - 3.$$

**Satz 27.6.** Sei $G$ eine endlich präsentierbare Gruppe mit der Eigenschaft $G/[G,G] \cong \mathcal{Z}$. Sei $\mathcal{P} = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m \rangle$ eine Präsentation von $G$. Dann gilt:

(a) $AlexPol(\mathcal{P})$ ist eindeutig bis auf die Spiegelung.

(b) $AlexPol(\mathcal{P})$ hängt von der Wahl einer endlichen Präsentation $\mathcal{P}$ der Gruppe $G$ nicht ab. Deswegen wird es einfach mit $AlexPol(G)$ bezeichnet.

(c) Ist $G$ die Fundamentalgruppe eines Knotens, dann ist das Alexander-Polynom von $G$ palindromisch.

*Beweis.*

(a) folgt aus Lemmata 25.5 und 27.2 (b).

(b) folgt aus zwei Lemmata 27.7 und 27.8, die völlig analog den Sätzen 25.2 und 25.3 bewiesen werden können.

(c) ist kompliziert und benutzt topologische Überlegungen. □

**Lemma 27.7.** Sei $G$ eine Gruppe mit der Eigenschaft $G/[G,G] \cong \mathcal{Z}$. Sei $\mathcal{P} = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m \rangle$ eine Präsentation von $G$. Wir betrachten eine Tietze-Transformation des Typs (1):

$$\mathcal{P} = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m \rangle \to \mathcal{P}' = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m, r \rangle$$

und die entsprechende Transformation von assoziierten Matrizen:

$$AlexMat(\mathcal{P}) = \begin{pmatrix} \delta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_1}) & \ldots & \delta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_1}) \\ \vdots & & \vdots \\ \delta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_n}) & \ldots & \delta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_n}) \end{pmatrix} \to AlexMat(\mathcal{P}') = \begin{pmatrix} \delta^*_{\mathcal{P}'}(\frac{\partial r_1}{\partial x_1}) & \ldots & \delta^*_{\mathcal{P}'}(\frac{\partial r_m}{\partial x_1}) & \delta^*_{\mathcal{P}'}(\frac{\partial r}{\partial x_1}) \\ \vdots & & & \vdots \\ \delta^*_{\mathcal{P}'}(\frac{\partial r_1}{\partial x_n}) & \ldots & \delta^*_{\mathcal{P}'}(\frac{\partial r_m}{\partial x_n}) & \delta^*_{\mathcal{P}'}(\frac{\partial r}{\partial x_n}) \end{pmatrix}.$$

Wir können $\delta_{\mathcal{P}'}$ so wählen, dass $\delta_{\mathcal{P}} = \delta_{\mathcal{P}'}$ gilt. Dann wird gelten:

- $\delta^*_{\mathcal{P}} = \delta^*_{\mathcal{P}'}$.
- Die ersten $m$ Spalten von $M(\mathcal{P})$ und $M(\mathcal{P}')$ sind gleich.
- Die letzte Spalte der Matrix $M(\mathcal{P}')$ ist eine lineare Kombination der Spalten von Matrix $M(\mathcal{P})$ mit Koeffizienten aus $\mathbb{Z}\mathcal{Z} = \mathbb{Z}[t, t^{-1}]$.

Genauer: es existieren $c_1, \ldots, c_m \in \mathbb{Z}\mathcal{Z}$, so dass das Folgende gilt:

$$\begin{pmatrix} \delta^*_{\mathcal{P}'}(\frac{\partial r}{\partial x_1}) \\ \vdots \\ \delta^*_{\mathcal{P}'}(\frac{\partial r}{\partial x_n}) \end{pmatrix} = \begin{pmatrix} \delta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_1}) \\ \vdots \\ \delta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_n}) \end{pmatrix} \cdot c_1 + \cdots + \begin{pmatrix} \delta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_1}) \\ \vdots \\ \delta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_n}) \end{pmatrix} \cdot c_m.$$

**Lemma 27.8.** Sei $G$ eine Gruppe mit der Eigenschaft $G/[G,G] \cong \mathcal{Z}$. Sei $\mathcal{P} = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m \rangle$ eine Präsentation von $G$. Wir betrachten eine Tietze-Transformation des Typs (2):

$$\mathcal{P} = \langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m \rangle \to \mathcal{P}' = \langle x_1, \ldots, x_n, y \,|\, r_1, \ldots, r_m, y^{-1}w \rangle.$$

