mosch [1,2] mail@math.moschpit.de

Algebra III

Vorlesungsskript – Wintersemester 2026/27
Leitung: Prof. E. Henke

Inhaltsverzeichnis

1 Gruppen **4**

1.1 Definition und erste Eigenschaften . . . 4
Definition 1.2 (Gruppe) . . . 4
Lemma 1.3 (Neutrale und inverse Elemente) . . . 4
1.4 Schreibweisen und Rechenregeln . . . 4
Bemerkung 1.5 (Rechenregeln) . . . 5
Definition 1.6 (Potenzen) . . . 5
Lemma 1.7 (Potenzrechenregeln) . . . 5
1.8 Untergruppen und Nebenklassen . . . 5
Definition 1.9 (Untergruppe) . . . 5
Definition 1.10 (Nebenklasse) . . . 5
Satz 1.11 (Lagrange) . . . 5
Definition 1.13 (Linksnebenklasse) . . . 6
Definition 1.14 (Erzeugnis) . . . 6

2 Homomorphismen und Normalteiler **6**

2.1 Homomorphismen . . . 6
Definition 2.2 (Homomorphismus) . . . 6
2.3 Normalteiler und Faktorgruppen . . . 6
Definition 2.4 (Normalteiler) . . . 6
Lemma 2.5 (Robinson 1.3.15) . . . 6
Definition 2.7 (Faktorgruppe) . . . 7
2.8 Die Isomorphiesätze . . . 7
Satz 2.9 (Erster Isomorphiesatz) . . . 7
Satz 2.10 (Zweiter Isomorphiesatz) . . . 7
Satz 2.11 (Dritter Isomorphiesatz) . . . 8
2.12 Untergruppenkorrespondenz . . . 8
Satz 2.13 (Untergruppenkorrespondenz) . . . 8

3 Beispiele für Gruppen **9**

3.1 Zahlbereiche und Matrixgruppen . . . 9
3.5 Gruppen von Isometrien . . . 10
Definition 3.6 (Isometrie) . . . 10
Definition 3.7 (Symmetriegruppe) . . . 10

zul. geändert am 7. November 2026

3.9 Gruppen von Permutationen . . . 10

4 Automorphismen und Konjugation **11**

4.1 Automorphismen . . . 11
Definition 4.3 (Automorphismengruppe) . . . 11
Definition 4.4 (Charakteristische Untergruppe) . . . 11
4.5 Konjugation . . . 11
Definition 4.6 (Konjugation) . . . 11
Definition 4.8 (Normaler Abschluss) . . . 11

5 Zyklische Gruppen **11**

5.1 Die Ordnung eines Elements . . . 11
Definition 5.2 (Ordnung) . . . 12
Definition 5.3 (Torsion) . . . 12
5.5 Untergruppen zyklischer Gruppen . . . 13
Satz 5.6 (Untergruppen zyklischer Gruppen) . . . 13
Satz 5.7 (Gruppen mit genau zwei Untergruppen) . . . 13
5.8 Automorphismen zyklischer Gruppen . . . 13
Satz 5.9 (Automorphismen zyklischer Gruppen) . . . 13

6 Operationen von Gruppen **14**

6.1 Definition und Beispiele . . . 14
Definition 6.2 (Operation) . . . 14
6.6 Operationen und Homomorphismen . . . 16
6.7 Bahnen und Stabilisatoren . . . 16
Definition 6.8 (Bahn und Stabilisator) . . . 16
Lemma 6.9 (Stabilisatoren) . . . 16
Lemma 6.10 (Bahn-Stabilisator-Lemma) . . . 16
Definition 6.11 (Transitive Operation) . . . 17

7 Diedergruppen **17**

7.1 Produkte von Untergruppen . . . 17
Lemma 7.2 (Produkt von Untergruppen) . . . 17
7.4 Normalisator und semidirektes Produkt . . . 18
Definition 7.5 (Normalisator) . . . 18
Definition 7.6 (Involution) . . . 18
Definition 7.7 (Semidirektes Produkt) . . . 18
Definition 7.9 (Externes semidirektes Produkt) . . . 18
7.10 Diedergruppen . . . 18
Lemma 7.11 (Diederbedingung) . . . 18
Definition 7.12 (Diedergruppe) . . . 19

8 Freie Gruppen **19**

8.1 Definition und Existenz . . . 19
Definition 8.2 (Freie Gruppe) . . . 19

Satz 8.4 (Existenz freier Gruppen) . . . 20
8.5 Reduzierte Wörter und Normalform . . . 21
Definition 8.6 (Reduziertes Wort) . . . 21
Satz 8.7 (Eindeutigkeit reduzierter Wörter) . . . 21
Korollar 8.8 (Existenz der Normalform) . . . 22
8.9 Charakterisierung freier Gruppen . . . 22
Satz 8.10 (Normalform) . . . 22
Satz 8.11 (Eindeutigkeit freier Gruppen) . . . 22
8.14 Freie Gruppen und Erzeugendensysteme . . . 23
Satz 8.17 (Projektivität) . . . 23

9 Präsentationen von Gruppen **24**

9.1 Freie Präsentationen . . . 24
Definition 9.2 (Freie Präsentation) . . . 24
9.4 Der Satz von Dyck . . . 24
Satz 9.5 (von Dyck, abstrakte Version) . . . 24
Satz 9.6 (von Dyck, anwendungsorientierte Version) . . . 25
9.7 Präsentationen der Diedergruppen . . . 25
Proposition 9.8 (Unendliche Diedergruppe) . . . 25
Proposition 9.9 (Endliche Diedergruppen) . . . 26
9.10 Präsentation der symmetrischen Gruppe . . . 26
Satz 9.11 (Präsentation der symmetrischen Gruppe) . . . 26
9.12 Endlich präsentierte Gruppen . . . 27
Definition 9.13 (Endlich präsentierte Gruppe) . . . 27
Lemma 9.14 (Endliche Erzeugendensysteme) . . . 27
Satz 9.15 (Wahl der Erzeuger) . . . 28
Lemma 9.17 (Untergruppen von endlichem Index) . . . 28
Satz 9.18 (P. Hall) . . . 29
Definition 9.19 (Polyzyklische Gruppe) . . . 30
Korollar 9.20 (Polyzyklische Gruppen) . . . 30

1 Gruppen

1.1 Definition und erste Eigenschaften

Dieser Abschnitt folgt Robinson, Abschnitt 1.1.

Definition 1.2 (Gruppe)**.** *Eine* **Gruppe** *ist eine Menge G zusammen mit einer inneren Verknüpfung $G \times G \to G$, $(a, b) \mapsto a \circ b$, sodass gilt:*

(i) $\circ$ *ist* **assoziativ**, *das heißt $a \circ (b \circ c) = (a \circ b) \circ c$ für alle $a, b, c \in G$.*

(ii) Es existiert ein **rechtsneutrales Element** *$e \in G$, das heißt $x \circ e = x$ für alle $x \in G$.*

(iii) Zu jedem Element $x \in G$ existiert ein $y \in G$, genannt **Rechtsinverses** *zu x, mit $x \circ y = e$.*

Lemma 1.3 (Neutrale und inverse Elemente)**.** *Sei G eine Gruppe und $e \in G$ ein rechtsneutrales Element von G. Sei $x \in G$ und $y \in G$ rechtsinvers zu x. Dann gilt:*

(i) $e \circ x = x$, das heißt, e ist auch **linksneutral**.

(ii) $y \circ x = e$, das heißt, y ist auch **linksinvers** *zu x.*

(iii) e ist das eindeutige linksneutrale und das eindeutige rechtsneutrale Element von G. Ferner ist y das eindeutige Rechtsinverse und das eindeutige Linksinverse zu x.

Beweis. (ii) Setze $z \coloneqq y \circ x$. Dann gilt

$$z \circ z = y \circ (x \circ y) \circ x = (y \circ e) \circ x = y \circ x = z.$$

Sei $w \in G$ rechtsinvers zu z, das heißt $z \circ w = e$. Multipliziert man die obige Gleichung von rechts mit w, so erhält man

$$z = z \circ \underbrace{(z \circ w)}_{=e} = z \circ w = e.$$

(i) Nach (ii) gilt

$$x = x \circ e \overset{\text{(ii)}}{=} x \circ (y \circ x) = (x \circ y) \circ x = e \circ x.$$

(iii) Wir haben gezeigt: Jedes Rechtsinverse ist auch linksinvers, und e ist auch linksneutral. Ist e' ein linksneutrales Element, so gilt

$$e' = e' \circ e = e.$$

Sei t ein Linksinverses zu x. Dann gilt

$$t = t \circ \underbrace{(x \circ y)}_{=e} = \underbrace{(t \circ x)}_{=e} \circ y = y. \qquad \square$$

1.4 Schreibweisen und Rechenregeln

Anstelle von $\circ$ benutzen wir oft auch $\cdot$ oder $+$.

- Schreiben wir $\cdot$, so wird das neutrale Element mit 1 oder 1_G bezeichnet. Wir schreiben oft xy anstelle von $x \cdot y$. Das Inverse zu x wird mit x^{-1} bezeichnet.
- Schreiben wir $+$, so wird das neutrale Element üblicherweise mit 0 oder 0_G bezeichnet, das Inverse zu $x \in G$ mit $-x$. Normalerweise wird $+$ nur für **abelsche** Gruppen benutzt, das heißt, falls $a + b = b + a$ für alle $a, b \in G$ gilt.

Meistens benutzen wir die multiplikative Schreibweise $\cdot$. Wegen der Assoziativität können Klammern weggelassen werden, zum Beispiel

$$g_1 g_2 \cdots g_n \coloneqq g_1(\cdots(g_{n-2}(g_{n-1}g_n))\cdots).$$

Bemerkung 1.5 (Rechenregeln)**.** In einer Gruppe $(G, \cdot)$ gilt:

$$\begin{aligned} xa = b &\Longrightarrow x = ba^{-1}, \\ ax = b &\Longrightarrow x = a^{-1}b, \\ (xy)^{-1} &= y^{-1}x^{-1}. \end{aligned}$$

Definition 1.6 (Potenzen)**.** *Für $x \in G$ setzen wir*

$$\begin{aligned} x^0 &\coloneqq 1_G, \\ x^{i+1} &\coloneqq x^i \cdot x \quad \textit{für alle } i \geq 0, \\ x^i &\coloneqq (x^{-i})^{-1} \quad \textit{für } i < 0. \end{aligned}$$

Lemma 1.7 (Potenzrechenregeln)**.** *Für alle $x \in G$ und $m, n \in \mathbb{Z}$ gilt:*

(i) $x^m x^n = x^{m+n} = x^n x^m$,

(ii) $(x^m)^n = x^{mn} = (x^n)^m$.

1.8 Untergruppen und Nebenklassen

Sei $(G, \cdot)$ stets eine Gruppe.

Definition 1.9 (Untergruppe)**.** *Eine Teilmenge $H \subseteq G$ heißt* **Untergruppe** *von G, falls*

$$H \neq \emptyset, \qquad xy \in H \quad \textit{für alle } x, y \in H, \qquad x^{-1} \in H \quad \textit{für alle } x \in H.$$

Wir schreiben dann $H \leq G$.

Definition 1.10 (Nebenklasse)**.** *Eine* **Nebenklasse** *von $H \leq G$ in G ist eine Teilmenge der Form*

$$Hg \coloneqq \{hg \mid h \in H\}.$$

Die Abbildung $H \to Hg$, $h \mapsto hg$, ist eine Bijektion, also gilt $|H| = |Hg|$. Die Nebenklassen von H in G bilden eine Partition von G. Daher gilt:

Satz 1.11 (Lagrange)**.** *Sei $H \leq G$ und sei*

$$|G : H| \coloneqq |\{Hg \mid g \in G\}|$$

der **Index** *von H in G. Dann gilt*

$$|G| = |H| \cdot |G : H|.$$

Lemma 1.12. *Für $H \leq G$ und $x, y \in G$ gilt*

$$Hx = Hy \iff x \in Hy \iff y \in Hx \iff xy^{-1} \in H.$$

Definition 1.13 (Linksnebenklasse)**.** *Eine* **Linksnebenklasse** *von $H \leq G$ ist eine Teilmenge der Form*

$$gH \coloneqq \{gh \mid h \in H\}.$$

Für $X \subseteq G$ definieren wir

$$X^{-1} \coloneqq \{x^{-1} \mid x \in X\}.$$

Ist $H \leq G$, so gilt $H^{-1} = H$. Die Abbildung

$$\{Hg \mid g \in G\} \longrightarrow \{gH \mid g \in G\}, \quad Hg \longmapsto (Hg)^{-1} = g^{-1}H,$$

ist eine Bijektion mit Umkehrabbildung $gH \longmapsto (gH)^{-1} = Hg^{-1}$.

Definition 1.14 (Erzeugnis)**.** *Für $X \subseteq G$ heißt*

$$\langle X \rangle \coloneqq \bigcap_{\substack{U \leq G \\ X \subseteq U}} U$$

das **Erzeugnis** *von X in G.*

Lemma 1.15.

$$\langle X \rangle = \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \mid n \geq 0,\ x_i \in X,\ \varepsilon_i \in \{-1, 1\}\}.$$

2 Homomorphismen und Normalteiler

2.1 Homomorphismen

Definition 2.2 (Homomorphismus)**.** *Sind $(G, \cdot)$ und $(G', *)$ Gruppen, so ist ein* **Homomorphismus** *von G nach G' eine Abbildung $\varphi\colon G \to G'$ mit*

$$(gh)\varphi = (g\varphi) * (h\varphi) \quad \textit{für alle } g, h \in G.$$

Ein Homomorphismus $\varphi\colon G \to G'$ heißt

- **Monomorphismus**, *falls φ injektiv ist,*
- **Epimorphismus**, *falls φ surjektiv ist,*
- **Isomorphismus**, *falls φ bijektiv ist.*

Existiert ein Isomorphismus $G \to G'$, so schreiben wir $G \cong G'$ und nennen G und G' **isomorph**.

2.3 Normalteiler und Faktorgruppen

Definition 2.4 (Normalteiler)**.** *Eine Untergruppe N von G heißt* **Normalteiler** *von G, falls*

$$gN = Ng \quad \textit{für alle } g \in G.$$

Wir schreiben dann $N \trianglelefteq G$.

Lemma 2.5 (Robinson 1.3.15)**.** *Sei $N \leq G$. Dann gilt*

$$\begin{aligned} N \trianglelefteq G &\iff g^{-1}Ng = N \quad \textit{für alle } g \in G \\ &\iff g^{-1}xg \in N \quad \textit{für alle } g \in G,\ x \in N. \end{aligned}$$

Ergänzung

Für einen Homomorphismus $\varphi\colon G \to G'$ heißt

$$\ker\varphi \coloneqq \{x \in G \mid x\varphi = 1\}$$

der **Kern** von φ.

Lemma 2.6. *Ist $\varphi\colon G \to G'$ ein Homomorphismus, so gilt*

$$\mathrm{Bild}(\varphi) \coloneqq \{x\varphi \mid x \in G\} \leq G' \quad \textit{und} \quad \ker\varphi \trianglelefteq G.$$

Definition 2.7 (Faktorgruppe)**.** *Ist $N \trianglelefteq G$, so ist*

$$G/N \coloneqq \{Ng \mid g \in G\}$$

eine Gruppe mit

$$(Ng)\cdot(Nh) \coloneqq N(gh),$$

neutralem Element $1_{G/N} = N \cdot 1_G = N$ und

$$(Ng)^{-1} = Ng^{-1} \quad \textit{für alle } g \in G.$$

Man nennt G/N die **Faktorgruppe** *oder* **Quotientengruppe** *modulo N.*

Die Abbildung

$$\pi\colon G \longrightarrow G/N, \quad g \longmapsto gN = Ng,$$

ist ein Epimorphismus mit $\ker\pi = N$.

2.8 Die Isomorphiesätze

Satz 2.9 (Erster Isomorphiesatz)**.** *Ist $\alpha\colon G \to G'$ ein Homomorphismus, so ist die Abbildung*

$$\overline{\alpha}\colon G/\ker\alpha \longrightarrow G', \quad (\ker\alpha)x \longmapsto x\alpha,$$

wohldefiniert und ein Isomorphismus von $G/\ker\alpha$ nach $\mathrm{Bild}(\overline{\alpha}) = \mathrm{Bild}(\alpha)$. Insbesondere gilt

$$G/\ker\alpha \cong \mathrm{Bild}(\alpha).$$

Satz 2.10 (Zweiter Isomorphiesatz)**.** *Sei $H \leq G$ und $N \trianglelefteq G$. Dann gilt $N \cap H \trianglelefteq H$, und*

$$\varphi\colon H/(N\cap H) \longrightarrow HN/N, \quad h(N\cap H) \longmapsto hN,$$

ist ein Isomorphismus. Insbesondere gilt

$$HN/N \cong H/(N\cap H).$$

Beweis.

Ergänzung

Zunächst ist $HN = \{hn \mid h \in H,\ n \in N\}$ eine Untergruppe von G: Wegen $N \trianglelefteq G$ ist $hN = Nh$ für alle $h \in H$, also $HN = NH$. Für $h, h' \in H$ und $n, n' \in N$ gilt daher

$$(hn)(h'n') = hh'\underbrace{(h'^{-1}nh')}_{\in N}n' \in HN \quad \text{und} \quad (hn)^{-1} = n^{-1}h^{-1} \in NH = HN.$$

Außerdem ist $N \leq HN$ und $N \trianglelefteq HN$, da $N \trianglelefteq G$. Also ist HN/N definiert.

Offenbar ist

$$\varphi\colon H \longrightarrow HN/N, \quad h \longmapsto hN,$$

ein Homomorphismus, nämlich die Einschränkung der Projektion $\pi\colon HN \to HN/N$ auf H. Er ist surjektiv, denn jede Nebenklasse in HN/N hat die Form hnN mit $h \in H$, $n \in N$, und es ist $hnN = hN$, da $nN = N \iff n \in N$. Für $h \in H$ gilt

$$h \in \ker\varphi \iff hN = N \iff h \in N,$$

also $\ker\varphi = H \cap N$. Insbesondere ist $N \cap H \trianglelefteq H$ als Kern eines Homomorphismus. Nach dem ersten Isomorphiesatz ist daher

$$H/(N \cap H) \longrightarrow HN/N, \quad h(N \cap H) \longmapsto hN,$$

ein Isomorphismus. □

Satz 2.11 (Dritter Isomorphiesatz)**.** *Seien $M, N \trianglelefteq G$ mit $N \leq M$. Dann gilt*

$$M/N \trianglelefteq G/N \quad \textit{und} \quad (G/N)/(M/N) \cong G/M.$$

Beweis. Definiere

$$\psi\colon G/N \longrightarrow G/M, \quad Nx \longmapsto Mx.$$

Die Abbildung ist wohldefiniert wegen $N \leq M$:

$$Nx = Ny \iff xy^{-1} \in N \leq M \Longrightarrow Mx = My.$$

Sie ist ein Epimorphismus mit $\ker\psi = M/N$. Wende den ersten Isomorphiesatz an. □

2.12 Untergruppenkorrespondenz

Ist $\varphi\colon G \to G'$ ein Homomorphismus und $U \subseteq G'$, so schreiben wir

$$\varphi^{-1}(U) \coloneqq \{x \in G \mid x\varphi \in U\}$$

für das **Urbild** von U in G. Ist $U \leq G'$, so gilt $\varphi^{-1}(U) \leq G$. Ist $H \leq G$, so ist

$$H\varphi \coloneqq \{h\varphi \mid h \in H\} \leq G'.$$

Satz 2.13 (Untergruppenkorrespondenz)**.** *Sei $\varphi\colon G \to G'$ ein Homomorphismus. Dann ist die Abbildung*

$$\theta\colon \{H \leq G \mid \ker\varphi \leq H\} \longrightarrow \{U \mid U \leq \mathrm{Bild}(\varphi)\}, \quad H \longmapsto H\varphi,$$

eine Bijektion mit Umkehrabbildung $U \mapsto \varphi^{-1}(U)$. Sie lässt sich einschränken zu einer Bijektion

$$\{N \trianglelefteq G \mid \ker\varphi \leq N\} \longrightarrow \{M \mid M \trianglelefteq \mathrm{Bild}(\varphi)\}.$$

Beweis. Es gilt $H\varphi \leq \mathrm{Bild}(\varphi)$ für alle $H \leq G$, also ist θ wohldefiniert. Die Abbildung

$$\theta^*\colon \{U \mid U \leq \mathrm{Bild}(\varphi)\} \longrightarrow \{H \leq G \mid \ker\varphi \leq H\}, \quad U \longmapsto \varphi^{-1}(U),$$

ist wohldefiniert, da $\varphi^{-1}(U) \leq G$ und $\ker\varphi = \{x \in G \mid x\varphi = 1\} \subseteq \varphi^{-1}(U)$.
Zu zeigen ist $\theta\theta^* = \mathrm{id}$ und $\theta^*\theta = \mathrm{id}$. Sei $H \leq G$ mit $\ker\varphi \leq H$. Dann gilt

$$\begin{aligned} H\theta\theta^* &= \varphi^{-1}(H\varphi) = \{x \in G \mid x\varphi \in H\varphi\} \\ &= \{x \in G \mid \exists\, h \in H\colon x\varphi = h\varphi\} = \{x \in G \mid x \in H\} = H, \end{aligned}$$

denn $x\varphi = h\varphi \iff xh^{-1} \in \ker\varphi \leq H$. Also ist $\theta\theta^* = \mathrm{id}$. Sei $U \leq \mathrm{Bild}(\varphi)$. Dann gilt

$$U\theta^*\theta = (\varphi^{-1}(U))\varphi = \{x \in G \mid x\varphi \in U\}\varphi = U.$$

Sei nun $\ker\varphi \leq N \leq G$. Zu zeigen ist

$$N \trianglelefteq G \iff N\varphi \trianglelefteq \mathrm{Bild}(\varphi).$$

Es gilt

$$\begin{aligned} N \trianglelefteq G &\iff g^{-1}ng \in N \quad \text{für alle } g \in G,\ n \in N \\ &\implies (g\varphi)^{-1}(n\varphi)(g\varphi) \in N\varphi \quad \text{für alle } g \in G,\ n \in N \\ &\iff N\varphi \trianglelefteq \mathrm{Bild}(\varphi). \end{aligned}$$

»$\Longleftarrow$«: Seien $g \in G$, $n \in N$ mit $(g\varphi)^{-1}(n\varphi)(g\varphi) \in N\varphi$. Dann folgt

$$\begin{aligned} &\implies \exists\, m \in N \text{ mit } m\varphi = (g\varphi)^{-1}(n\varphi)(g\varphi) \\ &\implies (g^{-1}ngm^{-1})\varphi = 1 \\ &\implies g^{-1}ngm^{-1} \in \ker\varphi \leq N \\ &\implies g^{-1}ng \in N. \end{aligned}$$

□

3 Beispiele für Gruppen

3.1 Zahlbereiche und Matrixgruppen

Beispiel 3.2.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, …; allgemein $(R, +)$ für einen Ring R.
- $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$; allgemein $(K \setminus \{0\}, \cdot)$, wobei K ein Körper ist.

Beispiel 3.3 (Allgemeine und spezielle lineare Gruppe)**.** Sei R ein kommutativer Ring mit 1 und

$$\mathrm{GL}(n, R) = \{A \in \mathrm{M}_n(R) \mid \det A \in R^\times\}.$$

Dann ist

$$\det\colon \mathrm{GL}(n, R) \to R^\times$$

ist ein Gruppenhomomorphismus mit

$$\ker(\det) = \mathrm{SL}(n, R) \coloneqq \{A \in \mathrm{GL}(n, R) \mid \det(A) = 1\} \trianglelefteq \mathrm{GL}(n, R).$$

Beispiel 3.4. Sei V ein Vektorraum über K. Dann ist

$$\mathrm{GL}(V) \coloneqq \{\varphi\colon V \to V \mid \varphi \text{ linear und bijektiv}\}$$

eine Gruppe. Ist $\dim V = n < \infty$, so ist $\mathrm{GL}(V) \cong \mathrm{GL}(n, K)$. Dann ist auch $\det(\varphi)$ für alle $\varphi \in \mathrm{GL}(V)$ definiert, und

$$\det\colon \mathrm{GL}(V) \longrightarrow (K \setminus \{0\}, \cdot)$$

ist ein Homomorphismus mit $\ker(\det) = \mathrm{SL}(V) \cong \mathrm{SL}(n, K)$.

3.5 Gruppen von Isometrien

Definition 3.6 (Isometrie)**.** *Sei (M, d) ein metrischer Raum. Eine* **Isometrie** *von M ist eine bijektive Abbildung $\alpha\colon M \to M$ mit*

$$d(x, y) = d(x\alpha, y\alpha) \quad \textit{für alle } x, y \in M.$$

Die Menge $\mathrm{Isom}(M) = \{\alpha \mid \alpha \textit{ Isometrie von } M\}$ *ist eine Gruppe unter Komposition.*

Definition 3.7 (Symmetriegruppe)**.** *Sei $X \subseteq M$ und $\alpha \in \mathrm{Isom}(M)$. Setze $X\alpha \coloneqq \{x\alpha \mid x \in X\}$. Die Gruppe*

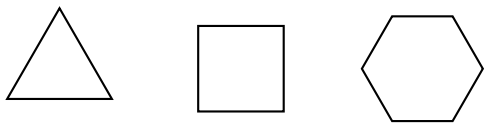
$$S_M(X) = \{\alpha \in \mathrm{Isom}(M) \mid X\alpha = X\}$$

heißt **Symmetriegruppe** *von X.*

Isometrien von E^2. Sei $E^n \coloneqq \mathbb{R}^n$ mit der üblichen Abstandsfunktion. Man kann zeigen, dass es für E^2 nur die folgenden drei Arten von Isometrien gibt:

- Spiegelungen an Geraden,
- Drehungen um einen Punkt,
- Translationen $\tau_{a,b}\colon E^2 \to E^2$, $(x, y) \mapsto (x + a, y + b)$ mit $a, b \in \mathbb{R}$.

Beispiel 3.8 (Diedergruppe)**.** Sei X ein reguläres n-Eck ($n \geq 3$).



Die Gruppe $S_{E^2}(X)$ hat folgende Elemente:

- Rotationen um $\frac{2\pi k}{n}$, $k = 1, \ldots, n$, insgesamt n Stück.
- Spiegelungen:
  - n ungerade: Spiegelungen an Geraden durch eine Ecke und den Mittelpunkt der gegenüberliegenden Seite (n Spiegelungen).
  - n gerade: Spiegelungen an Geraden durch gegenüberliegende Ecken und an Geraden durch die Mittelpunkte gegenüberliegender Seiten, insgesamt $n/2 + n/2 = n$ Spiegelungen.

Also hat $S_{E^2}(X)$ genau $2n$ Elemente. Die Gruppe

$$D_{2n} \coloneqq S_{E^2}(X)$$

heißt **Diedergruppe** der Ordnung $2n$. Sie wird später abstrakter behandelt.

3.9 Gruppen von Permutationen

Beispiel 3.10 (Symmetrische und alternierende Gruppe)**.** Sei X eine Menge. Dann ist

$$\mathrm{Sym}(X) = \{\alpha\colon X \to X \mid \alpha \text{ bijektiv}\}$$

eine Gruppe unter Komposition. Es ist

$$S_n = \mathrm{Sym}(\{1, 2, \ldots, n\}) \cong \mathrm{Sym}(X), \quad \text{falls } |X| = n.$$

Die **alternierende Gruppe**

$$A_n = \ker(\mathrm{sgn}) = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}$$

ist ein Normalteiler von S_n.