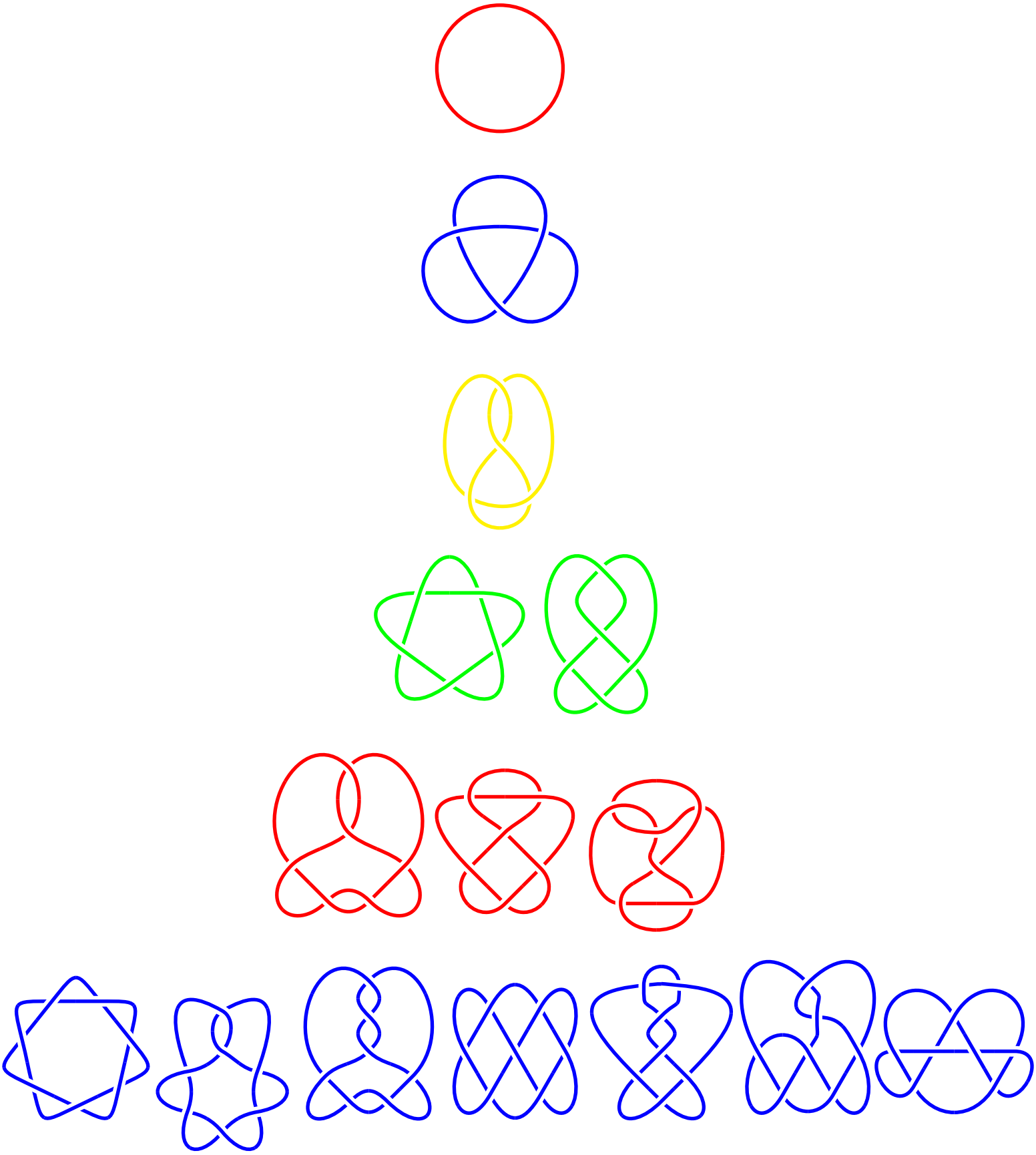
Dann sieht die entsprechende Transformation von assoziierten Matrizen so aus:

$$AlexMat(\mathcal{P}) = \begin{pmatrix} \delta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_1}) & \ldots & \delta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_1}) \\ \vdots & & \vdots \\ \delta^*_{\mathcal{P}}(\frac{\partial r_1}{\partial x_n}) & \ldots & \delta^*_{\mathcal{P}}(\frac{\partial r_m}{\partial x_n}) \end{pmatrix} \to AlexMat(\mathcal{P}') = \begin{pmatrix} \delta^*_{\mathcal{P}'}(\frac{\partial r_1}{\partial x_1}) & \ldots & \delta^*_{\mathcal{P}'}(\frac{\partial r_m}{\partial x_1}) & \star \\ \vdots & & & \vdots \\ \delta^*_{\mathcal{P}'}(\frac{\partial r_1}{\partial x_n}) & \ldots & \delta^*_{\mathcal{P}'}(\frac{\partial r_m}{\partial x_n}) & \star \\ 0 & & 0 & \mathbf{-1} \end{pmatrix}.$$

Dabei kann $\delta_{\mathcal{P}'}$ so gewählt werden, dass $\delta_{\mathcal{P}}(u) = \delta_{\mathcal{P}'}(u)$ für alle $u \in F(x_1, \ldots, x_n)$ gilt.

**Definition. 27.9.** Das Alexander-Polynom eines Knotens $K$ ist das Alexander-Polynom der Gruppe $G = \pi_1(\mathbb{R}^3 \setminus K)$.

**Korollar 27.10.** Äquivalente Knoten haben gleiche Alexander-Polynome. Insbesondere sind Knoten auf dem folgenden Bild paarweise nicht äquivalent.



# 28 Der Umschreibungs-Prozess von Reidemeister-Schreier

Sei $G$ eine Gruppe und $G_1$ eine Untergruppe von $G$. Es wird erklärt, wie man eine Präsentation von $G_1$ aus einer Präsentation von $G$ ableiten kann.

**Definition 28.1.** Sei $F = F(X)$ eine freie Gruppe mit der Basis $X$ und sei $H$ eine Untergruppe von $F$. Eine Teilmenge $T \subseteq F$ heißt *Menge von Schreier-Repräsentanten der rechten Nebenklassen von $H$ in $F$* (oder rechte *Schreier-Transversal von $H$ in $G$*), falls:

1) $1 \in T$;
2) in jeder rechten Nebenklasse $Hg$ gibt es genau ein Element aus $T$;
3) jedes Anfangssegment eines jeden Elements $t \in T$ wieder in $T$ liegt:
   wenn $t = x_1 x_2 \dots x_n \in T$ mit $x_1, \dots, x_n \in X \cup X^{-1}$ ist, dann ist $x_1$, $x_1 x_2$, $x_1 x_2 x_3, \dots \in T$.

**Bezeichnungen.**

1) Für $g \in F$ sei $\overline{g}$ das Element von $T$ mit $Hg = H\overline{g}$.
   Wir haben die folgenden Eigenschaften:
   a) $Hg_1 = Hg_2 \Leftrightarrow \overline{g_1} = \overline{g_2}$,
   b) $\overline{\overline{g}} = \overline{g}$,
   c) $\overline{\overline{g}f} = \overline{gf}$.
2) Für $t \in T$ und $x \in X \cup X^{-1}$ bezeichnen wir $\gamma(t,x) := tx\big(\overline{tx}\,\big)^{-1}$.
   Es ist klar, dass das Folgende gilt:
   a) $\gamma(t,x) \in H$;
   b) $\gamma(t,x^{-1}) = \gamma(\overline{tx^{-1}},x)^{-1}$.

**Satz 28.2.** Sei $F = F(X)$ eine freie Gruppe, sei $H \leqslant F$ und sei $T$ eine Menge von Schreier-Repräsentanten der rechten Nebenklassen von $H$ in $F$. Dann gilt:
1) Jedes Element $h \in H$ kann als ein Produkt von Elementen der Form $\gamma(t,x)$ dargestellt werden: Wenn

$$\begin{aligned} h = &\ x_1 x_2 \dots x_n \text{ mit } x_i \in X \cup X^{-1} \text{ ist, dann ist} \\ h = &\ \gamma(1,x_1)\cdot\gamma(\overline{x_1},x_2)\cdot\gamma(\overline{x_1x_2},x_3)\cdot\ldots\cdot\gamma(\overline{x_1x_2\dots x_{n-1}},x_n). \end{aligned}$$

2) $H$ ist eine freie Gruppe mit der Basis

$$Y := \{\gamma(t,x) \mid t \in T, x \in X,\ \gamma(t,x) \neq 1\}.$$

**Bezeichnung.** Nach dem Satz kann jedes $h \in H$ eindeutig als gekürztes Wort in dem Alphabet $Y \cup Y^{-1}$ geschrieben werden. Das Wort wird mit $\tau(h)$ bezeichnet.