4 Automorphismen und Konjugation

4.1 Automorphismen

Bemerkung 4.2. Ist $\varphi\colon G \to G'$ ein Gruppenhomomorphismus, so gilt

$$\varphi \text{ injektiv} \iff \ker\varphi = \{1\}.$$

Statt $\{1\}$ schreiben wir auch kurz 1.

Definition 4.3 (Automorphismengruppe)**.** *Die Menge*

$$\mathrm{Aut}(G) \coloneqq \{\alpha\colon G \to G \mid \alpha \textit{ Isomorphismus}\}$$

der **Automorphismen** *von G ist eine Gruppe unter Komposition.*

Definition 4.4 (Charakteristische Untergruppe)**.** *Eine Untergruppe $U \leq G$ heißt* **charakteristisch** *in G, falls $U\alpha = U$ für alle $\alpha \in \mathrm{Aut}(G)$. Wir schreiben dann U char G.*
Eine Untergruppe $U \leq G$ heißt **vollinvariant***, falls $U\alpha \subseteq U$ für alle Homomorphismen $\alpha\colon G \to G$.*

4.5 Konjugation

Definition 4.6 (Konjugation)**.** *Sei $(G,\cdot)$ eine Gruppe und $g \in G$. Für $x \in G$ heißt*

$$x^g \coloneqq g^{-1}xg$$

die **Konjugierte** *von x unter g. Für $H \subseteq G$ definieren wir $H^g \coloneqq \{h^g \mid h \in H\}$.*

Die **Konjugationsabbildung** $c_g\colon G \to G$, $x \mapsto x^g$, ist ein Automorphismus von G. Ist $H \leq G$, so ist $H^g \leq G$. Für $N \leq G$ gilt

$$N \trianglelefteq G \iff N^g = N \quad \text{für alle } g \in G.$$

Lemma 4.7. *Ist M char $N \trianglelefteq G$, so ist $M \trianglelefteq G$.*

Beweis. Sei $g \in G$. Da $N \trianglelefteq G$, ist $N^{c_g} = N$. Wegen $c_g \in \mathrm{Aut}(G)$ ist $c_g|_N \in \mathrm{Aut}(N)$. Da $M \leq N$, ist $M^{c_g} = M^{c_g|_N}$, und wegen M char N gilt $M^{c_g|_N} = M$. Also ist $M^{c_g} = M$. □

Definition 4.8 (Normaler Abschluss)**.** *Sei $(G,\cdot)$ eine Gruppe und $X \subseteq G$. Dann heißt*

$$X^G \coloneqq \bigcap_{X \subseteq N \trianglelefteq G} N$$

der **normale Abschluss** *von X in G, also der kleinste Normalteiler von G, der X enthält. Es gilt*

$$X^G = \langle x^g \mid x \in X,\ g \in G\rangle.$$

5 Zyklische Gruppen

5.1 Die Ordnung eines Elements

Sei $(G,\cdot)$ eine Gruppe.

Definition 5.2 (Ordnung)**.** *Für $x \in G$ heißt*

$$\operatorname{ord}(x) = \begin{cases} |\langle x \rangle|, & \text{falls } \langle x \rangle \text{ endlich,} \\ \infty, & \text{sonst,} \end{cases}$$

die **Ordnung** *von x. Man schreibt auch $|x|$ oder $o(x)$.*

Definition 5.3 (Torsion)**.** *G heißt* **Torsionsgruppe**, *falls* $\operatorname{ord}(x)$ *für alle $x \in G$ endlich ist. G heißt* **torsionsfrei**, *falls $o(x) = \infty$ für alle $x \in G \setminus \{1\}$.*

Proposition 5.4. *Sei $x \in G$.*

(i) $\operatorname{ord}(x) = \infty \iff x^i \neq x^j$ *für alle $i \neq j \in \mathbb{Z}$.*

(ii) Ist $n = \operatorname{ord}(x) < \infty$, so gilt $x^m = 1 \iff n \mid m$ für alle $m \in \mathbb{Z}$. Ferner ist

$$\langle x \rangle = \{1, x, x^2, \ldots, x^{n-1}\},$$

und $1, x, \ldots, x^{n-1}$ sind paarweise verschieden.

(iii) Ist $\operatorname{ord}(x) = n < \infty$, *so gilt*

$$o(x^k) = \frac{n}{\operatorname{ggT}(n,k)}, \quad k \in \mathbb{Z}.$$

Beweis. Bei (i) ist „$\Leftarrow$“ klar. Es gelte nun $x^l = x^m$ für $l, m \in \mathbb{Z}$ mit $l \neq m$ (dies existiert insbesondere, falls $o(x) < \infty$). Dann folgt

$$x^{l-m} = 1 = x^{-(l-m)},$$

also existiert ein $n \in \mathbb{N}_{\geq 1}$ mit $x^n = 1$. Wähle n minimal mit dieser Eigenschaft.
Ist $m \in \mathbb{Z}$, so können wir $m = qn + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r \leq n-1$ schreiben. Dann gilt

$$x^m = \underbrace{(x^n)^q}_{=1} \cdot x^r = x^r.$$

Das ist wegen der Minimalität von n genau dann gleich 1, wenn $r = 0$ ist. Also gilt $x^m = 1 \iff n \mid m$. Außerdem ist stets $x^m = x^r \in \{1, x, \ldots, x^{n-1}\}$, das heißt $|\langle x \rangle| \leq n < \infty$, also $o(x) < \infty$.
Wir zeigen nun, dass $1, x, \ldots, x^{n-1}$ paarweise verschieden sind. Angenommen, $x^i = x^j$ für $0 \leq i < j \leq n-1$. Dann ist $x^{j-i} = 1$, nach der obigen Eigenschaft also $n \mid j - i$. Es ist aber $0 \leq j - i \leq n-1$, also $j - i = 0$, das heißt $j = i$. Damit sind (i) und (ii) gezeigt.
Zu (iii): Sei $o(x) = n < \infty$ und $k \in \mathbb{Z}$. Dann gilt

$$\left(x^k\right)^{\frac{n}{\operatorname{ggT}(n,k)}} = \left(x^n\right)^{\frac{k}{\operatorname{ggT}(n,k)}} \overset{\text{(ii)}}{=} 1 \Longrightarrow o\left(x^k\right) \leq \frac{n}{\operatorname{ggT}(n,k)}.$$

Sei $m \geq 1$ mit $x^{km} = \left(x^k\right)^m = 1$. Nach (ii) folgt $n \mid km$, also

$$\frac{n}{\operatorname{ggT}(n,k)} \;\Big|\; \frac{k}{\operatorname{ggT}(n,k)} \cdot m.$$

Da $\frac{k}{\operatorname{ggT}(n,k)}$ teilerfremd zu $\frac{n}{\operatorname{ggT}(n,k)}$ ist, folgt mit dem Lemma von Euklid

$$\frac{n}{\operatorname{ggT}(n,k)} \;\Big|\; m,$$

also $m \geq \frac{n}{\operatorname{ggT}(n,k)}$ und damit $o(x^k) = \frac{n}{\operatorname{ggT}(n,k)}$. □

5.5 Untergruppen zyklischer Gruppen

Satz 5.6 (Untergruppen zyklischer Gruppen)**.** *Sei $G = \langle x \rangle$ und $H \leq G$.*

(i) Ist G unendlich, so ist H unendlich zyklisch oder trivial.

(ii) Ist G endlich und $n = |G|$, so ist H zyklisch und $|H| \mid n$. Umgekehrt existiert zu jedem Teiler d von n genau eine Untergruppe von G der Ordnung d.

Beweis. (i) Wir zeigen zunächst, dass H zyklisch ist. Für $H = 1$ ist das klar. Sei also $H \neq 1$. Dann existiert ein $s \in \mathbb{Z}$ mit $1 \neq x^s \in H$. Ist $s < 0$, so ist $-s > 0$ und $x^{-s} = (x^s)^{-1} \in H$. Wir können also $s > 0$ annehmen und s minimal mit $1 \neq x^s \in H$ wählen.
Zu zeigen ist $H = \langle x^s \rangle$. Klar ist $\langle x^s \rangle \subseteq H$. Sei $x^t \in H$. Schreibe $t = sq + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < s$. Dann gilt

$$H \ni x^t = \underbrace{(x^s)^q}_{\in H} x^r \Longrightarrow x^r \in H.$$

Ergänzung

Wegen $0 \leq r < s$ und der Wahl von s ist $x^r = 1$, also $x^t = (x^s)^q \in \langle x^s \rangle$. Damit ist $H = \langle x^s \rangle$ zyklisch. Ist G unendlich, so hat x^s unendliche Ordnung, also ist H unendlich zyklisch. Das zeigt (i).

Zu (ii): Dass H zyklisch ist, wurde oben gezeigt, und $|H| \mid |G|$ folgt aus dem Satz von Lagrange.
Sei $d \geq 1$ ein Teiler von n. Dann gilt nach Proposition 5.4

$$\left|\langle x^{n/d} \rangle\right| = o\left(x^{n/d}\right) = d.$$

Sei nun $\langle x^k \rangle$ eine Untergruppe der Ordnung d. Dann gilt

$$\begin{aligned} x^{kd} = (x^k)^d = 1 &\Longrightarrow n \mid kd \Longrightarrow \tfrac{n}{d} \mid k \Longrightarrow k = \tfrac{n}{d} \cdot \ell \text{ für ein } \ell \in \mathbb{Z} \\ &\Longrightarrow x^k = \left(x^{n/d}\right)^\ell \in \langle x^{n/d} \rangle \Longrightarrow \langle x^k \rangle \leq \langle x^{n/d} \rangle. \end{aligned}$$

Beides sind Untergruppen der Ordnung d, also sind sie gleich. □

Satz 5.7 (Gruppen mit genau zwei Untergruppen)**.** *Eine Gruppe G hat genau dann genau zwei Untergruppen (nämlich 1 und G), wenn G zyklisch von Primzahlordnung ist.*

Beweis. „$\Longrightarrow$“: Hat G genau zwei Untergruppen, so gilt $G \neq 1$. Wähle also $1 \neq x \in G$. Dann gilt

$$1 \neq \langle x \rangle \leq G \Longrightarrow G = \langle x \rangle.$$

Ergänzung

G ist endlich: Andernfalls hat x unendliche Ordnung, also ist $x^2 \neq 1$. Wäre $x \in \langle x^2 \rangle$, etwa $x = x^{2m}$, so wäre $x^{2m-1} = 1$ mit $2m - 1 \neq 0$, ein Widerspruch. Also wäre $1 \neq \langle x^2 \rangle \neq G$ eine dritte Untergruppe.

Nach Satz 5.6 ist damit $|G|$ eine Primzahl.
„$\Longleftarrow$“: Satz von Lagrange. □

5.8 Automorphismen zyklischer Gruppen

Satz 5.9 (Automorphismen zyklischer Gruppen)**.** *Sei G eine zyklische Gruppe.*

(i) Ist G unendlich, so hat G genau zwei Automorphismen, nämlich id_G und $G \to G$, $g \mapsto g^{-1}$. Insbesondere ist $\mathrm{Aut}(G)$ zyklisch der Ordnung 2.

(ii) Sei $|G| = n < \infty$. Dann ist

$$\mathrm{Aut}(G) = \{\alpha_k \mid 1 \le k < n,\ \mathrm{ggT}(k,n) = 1\}, \quad \textit{wobei } \alpha_k \colon G \to G,\ g \mapsto g^k.$$

Außerdem ist die Abbildung

$$\Theta \colon \mathbb{Z}_n^* \to \mathrm{Aut}(G), \quad n\mathbb{Z} + k \mapsto \alpha_k,$$

ein Isomorphismus. Insbesondere ist $|\mathrm{Aut}(G)| = \varphi(n)$.

Dabei ist $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}_n^*$ die Gruppe der invertierbaren Elemente in $\mathbb{Z}_n$ und φ die Eulersche φ-Funktion.

Beweis. Sei $G = \langle x \rangle$ und $\alpha \in \mathrm{Aut}(G)$. Für $\ell \in \mathbb{Z}$ gilt $x^\ell \alpha = (x\alpha)^\ell$. Daher ist α durch $x\alpha$ eindeutig bestimmt. Außerdem ist $G = \langle x\alpha \rangle$.
(i) Sei zunächst G unendlich. Dann sind x und x^{-1} die einzigen Erzeuger von G, also ist $x\alpha = x$ oder $x\alpha = x^{-1}$. Weil G abelsch ist, ist $G \to G$, $g \mapsto g^{-1}$, ein Automorphismus. Daraus folgt (i).
(ii) Sei $|G| = n < \infty$. Dann ist $o(x\alpha) = o(x) = n$. Schreibe $x\alpha = x^k$. Nach Proposition 5.4 gilt

$$n = o(x^k) = \frac{n}{\mathrm{ggT}(k,n)} \Longrightarrow \mathrm{ggT}(k,n) = 1.$$

Ist umgekehrt $\mathrm{ggT}(k,n) = 1$, so existieren nach dem Lemma von Bézout $u, v \in \mathbb{Z}$ mit

$$uk + vn = 1, \quad \text{d. h. } uk \equiv 1 \bmod n.$$

Daraus folgt

$$(x^u)^k = (x^k)^u = x^{uk} = x.$$

Wir können dabei $1 \le u < n$ wählen. Dann ist α_u die Umkehrabbildung zu α_k, also ist α_k bijektiv. Da G abelsch ist, ist α_k ein Homomorphismus, also $\alpha_k \in \mathrm{Aut}(G)$.
Wegen $g^{k\ell} = (g^k)^\ell$ gilt

$$\alpha_{k\ell} = \alpha_k \alpha_\ell \quad \text{für } k, \ell \in \{1, \dots, n-1\}.$$

Also ist Θ ein Homomorphismus. Nach dem eben Gezeigten ist Θ surjektiv.
Ist $x^k = x^\ell$ mit $\mathrm{ggT}(n,k) = \mathrm{ggT}(n,\ell) = 1$, so sind $k + n\mathbb{Z}$ und $\ell + n\mathbb{Z}$ invertierbar, etwa $\bar{\ell} + n\mathbb{Z} = (\ell + n\mathbb{Z})^{-1}$. Dann gilt

$$\begin{aligned} x^{k\bar{\ell}} = x &\Longrightarrow x^{k\bar{\ell}-1} = 1 \Longrightarrow n \mid k\bar{\ell} - 1 \\ &\Longrightarrow (\ell + n\mathbb{Z})^{-1} = \bar{\ell} + n\mathbb{Z} = (k + n\mathbb{Z})^{-1} \Longrightarrow \ell + n\mathbb{Z} = k + n\mathbb{Z}. \end{aligned}$$

Also ist Θ injektiv. □

6 Operationen von Gruppen

6.1 Definition und Beispiele

Sei G stets eine Gruppe und X eine Menge.

Definition 6.2 (Operation)**.** *Eine* **Operation** *von G auf X (von rechts) ist eine Abbildung*

$$X \times G \to X, \quad (x,g) \mapsto xg,$$

sodass

$$\begin{aligned} x1_G &= x && \textit{für alle } x \in X, \\ (xg)h &= x(gh) && \textit{für alle } x \in X,\ g,h \in G. \end{aligned}$$

Beispiel 6.3.

- G operiert auf sich selbst durch „Rechtsmultiplikation“, d. h. die Multiplikation

$$G \times G \to G, \quad (x, g) \mapsto x \cdot g,$$

ist eine Operation von G auf G.

- G operiert auf sich selbst durch „Linksmultiplikation mit Inversen“. Genauer ist

$$G \times G \to G, \quad (x, g) \mapsto \underbrace{g^{-1}x}_{=:x \circ g},$$

eine Operation:

$$\begin{aligned} x \circ 1_G &= 1_G^{-1} x = 1_G x = x, \\ (x \circ g) \circ h &= h^{-1}(g^{-1}x) = (h^{-1}g^{-1})x = (gh)^{-1}x = x \circ (gh). \end{aligned}$$

- G operiert auf G durch Konjugation, d. h.

$$G \times G \to G, \quad (x, g) \mapsto x^g = g^{-1}xg,$$

ist eine Operation:

$$\begin{aligned} x^1 &= x, \\ (x^g)^h &= h^{-1}(g^{-1}xg)h = (h^{-1}g^{-1})\, x\, (gh) = (gh)^{-1}\, x\, (gh) = x^{gh}. \end{aligned}$$

Bemerkung 6.4. Ist $X \times G \to X$, $(x, g) \mapsto xg$, eine Operation, so operiert G auch auf der Potenzmenge $\mathscr{P}(X)$ von X, d. h.

$$\mathscr{P}(X) \times G \to \mathscr{P}(X), \quad (A, g) \mapsto Ag \coloneqq \{ag : a \in A\},$$

ist eine Operation.
Ist $B \subseteq X$ mit $Bg = B$ für alle $g \in G$, so operiert G auf B, denn die Einschränkung der Operation $X \times G \to X$ zu einer Abbildung $B \times G \to B$ ist eine Operation.

Beispiel 6.5.

- G operiert auf jedem Normalteiler von G durch Konjugation.
- G operiert auf $\mathscr{P}(G)$ durch Rechtsmultiplikation, durch Linksmultiplikation mit Inversen und durch Konjugation.
- Ist $H \leq G$, so ist $H^g \leq G$ für alle $g \in G$. Also operiert G auf der Menge der Untergruppen von G durch Konjugation.
- Ist $H \leq G$ und sind $x, g \in G$, so ist $(Hx)g = H(xg)$ wieder eine Rechtsnebenklasse. Das heißt, G operiert auf den Rechtsnebenklassen von H durch Rechtsmultiplikation.

  Genauso ist $g^{-1}(xH) = (g^{-1}x)H$. Daher operiert G auf den Linksnebenklassen von H in G durch Linksmultiplikation mit Inversen:

$$\{xH : x \in G\} \times G \to \{xH : x \in G\}, \quad (xH, g) \mapsto g^{-1}xH,$$

ist eine Operation.

6.6 Operationen und Homomorphismen

Ist $X \times G \to X$, $(x, g) \mapsto xg$, eine Operation, so ist für jedes $g \in G$

$$\pi_g \colon X \to X, \quad x \mapsto xg,$$

eine Bijektion, denn $\pi_{g^{-1}}$ ist die Umkehrabbildung: $(xg)g^{-1} = x(gg^{-1}) = x1_G = x$, und genauso $(xg^{-1})g = x$. Also ist $\pi_g \in \mathrm{Sym}(X)$.
Sei $\pi \colon G \to \mathrm{Sym}(X)$, $g \mapsto \pi_g$. Dann ist π ein Homomorphismus, d. h. $\pi_{gh} = \pi_g \pi_h$, denn für $x \in X$ gilt

$$x\pi_{gh} = x(gh) = (xg)h = x\pi_g\pi_h.$$

Ist umgekehrt $\varphi \colon G \to \mathrm{Sym}(X)$ ein Homomorphismus, so ist

$$X \times G \to X, \quad (x, g) \mapsto \overbrace{x(\underbrace{g\varphi}_{\in \mathrm{Sym}(X)})}^{=: x \cdot g},$$

eine Operation:

$$x \cdot 1_G = x(1_G\varphi) = x\mathrm{id}_X = x,$$
$$(x \cdot g) \cdot h = x(g\varphi)(h\varphi) \overset{\varphi \text{ Hom.}}{=} x\big((gh)\varphi\big) = x \cdot (gh).$$

Bildet man für diese Operation die Abbildung π wie oben, so gilt $\pi = \varphi$.

6.7 Bahnen und Stabilisatoren

Definition 6.8 (Bahn und Stabilisator)**.** *Sei $X \times G \to X$, $(x, g) \mapsto xg$, eine Operation. Für $x \in X$ heißt*

- $xG \coloneqq \{xg : g \in G\}$ *die* **Bahn** *von x unter G,*
- $G_x \coloneqq \{g \in G \mid xg = x\}$ *der* **Stabilisator** *von x in G.*

Lemma 6.9 (Stabilisatoren)**.** *Sei $X \times G \to X$ eine Operation, $x \in X$ und $g \in G$.*

(i) G_x ist eine Untergruppe von G.

(ii) $G_x^g = G_{xg}$.

Beweis. (i) Wegen $x \cdot 1_G = x$ ist $1_G \in G_x$. Für $g, h \in G_x$ gilt

$$xg = x,\ xh = x \Longrightarrow x(gh) = (xg)h = xh = x \Longrightarrow gh \in G_x.$$

Außerdem ist $xg^{-1} = (xg)g^{-1} = x(gg^{-1}) = x1_G = x$, also $g^{-1} \in G_x$.
(ii) Es gilt

$$\begin{aligned} G_{xg} &= \{a \in G : xga = xg\} = \{a \in G : xgag^{-1} = x\} = \{a \in G : gag^{-1} \in G_x\} \\ &= \{a \in G : a \in g^{-1}G_xg\} = G_x^g. \end{aligned}$$

□

Lemma 6.10 (Bahn-Stabilisator-Lemma)**.** *Sei $X \times G \to X$ eine Operation und $x \in X$. Dann ist die Abbildung*

$$\{G_xh : h \in G\} \to xG, \quad G_xh \mapsto xh,$$

wohldefiniert und eine Bijektion. Insbesondere ist

$$|G : G_x| = |xG|,$$

d. h. die Länge der Bahn ist gleich dem Index des Stabilisators.

Beweis. Für $g, h \in G$ gilt

$$G_x h = G_x g \iff hg^{-1} \in G_x \iff x(hg^{-1}) = x \iff x(hg^{-1})g = xg \iff xh = xg.$$

Die Richtung „$\Longrightarrow$“ bedeutet, dass die Abbildung wohldefiniert ist, die Richtung „$\Longleftarrow$“ zeigt die Injektivität. Die Surjektivität folgt aus der Definition der Bahn. □

Definition 6.11 (Transitive Operation)**.** *Eine Operation $X \times G \to X$ heißt* **transitiv***, falls ein $x \in X$ mit $xG = X$ existiert. Wir sagen dann auch, dass G* **transitiv** *auf X operiert.*

Bemerkung 6.12. Ist die Operation transitiv, so gilt $yG = X$ für alle $y \in X$. Ist nämlich $xG = X$, so ist $y = xh$ für ein $h \in G$, und damit

$$yG = \{(xh)g : g \in G\} = \{x(hg) : g \in G\} = \{xa : a \in \underbrace{hG}_{=G}\} = xG = X.$$

Für eine transitive Operation besagt das Bahn-Stabilisator-Lemma daher

$$|X| = |G : G_x| \quad \text{für alle } x \in X.$$

7 Diedergruppen

7.1 Produkte von Untergruppen

Für Teilmengen $A, B \subseteq G$ schreiben wir

$$AB \coloneqq \{ab \mid a \in A,\ b \in B\}, \qquad A^{-1} \coloneqq \{a^{-1} \mid a \in A\}.$$

Ergänzung

Lemma 7.2 (Produkt von Untergruppen)**.** *Seien $A, B \leq G$. Dann gilt*

$$AB \leq G \iff AB = BA.$$

Beweis. „$\Longrightarrow$“: Ist $AB \leq G$, so ist $AB = (AB)^{-1} = B^{-1}A^{-1} = BA$.
„$\Longleftarrow$“: Sei $AB = BA$. Wegen $1 = 1 \cdot 1 \in AB$ ist $AB \neq \emptyset$. Es gilt

$$(AB)^{-1} = B^{-1}A^{-1} = BA = AB$$

und

$$(AB)(AB) = A(BA)B = A(AB)B = (AA)(BB) = AB,$$

da $A, B \leq G$. Also ist AB unter Produkten und Inversen abgeschlossen, d. h. $AB \leq G$. □

Lemma 7.3. *Ist $A \leq G$ und $N \trianglelefteq G$, so gilt $AN = NA \leq G$.*

Beweis. Nach dem vorigen Lemma genügt es, $AN = NA$ zu zeigen. Da $N \trianglelefteq G$, ist $aN = Na$ für alle $a \in A$, also

$$AN = \bigcup_{a \in A} aN = \bigcup_{a \in A} Na = NA.$$ □

7.4 Normalisator und semidirektes Produkt

Ergänzung

Definition 7.5 (Normalisator)**.** *Sei $U \leq G$. Dann heißt*

$$N_G(U) \coloneqq \{g \in G \mid U^g = U\}$$

der **Normalisator** *von U in G. Es gilt $U \leq N_G(U) \leq G$ und*

$$U \trianglelefteq G \iff N_G(U) = G.$$

Definition 7.6 (Involution)**.** *Ein Element $s \in G$ heißt* **Involution***, falls $o(s) = 2$.*

Ergänzung

Definition 7.7 (Semidirektes Produkt)**.** *Seien $A, N \leq G$. Dann heißt G ein* **(internes) semidirektes Produkt** *von A mit N, falls*

$$G = AN, \qquad A \cap N = 1, \qquad N \trianglelefteq G.$$

Wir schreiben dann $G = A \ltimes N$.

Bemerkung 7.8. Ist $G = A \ltimes N$, so lässt sich jedes Element von G eindeutig als an mit $a \in A$ und $n \in N$ schreiben, und es gilt

$$(a_1 n_1)(a_2 n_2) = (a_1 a_2)(n_1^{a_2} n_2).$$

Das legt die folgende Konstruktion nahe.

Definition 7.9 (Externes semidirektes Produkt)**.** *Seien A und N Gruppen, und A operiere auf N (von rechts) durch Automorphismen, d. h. es gibt eine Abbildung $N \times A \to N$, $(n, a) \mapsto n^a$, mit*

$$n^1 = n, \qquad (n^a)^b = n^{ab}, \qquad (nm)^a = n^a m^a$$

für alle $n, m \in N$ und $a, b \in A$. Dann ist $A \times N$ mit der Multiplikation

$$(a_1, n_1) \cdot (a_2, n_2) \coloneqq (a_1 a_2,\ n_1^{a_2} n_2)$$

eine Gruppe, das **(externe) semidirekte Produkt** *von A mit N. Sie ist das interne semidirekte Produkt ihrer Untergruppen $\bar{A} \coloneqq \{(a, 1) \mid a \in A\} \cong A$ und $\bar{N} \coloneqq \{(1, n) \mid n \in N\} \cong N$, und für $n \in N$, $a \in A$ gilt $(1, n)^{(a,1)} = (1, n^a)$.*

7.10 Diedergruppen

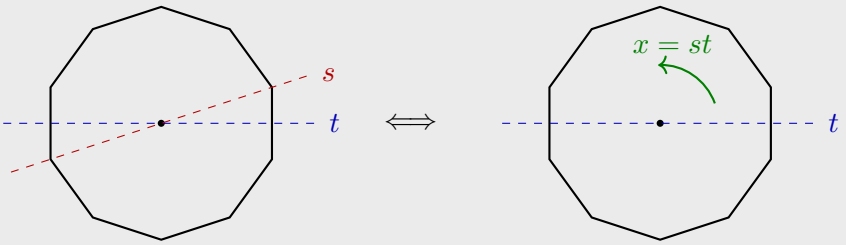
Ergänzung

Lemma 7.11 (Diederbedingung)**.** *Sei G eine Gruppe. Dann sind äquivalent:*

(i) Es gibt Involutionen $s \neq t$ in G mit $G = \langle s, t \rangle$.

(ii) Es gibt $t, x \in G$ mit $x \neq 1$, $o(t) = 2$, $x^t = x^{-1}$ und $G = \langle t \rangle \ltimes \langle x \rangle$.