**Satz 28.3.** Sei $G$ eine Gruppe mit der Präsentation $\langle X \mid R\rangle$ und $G_1$ eine Untergruppe von $G$. Sei $\varphi : F(X) \to G$ der kanonische Epimorphismus und $H = \varphi^{-1}(G_1)$ das volle Urbild von $G_1$ in $F(X)$ bezüglich $\varphi$. Sei $T$ eine Menge von Schreier-Repräsentanten der rechten Nebenklassen von $H$ in $F(X)$. Dann hat $G_1$ die Präsentation

$$\langle Y \mid S\rangle,$$

wobei $Y$ im Satz 28.2 definiert ist und $S := \{\tau(trt^{-1}) \mid t \in T, r \in R\}$ ist.

**Korollar 28.4.** Jede Untergruppe von endlichem Index in einer endlich präsentierbaren (endlich erzeugten) Gruppe ist endlich präsentierbar (endlich erzeugt).

**Beispiel 28.5.** Sei $G$ eine Gruppe mit der Präsentation $\langle a, b \mid a^2 = b^3\rangle$. Wir können annehmen, dass $G = F(a, b)/N$ ist, wobei $N = \{b^3a^{-2}\}^{F(a,b)}$ ist.

Wir definieren eine Untergruppe $G_1$ von $G$ wie folgt: Sei $G_1$ der Kern des Epimorphismus $\theta : G \to \mathbb{Z}_3$, $aN \mapsto 0$, $bN \mapsto 1$. Es ist klar, dass Index von $G_1$ in $G$ gleich 3 ist. Wir werden eine Präsentation von $G_1$ finden.

Mit Bezeichnungen aus dem Satz 28.3 betrachten wir folgendes Diagramm:

$$\begin{array}{ccc} F(a,b) & \xrightarrow{\varphi} & G \\ \bigvee & & \bigvee \\ H & \xrightarrow{\varphi} & G_1 \end{array}$$

Als Menge von Schreier-Repräsentanten der rechten Nebenklassen von $H$ in $F(a, b)$ können wir $T = \{1, b, b^2\}$ nehmen. Zuerst berechnen wir alle $\gamma(t, x)$ mit $t \in T$ und $x \in X = \{a, b\}$:

$$\begin{array}{lll} 1 \cdot a \cdot (\overline{a})^{-1} = a, & b \cdot a \cdot (\overline{ba})^{-1} = bab^{-1}, & b^2 \cdot a \cdot (\overline{b^2a})^{-1} = b^2ab^{-2}, \\ 1 \cdot b \cdot (\overline{b})^{-1} = 1, & b \cdot b \cdot (\overline{b^2})^{-1} = 1, & b^2 \cdot b \cdot (\overline{b^3})^{-1} = b^3. \end{array}$$

Wir bezeichnen $x = a$, $y = bab^{-1}$, $z = b^2ab^{-2}$, $t = b^3$. Dann ist $Y = \{x, y, z, t\}$ das Erzeugersystem von $G_1$. Um die Relationen $S$ zu berechnen, müssen wir die Wörter $trt^{-1}$, wobei $t \in T$ und $r = b^3a^{-2}$ ist, in dem Alphabet $Y$ umschreiben:

$$r = tx^{-2}, \quad brb^{-1} = ty^{-2}, \quad b^2rb^{-2} = tz^{-2}.$$

Also ist

$$\langle x, y, z, t \mid tx^{-2},\, ty^{-2},\, tz^{-2}\rangle$$

eine Präsentation von $G_1$. Durch Anwendung von Tietze-Transformationen erhalten wir eine etwas einfachere Präsentation von $G_1$

$$\langle x, y, z \mid x^2 = y^2 = z^2\rangle.$$