Ergänzung



Ergänzung

Beweis. „(i) $\Longrightarrow$ (ii)“: Sei $G = \langle s, t\rangle$ mit $o(s) = o(t) = 2$ und $s \neq t$. Setze $x \coloneqq st$. Wegen $s \neq t$ ist $x \neq 1$. Da $t = t^{-1}$ und $s = s^{-1}$, gilt

$$x^t = t^{-1}xt = tstt = ts = t^{-1}s^{-1} = (st)^{-1} = x^{-1}.$$

Also ist $\langle x\rangle^t = \langle x^t\rangle = \langle x\rangle$, d. h. $t \in N_G(\langle x\rangle)$, und offensichtlich ist $x \in N_G(\langle x\rangle)$. Wegen $s = xt$ ist

$$G = \langle s, t\rangle = \langle x, t\rangle \leq N_G(\langle x\rangle),$$

also $\langle x\rangle \trianglelefteq G$. Nach dem Lemma über Produkte von Untergruppen ist $\langle t\rangle\langle x\rangle \leq G$, und da diese Untergruppe x und t enthält, ist $\langle t\rangle\langle x\rangle = \langle x, t\rangle = G$.
Es bleibt $\langle t\rangle \cap \langle x\rangle = 1$ zu zeigen. Angenommen, nicht. Wegen $|\langle t\rangle| = 2$ ist dann $t \in \langle x\rangle$. Dann ist $x^t = x$, also $x = x^{-1}$, d. h. $x^2 = 1$. Da $x \neq 1$, ist $\langle x\rangle = \{1, x\}$ und damit $t = x = st$, also $s = 1$, ein Widerspruch zu $o(s) = 2$. Also ist $G = \langle t\rangle \ltimes \langle x\rangle$.
„(ii) $\Longrightarrow$ (i)“: Sei $G = \langle t\rangle \ltimes \langle x\rangle$ mit $o(t) = 2$, $x \neq 1$ und $x^t = x^{-1}$. Setze $s \coloneqq xt$. Wegen $\langle t\rangle \cap \langle x\rangle = 1$ ist $t \neq x^{-1}$, also $s \neq 1$, und wegen $x \neq 1$ ist $s \neq t$. Da $t = t^{-1}$, gilt

$$s^2 = xtxt = x\,(t^{-1}xt) = xx^t = xx^{-1} = 1,$$

also $o(s) = 2$. Schließlich ist $G = \langle t, x\rangle = \langle t, xt\rangle = \langle s, t\rangle$. □

Ergänzung

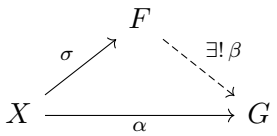
Definition 7.12 (Diedergruppe)**.** *Eine Gruppe, die eine der beiden äquivalenten Bedingungen des Lemmas erfüllt, heißt* **Diedergruppe**. *Sei $G = \langle t\rangle \ltimes \langle x\rangle$ wie in (ii).*

- *Ist $o(x) = n < \infty$, so schreiben wir D_{2n} für G und nennen G die* **Diedergruppe der Ordnung** $2n$. *Sie ist die Symmetriegruppe des regulären n-Ecks aus Abschnitt 3.*
- *Ist $o(x) = \infty$, d. h. $\langle x\rangle \cong (\mathbb{Z}, +)$, so schreiben wir D_∞ für G und nennen G die* **unendliche Diedergruppe**. *Dass sie existiert, sieht man am externen semidirekten Produkt von $\langle t\rangle \cong \mathbb{Z}/2\mathbb{Z}$ mit $(\mathbb{Z}, +)$, wobei t durch $n \mapsto -n$ operiert.*

8 Freie Gruppen

8.1 Definition und Existenz

Definition 8.2 (Freie Gruppe)**.** *Sei F eine Gruppe, $X \neq \emptyset$ eine Menge und $\sigma\colon X \to F$ eine Abbildung. Dann heißt F, genauer (F, σ),* **frei auf** *X, falls für jede Gruppe G und für jede Abbildung $\alpha\colon X \to G$ genau ein Homomorphismus $\beta\colon F \to G$ mit $\sigma\beta = \alpha$ existiert.*



Eine Gruppe, die frei auf irgendeiner Menge ist, heißt **freie Gruppe**.

Bemerkung 8.3. Ist (F, σ) frei auf X, so ist σ injektiv.

Beweis. Seien $x_1 \neq x_2 \in X$. Wähle eine Gruppe $G \neq 1$ und $g_1 \neq g_2 \in G$ sowie eine Abbildung $\alpha\colon X \to G$ mit $x_i\alpha = g_i$ für $i = 1, 2$. Dann existiert $\beta\colon F \to G$ mit $\sigma\beta = \alpha$. Wäre $x_1\sigma = x_2\sigma$, so wäre

$$g_1 = x_1\alpha = x_1\sigma\beta = x_2\sigma\beta = x_2\alpha = g_2,$$

ein Widerspruch. □

Wir werden später sehen, dass $\langle \operatorname{im}\sigma\rangle = F$ gilt. Ist (F, σ) frei auf X, so ist $(F, \text{Inklusion})$ frei auf $\operatorname{im}\sigma$.

Satz 8.4 (Existenz freier Gruppen)**.** *Sei $X \neq \emptyset$ eine Menge. Dann existieren eine Gruppe F und eine Abbildung $\sigma\colon X \to F$, sodass (F, σ) frei auf X ist und $F = \langle \operatorname{im}\sigma\rangle$.*

Beweis. Wähle eine zu X disjunkte Menge X^{-1} mit $|X^{-1}| = |X|$ und eine Bijektion $X \to X^{-1}$, $x \mapsto x^{-1}$. Dabei ist x^{-1} zunächst nur ein neues Symbol.
Wörter. Ein **Wort** in X ist eine endliche Folge von Symbolen aus $X \cup X^{-1}$, geschrieben als

$$w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} \quad \text{mit } r \geq 0,\ x_i \in X \text{ und } \varepsilon_i \in \{1, -1\} \text{ für alle } i = 1, \ldots, r.$$

Ist $r = 0$, so meinen wir das **leere Wort** 1. Das Produkt zweier Wörter in X ist einfach die Konkatenation: Ist $w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ und $v = y_1^{\delta_1} \cdots y_s^{\delta_s}$, so ist

$$wv = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} y_1^{\delta_1} \cdots y_s^{\delta_s}.$$

Dabei vereinbaren wir $w1 = w$ und $1w = w$. Das **Inverse** von w ist

$$w^{-1} \coloneqq x_r^{-\varepsilon_r} \cdots x_1^{-\varepsilon_1}, \qquad 1^{-1} = 1.$$

Die Gruppe F. Sei S die Menge der Wörter in X. Wir definieren eine Äquivalenzrelation auf S: Es sei $w \sim v$, wenn wir durch endlich viele Hintereinanderausführungen der folgenden Operationen von w nach v gelangen können:

(a) Einfügen von xx^{-1} oder $x^{-1}x$ ($x \in X$) als aufeinanderfolgende Elemente an beliebiger Stelle in das Wort,

(b) Streichen von xx^{-1} und $x^{-1}x$.

Dann ist $\sim$ eine Äquivalenzrelation. Wir schreiben $[w]$ für die Äquivalenzklasse von w und setzen

$$F \coloneqq S/\!\sim \coloneqq \{[w] : w \in S\}, \qquad [w] \cdot [v] \coloneqq [wv].$$

Das ist wohldefiniert: Ist $w \sim w'$ und $v \sim v'$, so ist $wv \sim w'v'$. Es gilt $[w] \cdot [1] = [w] = [1] \cdot [w]$ und

$$[w] \cdot [w^{-1}] = [ww^{-1}] = [1].$$

Da die Konkatenation assoziativ ist, ist auch das Produkt auf F assoziativ. Also ist F eine Gruppe.
(F, σ) ist frei auf X. Sei $\sigma\colon X \to F$, $x \mapsto [x]$. Sei G eine Gruppe und $\alpha\colon X \to G$ eine Abbildung. Zu zeigen ist, dass genau ein Homomorphismus $\beta\colon F \to G$ mit $\sigma\beta = \alpha$ existiert.
Definiere zunächst

$$\bar{\beta}\colon S \to G, \quad x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} \mapsto (x_1\alpha)^{\varepsilon_1} \cdots (x_r\alpha)^{\varepsilon_r}.$$

Ist $w \sim v$, so gilt $w\bar{\beta} = v\bar{\beta}$. Also können wir

$$\beta\colon F \to G, \quad [w] \mapsto w\bar{\beta},$$

definieren. Nach Definition von $\bar{\beta}$ gilt

$$([w] \cdot [v])\beta = [wv]\beta = (wv)\bar{\beta} = (w\bar{\beta})(v\bar{\beta}) = ([w]\beta) \cdot ([v]\beta),$$

also ist β ein Homomorphismus. Für $x \in X$ gilt nach Definition von $\bar{\beta}$

$$x\sigma\beta = [x]\beta = x\bar{\beta} = x\alpha,$$

also $\sigma\beta = \alpha$.
Es bleibt zu zeigen, dass β eindeutig ist. Sei $\gamma\colon F \to G$ ein Homomorphismus mit $\sigma\gamma = \alpha$. Offensichtlich ist $F = \langle [x] : x \in X\rangle = \langle \operatorname{im}\sigma\rangle$. Wegen $\sigma\gamma = \alpha = \sigma\beta$ ist $\gamma|_{\operatorname{im}\sigma} = \beta|_{\operatorname{im}\sigma}$, also $\gamma = \beta$. □

8.5 Reduzierte Wörter und Normalform

Betrachte die Konstruktion oben. Ist $w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$, so ist

$$[w] = [x_1^{\varepsilon_1}] \cdots [x_r^{\varepsilon_r}] = [x_1]^{\varepsilon_1} \cdots [x_r]^{\varepsilon_r}.$$

Wir wollen jedes Element von F so einfach wie möglich als ein solches Produkt darstellen, in dem sich nichts mehr „wegkürzen“ lässt.

Definition 8.6 (Reduziertes Wort)**.** *Ein Wort w in X heißt* **reduziert***, falls es kein Teilwort der Form xx^{-1} oder $x^{-1}x$ mit $x \in X$ besitzt.*

Offensichtlich existiert in jeder Äquivalenzklasse $[w] \in F$ ein reduziertes Wort.

Satz 8.7 (Eindeutigkeit reduzierter Wörter)**.** *Jede Äquivalenzklasse von Wörtern in X (wie oben konstruiert) enthält genau ein reduziertes Wort.*

Beweis. Sei R die Menge der reduzierten Wörter in X. Wir konstruieren mit der universellen Eigenschaft von F einen Homomorphismus $\theta\colon F \to \mathrm{Sym}(R)$.
Für $u \in X \cup X^{-1}$ definiere die Funktion $u'\colon R \to R$ durch

$$(x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r})u' := \begin{cases} x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} u, & u \neq x_r^{-\varepsilon_r}, \\ x_1^{\varepsilon_1} \cdots x_{r-1}^{\varepsilon_{r-1}}, & u = x_r^{-\varepsilon_r}, \end{cases}$$

für reduzierte Wörter $x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$.
Es gilt $u'(u^{-1})' = \mathrm{id}_R$: Ist $u \neq x_r^{-\varepsilon_r}$, so gilt

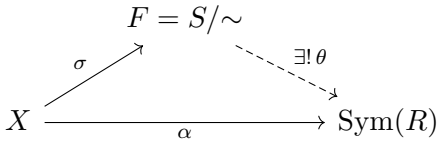
$$(x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r})u'(u^{-1})' = (x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} u)(u^{-1})' = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}.$$

Ist $u = x_r^{-\varepsilon_r}$, so gilt $u^{-1} = x_r^{\varepsilon_r} \neq x_{r-1}^{-\varepsilon_{r-1}}$, da $x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ reduziert ist. Also ist

$$(x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r})u'(u^{-1})' = (x_1^{\varepsilon_1} \cdots x_{r-1}^{\varepsilon_{r-1}})(u^{-1})' = x_1^{\varepsilon_1} \cdots x_{r-1}^{\varepsilon_{r-1}} \underbrace{x_r^{\varepsilon_r}}_{=u^{-1}}.$$

Also ist $u'(u^{-1})' = \mathrm{id}_R$ und genauso $(u^{-1})'u' = \mathrm{id}_R$. Damit ist u' eine Bijektion, d. h. $u' \in \mathrm{Sym}(R)$.
Also ist $\alpha\colon X \to \mathrm{Sym}(R)$, $x \mapsto x'$, wohldefiniert. Wegen der universellen Eigenschaft von F existiert ein Homomorphismus $\theta\colon F \to \mathrm{Sym}(R)$ mit $\sigma\theta = \alpha$, also

$$[x]\theta = x\alpha = x' \quad \text{für } x \in X.$$



Seien nun $v, w \in R$ mit $v \sim w$. Zu zeigen ist $v = w$. Aus $[v] = [w]$ folgt $[v]\theta = [w]\theta \in \mathrm{Sym}(R)$. Sei $v = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$. Dann ist $[v] = [x_1^{\varepsilon_1}] \cdots [x_r^{\varepsilon_r}]$ und

$$[v]\theta = ([x_1^{\varepsilon_1}]\theta) \cdots ([x_r^{\varepsilon_r}]\theta) = (x_1^{\varepsilon_1})' \cdots (x_r^{\varepsilon_r})' \in \mathrm{Sym}(R).$$

Wende diese Funktion auf das leere Wort 1 an:

$$1([v]\theta) = 1\,(x_1^{\varepsilon_1})' \cdots (x_r^{\varepsilon_r})' = x_1^{\varepsilon_1}(x_2^{\varepsilon_2})' \cdots (x_r^{\varepsilon_r})' = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_r^{\varepsilon_r} = v.$$

Hier geht ein, dass v reduziert ist. Also ist $1([v]\theta) = v$ und genauso $1([w]\theta) = w$. Nach Annahme gilt $[v]\theta = [w]\theta$, also $v = w$. □

Normalform. Nach dem Satz kann jedes Element von F (wie oben konkret konstruiert) eindeutig in der Form $[w]$ mit einem reduzierten Wort w geschrieben werden, etwa

$$w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} \quad \text{mit } r \geq 0,\ x_i \in X,\ \varepsilon_i = \pm 1.$$

Dann ist $[w] = [x_1]^{\varepsilon_1} \cdots [x_r]^{\varepsilon_r}$. Indem wir hintereinander auftretende Terme mit demselben Element x_i zusammenmultiplizieren, gelangen wir zu einem Ausdruck der Form

$$[w] = [y_1]^{l_1} \cdots [y_s]^{l_s} \quad \text{mit } s \geq 0,\ l_i \in \mathbb{Z} \setminus \{0\},\ y_i \neq y_{i+1},\ y_i \in X.$$

Daraus kann man das ursprüngliche reduzierte Wort wieder herleiten. Daher ist dieser Ausdruck eindeutig.
Um die Notation zu vereinfachen, schreiben wir w für $[w]$, wenn w reduziert ist, insbesondere x für $[x]$ für $x \in X$.

Korollar 8.8 (Existenz der Normalform)**.** *Jedes Element von F kann eindeutig in der Form*

$$w = x_1^{l_1} x_2^{l_2} \cdots x_s^{l_s} \quad \textit{mit } s \geq 0,\ l_i \in \mathbb{Z} \setminus \{0\},\ x_i \neq x_{i+1},\ x_i \in X,$$

geschrieben werden. Wir nennen dies die **Normalform** *von $w \in F$.*

Manchmal ist es praktisch, $w(x_1, \ldots, x_s)$ für w zu schreiben, bzw. $w(x)$ mit $x = (x_1, \ldots, x_s)$.

8.9 Charakterisierung freier Gruppen

Satz 8.10 (Normalform)**.** *Sei G eine Gruppe und $X \subseteq G$. Angenommen, jedes $g \in G$ kann eindeutig geschrieben werden als*

$$g = x_1^{l_1} \cdots x_s^{l_s} \quad \textit{mit } s \geq 0,\ x_i \in X,\ l_i \in \mathbb{Z} \setminus \{0\},\ x_i \neq x_{i+1}.$$

Dann ist G frei auf X, genauer: $(G, \mathit{Inklusion})$ ist frei auf X.

Beweis. Sei $F = S/\!\sim$ die vorher konstruierte freie Gruppe auf X und $\sigma\colon X \to F$, $x \mapsto [x]$. Nach der universellen Eigenschaft freier Gruppen existiert genau ein Homomorphismus $\beta\colon F \to G$ mit $\sigma\beta = \iota$, wobei $\iota\colon X \to G$ die Inklusion ist.
β ist surjektiv: Es gilt $(\operatorname{im}\sigma)\beta = X\iota = X$, also $X \subseteq \operatorname{im}\beta$. Wegen $G = \langle X \rangle$ und da β ein Homomorphismus ist, ist β surjektiv.
β ist injektiv: Seien $[w], [u] \in F$ mit $[u]\beta = [w]\beta$. Schreibe $w = x_1^{l_1} \cdots x_s^{l_s}$ in Normalform. Dann ist $[w] = [x_1]^{l_1} \cdots [x_s]^{l_s}$. Beachte $[x_i]\beta = x_i\sigma\beta = x_i$. Also ist

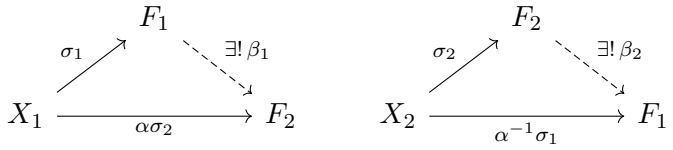
$$[w]\beta = ([x_1]\beta)^{l_1} \cdots ([x_s]\beta)^{l_s} = x_1^{l_1} \cdots x_s^{l_s} = w.$$

Genauso ist $[u]\beta = u$, falls u in Normalform ist. Daraus folgt $u = w$, also $[w] = [u]$, d. h. β ist injektiv.
Also ist β ein Isomorphismus. □

Satz 8.11 (Eindeutigkeit freier Gruppen)**.** *Sei (F_1, σ_1) frei auf X_1 und (F_2, σ_2) frei auf X_2 mit $|X_1| = |X_2|$. Dann gilt $F_1 \cong F_2$. Genauer: Ist $\alpha\colon X_1 \to X_2$ eine Bijektion, so existiert ein Isomorphismus $\beta\colon F_1 \to F_2$ mit $\sigma_1\beta = \alpha\sigma_2$.*

$$\begin{array}{ccc} F_1 & \xrightarrow{\beta} & F_2 \\ {\scriptstyle\sigma_1}\uparrow & & \uparrow{\scriptstyle\sigma_2} \\ X_1 & \xrightarrow[\alpha]{} & X_2 \end{array}$$

Beweis. Nach Voraussetzung existieren eindeutige Homomorphismen $\beta_1 \colon F_1 \to F_2$ und $\beta_2 \colon F_2 \to F_1$, sodass die Diagramme



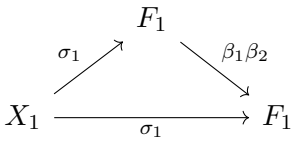
kommutieren, also

$$\sigma_1\beta_1 = \alpha\sigma_2, \qquad \sigma_2\beta_2 = \alpha^{-1}\sigma_1.$$

Es bleibt zu zeigen, dass $\beta \coloneqq \beta_1$ ein Isomorphismus ist. Dazu zeigen wir $\beta_1\beta_2 = \mathrm{id}_{F_1}$ und $\beta_2\beta_1 = \mathrm{id}_{F_2}$. Es gilt

$$\sigma_1(\beta_1\beta_2) = (\sigma_1\beta_1)\beta_2 = \alpha\sigma_2\beta_2 = \alpha\alpha^{-1}\sigma_1 = \sigma_1.$$

Also kommutiert das Diagramm



Dieses Diagramm kommutiert aber auch mit id_{F_1} anstelle von $\beta_1\beta_2$. Wegen der Eindeutigkeit folgt $\beta_1\beta_2 = \mathrm{id}_{F_1}$. Genauso folgt $\beta_2\beta_1 = \mathrm{id}_{F_2}$. □

Korollar 8.12. *Ist (F, σ) frei auf X, so gilt $F = \langle \operatorname{im}\sigma \rangle$.*

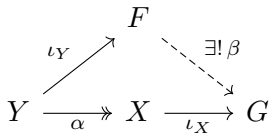
Oft ersetzen wir (X, σ) durch $(\operatorname{im}\sigma, \text{Inklusion})$ und nehmen so an, dass $X \subseteq F$ gilt und $(F, \text{Inklusion})$ frei auf X ist. Wir sagen dann einfach, F ist frei auf $X \subseteq F$.

Korollar 8.13. *Ist F frei auf $X \subseteq F$, so besitzt jedes Element von F eine eindeutige Normalform in X.*

8.14 Freie Gruppen und Erzeugendensysteme

Satz 8.15. *Sei G eine Gruppe und $X \subseteq G$ mit $G = \langle X \rangle$. Sei F frei auf $Y \subseteq F$. Ist $\alpha \colon Y \to X$ surjektiv, so existiert ein Epimorphismus $\beta \colon F \to G$ mit $\beta|_Y = \alpha$.*

Beweis. Seien $\iota_Y \colon Y \to F$ und $\iota_X \colon X \to G$ die Inklusionen.



Es existiert ein Homomorphismus $\beta \colon F \to G$ mit $\iota_Y\beta = \alpha\iota_X$, d. h. $\beta|_Y = \alpha$. Da $G = \langle X \rangle$ und $X = Y\alpha \subseteq \operatorname{im}\beta$, ist β surjektiv. □

Korollar 8.16. *Jede Gruppe ist epimorphes Bild einer freien Gruppe.*

Satz 8.17 (Projektivität)**.** *Sei F eine freie Gruppe und seien G, H Gruppen. Sei $\alpha \colon F \to H$ ein Homomorphismus und $\beta \colon G \to H$ ein Epimorphismus. Dann existiert ein Homomorphismus $\gamma \colon F \to G$ mit $\gamma\beta = \alpha$.*

Beweis. Sei F frei auf $X \subseteq F$. Ist $x \in X$, so ist $x\alpha \in H = \operatorname{im}\beta$. Also können wir $g_x \in G$ wählen mit $g_x\beta = x\alpha$. Wegen der universellen Eigenschaft von F existiert dann ein Homomorphismus $\gamma \colon F \to G$ mit $x\gamma = g_x$ für alle $x \in X$. Dann ist $x(\gamma\beta) = g_x\beta = x\alpha$, also $\gamma\beta|_X = \alpha|_X$. Wegen $F = \langle X \rangle$ und da $\gamma\beta$ und α Homomorphismen sind, folgt $\gamma\beta = \alpha$. □

9 Präsentationen von Gruppen

9.1 Freie Präsentationen

Definition 9.2 (Freie Präsentation)**.** *Eine* **freie Präsentation** *einer Gruppe G ist ein Epimorphismus $\pi\colon F \to G$, wobei F frei ist.*

Nach dem Korollar oben besitzt jede Gruppe eine freie Präsentation. Ist $\pi\colon F \to G$ eine freie Präsentation, so ist $R \coloneqq \ker\pi \trianglelefteq F$ und $F/R \cong G$. Man nennt die Elemente von R **Relationen**.

Beispiel 9.3 (Standardpräsentation)**.** Sei F die freie Gruppe auf der Menge

$$Y = \{y_g \mid 1 \neq g \in G\},$$

die in Bijektion zu $G \setminus \{1\}$ steht, und $Y \subseteq F$. Sei $\pi\colon F \to G$ der eindeutige Homomorphismus mit $y_g\pi = g$. Diesen Epimorphismus π nennt man die **Standardpräsentation** von G.

Sei $\pi\colon F \to G$ eine freie Präsentation und F frei auf $Y \subseteq F$. Wähle $S \subseteq F$ mit $\ker\pi = S^F$ (normaler Abschluss). Setze $X \coloneqq Y\pi$. Aus $F = \langle Y\rangle$ und da π ein Epimorphismus ist, folgt $G = \langle X\rangle$. Ist $r \in \ker\pi$, so kann r geschrieben werden als

$$r = (s_1^{\varepsilon_1})^{f_1} \cdots (s_k^{\varepsilon_k})^{f_k} \quad \text{mit } s_i \in S,\ \varepsilon_i = \pm 1,\ f_i \in F.$$

Wir sagen dann, r ist eine **Konsequenz** aus S bzw. aus $s_1, \ldots, s_k$.
Die Präsentation π zusammen mit der Wahl von Y und S legt eine Präsentation von G durch „Erzeuger und definierende Relationen“ fest. Dabei heißen die Elemente von Y **Erzeuger** und die Elemente von S **definierende Relationen**. Wir schreiben

$$G = \langle Y \mid S\rangle.$$

Das bedeutet: Es existiert eine freie Gruppe F auf Y mit $G \cong F/S^F$.
Oft will man sich die Erzeuger als Elemente von G vorstellen. Man schreibt dann

$$G = \langle X \mid s(x) = 1,\ s \in S\rangle$$

und nennt dies ebenso eine Präsentation von G durch erzeugende Relationen.

Schreibweise. Sei F frei auf Y und $w \in F$. Dann kann man w als Wort in Y schreiben, etwa $w = y_1^{l_1} \cdots y_s^{l_s}$ in Normalform. Ist G eine Gruppe, $X \subseteq G$ und $\alpha\colon Y \to X$, $y \mapsto \bar{y}$, eine Abbildung, so schreiben wir $w = w(y_1, \ldots, y_s) \in F$ und

$$w(\bar{y}_1, \ldots, \bar{y}_s) \coloneqq \bar{y}_1^{l_1} \cdots \bar{y}_s^{l_s}$$

für das entsprechende Produkt in G.

9.4 Der Satz von Dyck

Satz 9.5 (von Dyck, abstrakte Version)**.** *Seien G, H Gruppen mit freien Präsentationen $\varepsilon\colon F \to G$ und $\delta\colon F \to H$, und es gelte $\ker\varepsilon \subseteq \ker\delta$. Dann ist die Abbildung*

$$G \to H, \quad g\varepsilon \mapsto g\delta \quad (g \in F),$$

wohldefiniert und ein Epimorphismus.

Beweis. Das ist ein Spezialfall des Isomorphiesatzes:

$$G \cong F/\ker\varepsilon \to F/\ker\delta \cong H, \quad g\ker\varepsilon \mapsto g\ker\delta. \qquad \square$$

Satz 9.6 (von Dyck, anwendungsorientierte Version)**.** *Sei $G = \langle X \mid S\rangle$ eine Präsentation einer Gruppe G. Sei H eine Gruppe mit $H = \langle \bar{X}\rangle$ und $X \to \bar{X}$, $x \mapsto \bar{x}$, eine surjektive Abbildung, sodass für alle $s = s(x_1, \dots, x_n) \in S$ gilt:*

$$s(\bar{x}_1, \dots, \bar{x}_n) = 1 \quad \text{in } H.$$

Dann existiert ein Epimorphismus $\varphi\colon G \to H$ mit $x\varphi = \bar{x}$.

Beweis. Sei F frei auf X und $\varepsilon\colon F \to G$ ein Epimorphismus mit $\ker\varepsilon = S^F$. Sei $\delta\colon F \to H$ ein Epimorphismus mit $x\delta = \bar{x}$ für alle $x \in X$. Für $s = s(x_1, \dots, x_n) \in S$ gilt

$$s\delta = s(x_1, \dots, x_n)\delta = s(\bar{x}_1, \dots, \bar{x}_n) = 1.$$

Also ist $S \subseteq \ker\delta \trianglelefteq F$ und damit $\ker\varepsilon = S^F \subseteq \ker\delta$. Nach dem Satz von Dyck (abstrakte Version) existiert ein Homomorphismus $\varphi\colon G \to H$, $x\varepsilon \mapsto x\delta$. Insbesondere gilt $(x\varepsilon)\varphi = x\delta = \bar{x}$. □

9.7 Präsentationen der Diedergruppen

Ist eine Gruppe nur durch Erzeugende und Relationen gegeben, so ist es oft schwierig, ihre Struktur zu verstehen. Zunächst ist nicht einmal klar, ob es sich um die triviale Gruppe handelt. Um das auszuschließen, müssen wir eine nicht-triviale Gruppe konstruieren, in der die entsprechenden Relationen für geeignete Erzeuger gelten. Die Diedergruppen haben wir bereits als semidirekte Produkte konstruiert.

Proposition 9.8 (Unendliche Diedergruppe)**.** *Die Gruppen*

$$G \coloneqq \langle x, y \mid x^2 = 1,\ y^2 = 1\rangle \qquad \text{und} \qquad H \coloneqq \langle x, a \mid x^2 = 1,\ xaxa = 1\rangle$$

sind beide isomorph zu D_∞.

Beweis. Wir benutzen, dass

$$D_\infty = \langle \bar{x}\rangle \ltimes \langle \bar{a}\rangle \quad \text{mit } o(\bar{x}) = 2,\ o(\bar{a}) = \infty,\ \bar{a}^{\bar{x}} = \bar{a}^{-1}.$$

$G \cong D_\infty$: Setze $a \coloneqq xy$. Dann ist

$$a^x = x^{-1}xyx = yx = y^{-1}x^{-1} = (xy)^{-1} = a^{-1}.$$

Setze $\bar{y} \coloneqq \bar{x}\bar{a}$. Wegen $\bar{x} = \bar{x}^{-1}$ ist

$$\bar{y}^2 = \bar{x}\bar{a}\bar{x}\bar{a} = \bar{a}^{\bar{x}}\bar{a} = \bar{a}^{-1}\bar{a} = 1.$$

Nach dem Satz von Dyck existiert also ein Epimorphismus

$$\theta\colon G \to D_\infty \quad \text{mit } x \mapsto \bar{x} \text{ und } y \mapsto \bar{y}.$$

Dann gilt $a\theta = (xy)\theta = \bar{x}\bar{y} = \bar{x}\bar{x}\bar{a} = \bar{a}$. Wir zeigen $\ker\theta = 1$. Sei $g \in \ker\theta$. Es ist $G = \langle x, y\rangle = \langle x, a\rangle$, und wegen $a^x = a^{-1}$ ist $\langle a\rangle \trianglelefteq G$. Also ist $G = \langle x\rangle\langle a\rangle$, d. h. es existieren $r \in \{0, 1\}$ und $s \in \mathbb{Z}$ mit $g = x^r a^s$. Dann ist

$$1 = g\theta = \bar{x}^r\bar{a}^s \Longrightarrow \bar{x}^r = 1,\ \bar{a}^s = 1 \Longrightarrow r = 0,\ s = 0 \Longrightarrow g = x^r a^s = 1.$$

Also ist $\ker\theta = 1$, d. h. θ ist ein Isomorphismus und $G \cong D_\infty$.
$H \cong D_\infty$: Schreibe D_∞ wie oben. Nach dem Satz von Dyck existiert ein Epimorphismus

$$\beta\colon H \to D_\infty \quad \text{mit } x \mapsto \bar{x},\ a \mapsto \bar{a}.$$

Ein $h \in \ker\beta$ ist wie oben von der Form $h = x^r a^s$ mit $r \in \{0, 1\}$ und $s \in \mathbb{Z}$. Dann ist

$$1 = h\beta = \bar{x}^r\bar{a}^s \Longrightarrow r = s = 0 \Longrightarrow h = 1.$$

Also ist β ein Isomorphismus und $H \cong D_\infty$. □

Proposition 9.9 (Endliche Diedergruppen)**.** *Die Gruppen*

$$G \coloneqq \langle x, y \mid x^2 = y^2 = 1,\ (xy)^n = 1\rangle \qquad \textit{und} \qquad H \coloneqq \langle x, a \mid x^2 = 1 = a^n,\ xaxa = 1\rangle$$

sind beide Präsentationen von D_{2n}.

Beweis. Der Beweis ist ähnlich wie oben. Wir zeigen nur $H \cong D_{2n}$. Schreibe

$$D_{2n} = \langle \bar{x}\rangle \ltimes \langle \bar{a}\rangle, \quad o(\bar{x}) = 2,\ o(\bar{a}) = n,\ \bar{a}^{\bar{x}} = \bar{a}^{-1}.$$

Nach dem Satz von Dyck existiert ein Epimorphismus $\beta\colon H \to D_{2n}$ mit $x \mapsto \bar{x}$ und $a \mapsto \bar{a}$. Zu zeigen ist $\ker\beta = 1$. Sei $h \in \ker\beta$. Dann ist $h = x^r a^s$ mit $r \in \{0, 1\}$ und $s \in \mathbb{Z}$, und

$$1 = h\beta = \bar{x}^r\bar{a}^s \Longrightarrow \bar{x}^r = 1 = \bar{a}^s \Longrightarrow r = 0 \text{ und } n = o(\bar{a}) \mid s.$$

Da $a^n = 1$, folgt $a^s = 1$, also $h = x^r a^s = 1$. Damit ist $\ker\beta = 1$. □

9.10 Präsentation der symmetrischen Gruppe

Satz 9.11 (Präsentation der symmetrischen Gruppe)**.** *Sei $n \in \mathbb{N}$, $n > 1$. Dann ist*

$$S_n \cong G \coloneqq \left\langle x_1, \ldots, x_{n-1} \;\middle|\; \begin{array}{l} 1 = x_i^2 = (x_j x_{j+1})^3 = (x_k x_\ell)^2 \\ \textit{für } i = 1, \ldots, n-1,\ j = 1, \ldots, n-2,\ 1 \le \ell < k-1 < n-1 \end{array} \right\rangle.$$

Beweis. Beachte zuerst: Ist $x_k^2 = 1 = x_\ell^2$, so gilt

$$(x_k x_\ell)^2 = 1 \iff x_k x_\ell x_k x_\ell = 1 \iff x_k x_\ell = x_\ell^{-1} x_k^{-1} \iff x_k x_\ell = x_\ell x_k,$$

d. h. x_k und x_ℓ kommutieren.
Erzeuger von S_n mit diesen Relationen. Setze $\pi_i \coloneqq (i, i+1) \in S_n$ für $i = 1, \ldots, n-1$. Offensichtlich ist $\pi_i^2 = 1$. Für $j = 1, \ldots, n-2$ ist

$$\pi_j\pi_{j+1} = (j, j+1)(j+1, j+2) = (j, j+2, j+1)$$

ein 3-Zyklus, also $(\pi_j\pi_{j+1})^3 = 1$. Für $1 \le \ell < k-1$ ist $\ell + 1 < k$, also sind $\pi_\ell = (\ell, \ell+1)$ und $\pi_k = (k, k+1)$ disjunkte Zykel, d. h. $\pi_\ell\pi_k = \pi_k\pi_\ell$. Nach der Rechnung am Anfang ist damit $(\pi_k\pi_\ell)^2 = 1$. Also sind in S_n die entsprechenden Relationen erfüllt.
Wir zeigen noch $S_n = \langle \pi_1, \ldots, \pi_{n-1}\rangle$. Bekanntlich wird S_n von allen Transpositionen erzeugt. Eine Transposition hat die Form (i, j) mit $i < j$. Wir zeigen $(i, j) \in \langle \pi_1, \ldots, \pi_{n-1}\rangle$ durch Induktion über $j - i$.
Ist $j - i = 1$, so ist $j = i + 1$ und $(i, j) = (i, i+1) = \pi_i \in \langle \pi_1, \ldots, \pi_{n-1}\rangle$.
Sei nun $j - i > 1$ und die Behauptung wahr für alle $(\bar{\imath}, \bar{\jmath})$ mit $\bar{\jmath} - \bar{\imath} < j - i$. Dann ist $j > i + 1$, also $j - 1 > i$, aber $(j-1) - i < j - i$. Nach Induktionsannahme ist also $(i, j-1) \in \langle \pi_1, \ldots, \pi_{n-1}\rangle$, und damit

$$(i, j) = \underbrace{(j-1, j)}_{=\pi_{j-1}}(i, j-1)\underbrace{(j-1, j)}_{=\pi_{j-1}} \in \langle \pi_1, \ldots, \pi_{n-1}\rangle.$$

$G \cong S_n$. Nach dem Satz von Dyck existiert also ein Epimorphismus $\varphi\colon G \to S_n$ mit $x_i \mapsto \pi_i$. Wir zeigen, dass φ ein Isomorphismus ist, d. h. $\ker\varphi = 1$. Wegen $G/\ker\varphi \cong S_n$ ist $\frac{|G|}{|\ker\varphi|} = |S_n| = n!$. Es genügt also, $|G| \le n!$ zu zeigen. Wir benutzen Induktion nach n.
Für $n = 2$ ist $G = \langle x_1\rangle$ mit $x_1^2 = 1$, also $|G| \le 2 = 2!$.
Sei $n > 2$ und die Behauptung wahr für $n - 1$. Setze $H \coloneqq \langle x_1, \ldots, x_{n-2}\rangle \le G$ und

$$G_0 \coloneqq \left\langle x_1, \ldots, x_{n-2} \;\middle|\; \begin{array}{l} 1 = x_i^2 = (x_j x_{j+1})^3 = (x_k x_\ell)^2 \text{ für} \\ i = 1, \ldots, n-2,\ j = 1, \ldots, n-3,\ 1 \le \ell < k-1 < n-2 \end{array} \right\rangle.$$

Nach Induktionsannahme ist $|G_0| \leq (n-1)!$. Nach dem Satz von Dyck existiert ein Epimorphismus $G_0 \to H$, also ist $|H| \leq |G_0| \leq (n-1)!$. Es genügt also, $|G:H| \leq n$ zu zeigen, denn dann ist nach Lagrange

$$|G| = |H| \cdot |G:H| \leq (n-1)! \cdot n = n!.$$

Setze

$$\Omega_0 \coloneqq \{H,\ Hx_{n-1},\ Hx_{n-1}x_{n-2},\ \ldots,\ Hx_{n-1}x_{n-2}\cdots x_1\} \subseteq \Omega \coloneqq \{Hg : g \in G\}.$$

G operiert transitiv auf Ω durch Rechtsmultiplikation. Können wir zeigen, dass

$$(*) \qquad \alpha g \in \Omega_0 \quad \text{für alle } \alpha \in \Omega_0,\ g \in G,$$

so folgt $\Omega = \Omega_0$ und damit $|G:H| = |\Omega| = |\Omega_0| \leq n$. Wegen $G = \langle x_1, \ldots, x_{n-1}\rangle$ müssen wir für $(*)$ nur

$$\alpha x_j \in \Omega_0 \quad \text{für alle } \alpha \in \Omega_0 \text{ und } j = 1, \ldots, n-1$$

zeigen.
Sei $\alpha = Hx_{n-1}\cdots x_i \in \Omega_0$ mit $i \in \{1, \ldots, n\}$ (für $i = n$ ist hier $\alpha = H$ gemeint).
Fall $j < i-1$: Für $i \leq k \leq n-1$ gilt nach Definition von G, dass $(x_k x_j)^2 = 1$, nach der Rechnung am Anfang also $x_k x_j = x_j x_k$. Gleichzeitig ist $j \leq i-2 \leq n-2$, also $x_j \in H$. Damit folgt

$$\alpha x_j = Hx_{n-1}\cdots x_i\, x_j = Hx_j x_{n-1}\cdots x_i \overset{x_j \in H}{=} Hx_{n-1}\cdots x_i = \alpha.$$

Fall $j > i$: Wie vorher folgt aus der Definition von G, dass x_j mit $x_i, \ldots, x_{j-2}$ vertauschbar ist. Also ist

$$\alpha x_j = Hx_{n-1}\cdots x_{j+1}(x_j x_{j-1}) \underbrace{x_{j-2}\cdots x_i}_{\text{vertauschbar mit } x_j} x_j = Hx_{n-1}\cdots x_{j+1}(x_j x_{j-1} x_j)\, x_{j-2}\cdots x_i.$$

Wegen $(x_{j-1}x_j x_{j-1})(x_j x_{j-1} x_j) = (x_{j-1}x_j)^3 = 1$ und $x_j^2 = x_{j-1}^2 = 1$ gilt $x_j x_{j-1} x_j = x_{j-1} x_j x_{j-1}$, also

$$\alpha x_j = Hx_{n-1}\cdots x_{j+1}(x_{j-1}x_j x_{j-1})\, x_{j-2}\cdots x_i.$$

Ähnlich wie vorher vertauscht x_{j-1} mit $x_{j+1}, \ldots, x_{n-1}$. Da $x_{j-1} \in H$, folgt

$$\alpha x_j = \underbrace{Hx_{j-1}}_{=H}(x_{n-1}\cdots x_{j+1})(x_j x_{j-1})\, x_{j-2}\cdots x_i = Hx_{n-1}\cdots x_i = \alpha \in \Omega_0.$$

Fälle $j = i$ und $j = i-1$:

$$\alpha x_i = Hx_{n-1}\cdots x_{i+1}x_i x_i = Hx_{n-1}\cdots x_{i+1} \in \Omega_0,$$
$$\alpha x_{i-1} = Hx_{n-1}\cdots x_i x_{i-1} \in \Omega_0.$$

□

9.12 Endlich präsentierte Gruppen

Definition 9.13 (Endlich präsentierte Gruppe)**.** *Eine Gruppe heißt* **endlich präsentiert***, falls sie eine* **endliche Präsentation** *hat, d. h. eine Präsentation der Form $\langle X \mid R\rangle$ mit endlichen Mengen X und R.*

Lemma 9.14 (Endliche Erzeugendensysteme)**.** *Sei $G = \langle X\rangle = \langle Y\rangle$, wobei Y endlich ist. Dann existiert eine endliche Teilmenge $X_0 \subseteq X$ mit $G = \langle X_0\rangle$.*

Beweis. Sei $Y = \{y_1, \ldots, y_n\}$. Für $i \in \{1, \ldots, n\}$ ist $y_i \in G = \langle X\rangle$, kann also als Produkt von endlich vielen Elementen aus X und Inversen von Elementen aus X geschrieben werden. Für $i = 1, \ldots, n$ existiert also eine endliche Menge $X_i \subseteq X$ mit $y_i \in \langle X_i\rangle$. Setze

$$X_0 \coloneqq \bigcup_{i=1}^{n} X_i.$$

Dann ist $y_1, \ldots, y_n \in \langle X_0\rangle$, also $G = \langle y_1, \ldots, y_n\rangle = \langle X_0\rangle$, und X_0 ist endlich. □

Satz 9.15 (Wahl der Erzeuger)**.** *Sei G eine endlich präsentierte Gruppe und $X \subseteq G$ mit $G = \langle X \rangle$. Dann besitzt G eine endliche Präsentation der Form $\langle X_0 \mid R \rangle$ mit $X_0 \subseteq X$.*

Beweis. Sei $G = \langle y_1, \dots, y_m \mid s_1 = \cdots = s_k = 1 \rangle$ eine endliche Präsentation. Dann ist insbesondere $G = \langle y_1, \dots, y_m \rangle$, nach dem vorigen Lemma existiert also eine endliche Menge $X_0 \subseteq X$ mit $G = \langle X_0 \rangle$. Sei $n = |X_0|$ und $X_0 = \{x_1, \dots, x_n\}$, also $G = \langle x_1, \dots, x_n \rangle$.
Nun können die y_i durch $x_1, \dots, x_n$ und die x_j durch $y_1, \dots, y_m$ ausgedrückt werden, etwa

$$y_i = w_i(x) \quad (x = (x_1, \dots, x_n)), \qquad x_j = v_j(y) \quad (y = (y_1, \dots, y_m)).$$

Dann gelten die folgenden Relationen in $x_1, \dots, x_n$:

$$(*) \qquad s_i(w_1(x), \dots, w_m(x)) = 1 \quad (i = 1, \dots, k), \qquad x_j = v_j(w_1(x), \dots, w_m(x)) \quad (j = 1, \dots, n).$$

Sei

$$\bar{G} \coloneqq \langle \bar{x}_1, \dots, \bar{x}_n \mid s_i(w_1(\bar{x}), \dots, w_m(\bar{x})) = 1 \ (i = 1, \dots, k),\ v_j(w_1(\bar{x}), \dots, w_m(\bar{x}))\, \bar{x}_j^{-1} = 1 \ (j = 1, \dots, n) \rangle.$$

Nach dem Satz von Dyck und $(*)$ existiert ein Epimorphismus $\varphi\colon \bar{G} \to G$, $\bar{x}_j \mapsto x_j$.
Setze $\bar{y}_i \coloneqq w_i(\bar{x}) \in \bar{G}$. Dann gilt $s_i(\bar{y}_1, \dots, \bar{y}_m) = 1$ in $\bar{G}$ für $i = 1, \dots, k$. Nach dem Satz von Dyck existiert also ein Epimorphismus $\psi\colon G \to \bar{G}$, $y_i \mapsto \bar{y}_i$.
Zu zeigen ist $\varphi\psi = \mathrm{id}_{\bar{G}}$ und $\psi\varphi = \mathrm{id}_G$. In $\bar{G}$ gilt $\bar{x}_j = v_j(\bar{y}_1, \dots, \bar{y}_m)$ für $j = 1, \dots, n$. Also ist

$$\bar{x}_j \varphi\psi = x_j \psi = v_j(y_1, \dots, y_m)\psi = v_j(y_1\psi, \dots, y_m\psi) = v_j(\bar{y}_1, \dots, \bar{y}_m) = \bar{x}_j.$$

Da $\bar{G} = \langle \bar{x}_1, \dots, \bar{x}_n \rangle$, folgt $\varphi\psi = \mathrm{id}_{\bar{G}}$. Weiter ist

$$y_i \psi\varphi = \bar{y}_i \varphi = w_i(\bar{x})\varphi = w_i(x) = y_i,$$

also $\psi\varphi = \mathrm{id}_G$. Damit ist φ ein Isomorphismus.

> Ergänzung
>
> Also ist $\bar{G}$ eine endliche Präsentation von G mit den Erzeugern $x_1, \dots, x_n \in X_0 \subseteq X$.

□

Beispiel 9.16.

- Freie Gruppen über endlichen Mengen sind endlich präsentiert, durch $F(X) = \langle X \mid \emptyset \rangle$.
- Jede zyklische Gruppe ist endlich präsentiert, durch $\langle x \mid \emptyset \rangle$ oder $\langle x \mid x^n = 1 \rangle$ $(n \in \mathbb{N})$.
- Jede endliche Gruppe ist endlich präsentiert. Denn sei G endlich und $G = \langle X \rangle$ mit $X \subseteq G$ (z. B. $X = G$), und sei F frei auf X. Dann existiert $\pi\colon F \to G$ mit $\pi|_X = \mathrm{id}_X$, und es ist

  $$G = \langle X \mid \ker \pi \rangle, \quad \text{wobei } F/\ker \pi \cong G \text{ endlich ist.}$$

  Nach dem folgenden Lemma ist daher $\ker \pi$ endlich erzeugt.

Lemma 9.17 (Untergruppen von endlichem Index)**.** *Sei G eine endlich erzeugte Gruppe und $H \leq G$ mit $|G : H| < \infty$. Dann ist H endlich erzeugt.*

Beweis. Sei $G = \langle X \rangle$ mit $X \subseteq G$ endlich, und sei $\{1 = t_1, t_2, \dots, t_i\}$ ein **Rechtsschnitt** von H in G, d. h. $|G : H| = i$ und $Ht_1, \dots, Ht_i$ sind die Rechtsnebenklassen von H in G.
Ist $g \in G$, so ist die Abbildung $Ht_j \mapsto Ht_j g$ eine Permutation von $Ht_1, \dots, Ht_i$. Also existiert $\sigma \in \mathrm{Sym}(i)$ mit $Ht_j g = Ht_{j\sigma}$. Wir schreiben jg für $j\sigma$, d. h. $Ht_j g = Ht_{jg}$, und

$$t_j g = h(j, g)\, t_{jg} \quad \text{mit } h(j, g) \in H.$$

Für $g, h \in G$ gilt

$$Ht_{j(gh)} = Ht_j(gh) = (Ht_j g)h = (Ht_{jg})h = Ht_{(jg)h},$$

also $(jg)h = j(gh)$.
Wir zeigen $H = \langle h(j,g) : j = 1, \dots, i \text{ und } g \in X \cup X^{-1} \rangle$; das ist eine endliche Menge. Sei $a \in H$ und $a = y_1 \cdots y_k$ mit $y_l \in X \cup X^{-1}$ für $l = 1, \dots, k$. Dann ist

$$\begin{aligned} a = t_1 a = t_1 y_1 \cdots y_k &= h(1, y_1)\, t_{1y_1} y_2 \cdots y_k = \dots \\ &= h(1, y_1)\, h(1y_1, y_2) \cdots h(1y_1 \cdots y_{k-1}, y_k) \underbrace{t_{1y_1 y_2 \cdots y_k}}_{=t_{1a}}. \end{aligned}$$

Aber $Ht_{1a} = Ht_1 a = Ha = H = Ht_1$, also $t_{1a} = t_1 = 1$. Damit liegt a im Erzeugnis der $h(j,g)$. □

Satz 9.18 (P. Hall)**.** *Sei G eine Gruppe und $N \trianglelefteq G$, sodass N und G/N endlich präsentiert sind. Dann ist G endlich präsentiert.*

Beweis. Sei

$$N = \langle x_1, \dots, x_m \mid r_1, \dots, r_k \rangle \qquad \text{und} \qquad G/N = \langle y_1 N, \dots, y_n N \mid s_1, \dots, s_l \rangle.$$

Dann ist $G = \langle x_1, \dots, x_m, y_1, \dots, y_n \rangle$, und in G gelten die folgenden Relationen:

$$\begin{aligned} r_i(x) &= 1 && (i = 1, \dots, k), \\ s_j(y) &= t_j(x) \text{ für ein Wort } t_j(x) \text{ in } x_1, \dots, x_m && (j = 1, \dots, l), \\ y_j^{-1} x_i y_j &= u_{ij}(x) && (i = 1, \dots, m,\ j = 1, \dots, n), \\ y_j x_i y_j^{-1} &= v_{ij}(x) && (i = 1, \dots, m,\ j = 1, \dots, n). \end{aligned}$$

Sei $\bar{G}$ die Gruppe mit Erzeugern $\bar{x}_1, \dots, \bar{x}_m, \bar{y}_1, \dots, \bar{y}_n$ und den obigen Relationen, mit $\bar{x} = (\bar{x}_1, \dots, \bar{x}_m)$ anstelle von x und $\bar{y} = (\bar{y}_1, \dots, \bar{y}_n)$ anstelle von y. Nach dem Satz von Dyck existiert ein Epimorphismus $\alpha \colon \bar{G} \to G$ mit $\bar{x}_i \mapsto x_i$ und $\bar{y}_j \mapsto y_j$.
Wir zeigen, dass α ein Isomorphismus ist. Sei $K \coloneqq \ker \alpha$ und $\bar{N} \coloneqq \langle \bar{x}_1, \dots, \bar{x}_m \rangle$. Dann ist $\bar{N}\alpha = \langle x_1, \dots, x_m \rangle = N$.
$K \cap \bar{N} = 1$*:* Sei $w(\bar{x}) \in K \cap \bar{N}$. Dann ist $1 = w(\bar{x})\alpha = w(x) \in N$. Wegen $N = \langle x_1, \dots, x_m \mid r_1, \dots, r_k \rangle$ folgt, wenn F_N die freie Gruppe auf $\{x_1, \dots, x_m\}$ ist und $R = \{r_1, \dots, r_k\}$, dass $w \in R^{F_N}$. Also ist $w(\bar{x}) \in \bar{R}^{\bar{G}}$ mit $\bar{R} = \{r_1(\bar{x}), \dots, r_k(\bar{x})\}$. Wegen $r_i(\bar{x}) = 1$ in $\bar{G}$ (nach Definition von $\bar{G}$) folgt $w(\bar{x}) = 1$. Das zeigt $K \cap \bar{N} = 1$, also ist $\alpha|_{\bar{N}} \colon \bar{N} \to N$ ein Isomorphismus.
$\bar{N} \trianglelefteq \bar{G}$*:* Wegen $\bar{y}_j^{-1} \bar{x}_i \bar{y}_j \in \bar{N}$ und $\bar{y}_j \bar{x}_i \bar{y}_j^{-1} \in \bar{N}$ nach Definition von $\bar{G}$ ist $\bar{N} = \langle \bar{x}_1, \dots, \bar{x}_m \rangle \trianglelefteq \bar{G} = \langle \bar{x}_1, \dots, \bar{x}_m, \bar{y}_1, \dots, \bar{y}_n \rangle$.
$K \subseteq \bar{N}$*:* Sei $\pi \colon G \to G/N$, $g \mapsto gN$. Dann ist $\bar{N}\alpha = N = \ker \pi$, also $\bar{N} \subseteq \ker(\alpha\pi)$. Nach dem Homomorphiesatz induziert $\alpha\pi$ einen Epimorphismus

$$\bar{\alpha} \colon \bar{G}/\bar{N} \to G/N, \quad \bar{g}\bar{N} \mapsto \bar{g}\alpha\pi = (\bar{g}\alpha)N.$$

Insbesondere ist $(\bar{y}_j \bar{N})\bar{\alpha} = y_j N$. Sei $v(\bar{y}_1 \bar{N}, \dots, \bar{y}_n \bar{N}) \in \ker \bar{\alpha}$. Dann ist

$$v(y_1 N, \dots, y_n N) = v(\bar{y}_1 \bar{N}, \dots, \bar{y}_n \bar{N})\bar{\alpha} = 1_{G/N}.$$

Wegen $G/N = \langle y_1 N, \dots, y_n N \mid s_1, \dots, s_l \rangle$ sind alle Relationen in G/N Konsequenzen von $s_1, \dots, s_l$. Nach Definition von $\bar{G}$ gilt $s_j(\bar{y}_1 \bar{N}, \dots, \bar{y}_n \bar{N}) = 1_{\bar{G}/\bar{N}}$, also $v(\bar{y}_1 \bar{N}, \dots, \bar{y}_n \bar{N}) = 1$, d. h. $\ker \bar{\alpha} = 1$. Damit ist

$$K\bar{N}/\bar{N} \subseteq \ker \bar{\alpha} = 1 \Longrightarrow K \subseteq \bar{N} \Longrightarrow K = K \cap \bar{N} = 1.$$

Also ist α ein Isomorphismus.

Ergänzung

Da $\bar{G}$ endlich viele Erzeuger und Relationen hat, ist $G \cong \bar{G}$ endlich präsentiert.

□

Definition 9.19 (Polyzyklische Gruppe)**.** *Eine Gruppe G heißt* **polyzyklisch***, wenn es eine Kette*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

gibt, sodass G_i/G_{i-1} für $i = 1, \ldots, n$ zyklisch ist.

Korollar 9.20 (Polyzyklische Gruppen)**.** *Jede polyzyklische Gruppe ist endlich präsentiert.*

Beweis. Das folgt aus dem Satz von P. Hall durch Induktion über n. □

Hinweis zur Urheberschaft / Copyright Notice

Diese Zusammenfassung ist eine eigenständige Aufbereitung von Lehrinhalten und erhebt keinen Anspruch auf inhaltliche Eigenständigkeit.[1] This summary is an independent compilation of course content and makes no claim to originality of the underlying material.[2]

[1] Deutsch: Die in diesem Werk enthaltenen Inhalte basieren vollständig auf Vorlesungsskripten und -notizen von Prof. E. Henke; Auswahl, Aufbereitung und Darstellung stammen vom Autor. Bei Weitergabe, Vervielfältigung oder Verwendung dieses Werkes (auch auszugsweise) wird um einen Hinweis auf den Autor als Zusammensteller gebeten. Hinweise oder Korrekturen können per E-Mail an `mail@math.moschpit.de` geschickt werden.

[2] English: The content of this work is based entirely on the lecture scripts and notes of Prof. E. Henke; the selection, arrangement, and presentation are the author's own work. In the event of redistribution, reproduction, or use of this work (in whole or in part), a reference to the author as compiler is kindly requested. Feedback or corrections may be sent via email to `mail@math.moschpit.de`.