GRUPPENTHEORIE*

Prof. Goulnara Arzhantseva

goulnara.arzhantseva@univie.ac.at
Dienstag, 09:45 – 11:15, 11:30 – 12:15, SR 9.

1 Gruppenwirkungen

Erinnerung:

Definition 1.1. Eine Menge G ist eine *Gruppe*, wenn auf den Elementen eine Verknüpfung definiert ist, die die folgenden Axiome erfüllt:

- Assoziativgesetz: $\forall g, h, f \in G$ es gilt $\quad g * (h * f) = (g * h) * f$;
- Neutrales Element von G: $\exists e \in G$ so daß gilt $\quad \forall g \in G$ es gilt $e * g = g = g * e$;
- Inverses Element: $\forall g \in G\ \exists g^{-1} \in G$ so daß gilt $\quad g * g^{-1} = e = g^{-1} * g$.

Beispiele 1.2 (Gruppen).

1. Symmetrische Gruppe: Sei $X \neq \emptyset$ eine beliebige Menge. Man definiert
$$S_X = \{\phi\colon X \to X \mid \phi \text{ bijektiv } \}$$
Man nennt eine bijektive Abbildung $\phi\colon X \to X$ auch *Permutation* von X. Dann ist S_X zusammen mit der üblichen Verknüpfung (Hintereinanderausführung) von Abbildungen eine Gruppe, $(S_X, \circ)$, die sogenannte symmetrische Gruppe auf der Menge X. Falls $n \in \mathbb{N}$, so nimmt man typischerweise oft $\{1, 2, \ldots, n\}$ für X und schreibt S_n statt S_X, und man bezeichnet S_n als symmetrische Gruppe vom Grad n.
2. Automorphismengruppe: Die Menge aller Automorphismen einer Gruppe G zusammen mit der Komposition von Automorphismen bildet eine Gruppe, die so genannte Automorphismengruppe von G, geschrieben als Aut(G).
3. Isometriegruppen/Symmetriegruppen: Sei X ein metrischer Raum. Die Menge $Isom(X)$ aller bijektiven Isometrien von X auf sich selbst ist eine Gruppe bezüglich der Komposition (eine Untergruppe von der symmetrischen Gruppe $S(X)$). Zum Beispiel, die Diedrische Gruppe D_n ist die symmetrische Gruppe $Isom(P_n)$ von regelmässigen n-Ecken P_n.

*Neufassung: 3. Okt. 2016.

4. Matrizen-Gruppen: Seien R ein kommutativer Ring (mit Eins) und V ein R-Modul. Dann ist die Menge Aut(V) aller R-lineare Automorphismen von V mit der Komposition eine Gruppe. Besonders ist die Menge $GL(n, R) \cong \mathrm{Aut}(\mathrm{R^n})$ der invertierbaren $n \times n$-Matrizen über R eine Gruppe (bezüglich der Matrizenmultiplikation) für jede $n \in \mathbb{N}$. Ähnlich ist $SL(n, k)$ eine Gruppe.

5. Galoisgruppen: Sei $K \subseteq L$ eine Galoiserkörpererweiterung. Man nennt die Menge $\mathrm{Gal(L/K)} = \{\sigma \in \mathrm{Aut(L)} \mid \sigma\big|_{\mathrm{K}} = \mathrm{id_K}\}$ aller Körperautomorphismen von L, die den Grundkörper K elementweise festlaßen, bezüglich der Komposition, die *Galoisgruppe* von Körpererweiterung L über K.

6. Decktransformationen Gruppen: Sei $\pi\colon X \to Y$ eine Überlagerung eines topologischen Raums. Die Menge $\{f \in \mathrm{Abb(X, X)} \mid f$ ist ein Homöomorphismus mit $\pi \circ \mathrm{f} = \pi\}$ aller Decktransformationen der Überlagerung bildet eine Gruppe mit der Verknüpfung der Komposition, die Decktransformationsgruppe.

Gegeben seien eine Gruppe G und eine Menge X.

Definition 1.3 (Gruppenwirkung I)**.** Eine *Gruppenwirkung* von G auf X ist eine Abbildung

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

sodaß zusätzlich gilt

(i) $1 \cdot x = x \quad \forall x \in X$ (1 ist das neutrale Element der Gruppe);

(ii) $(gh) \cdot x = g \cdot (h \cdot x) \quad \forall g, h \in G, x \in X.$

Wenn gibt es eine Gruppenwirkung von G auf X, wir sagen G *wirkt auf* X und wir schreiben $G \curvearrowright X$. In dieser Fall bemerken wir dass jedes $g \in G$ induziert eine Bijektion auf X

$$\begin{aligned} g\colon\ & X \to X \\ & x \mapsto g \cdot x \end{aligned}$$

die oben (i) und (ii) erfült.

Alternative Definition ist die folgende. Seien G eine Gruppe, X eine Menge und S_X die Gruppe aller bijektiven Abbildungen von X nach X (Permutationen).

Definition 1.4 (Gruppenwirkung II)**.** Eine *Gruppenwirkung* von G auf X ist ein Homomorphismus $\alpha\colon G \to S_X, \quad g \mapsto \alpha(g)$.

Zusammenhang zwischen zwei Definitionen ist gegeben mit

$$\alpha(g)(x) = g \cdot x \quad \forall x \in X, \forall g \in G.$$

Beispiele 1.5 (Gruppenwirkungen).

1. S_n, die Gruppe aller Permutationen von $\{1, \ldots, n\}$, wirkt auf $\{1, \ldots, n\}$.

2. K ein Körper, $GL(n, K)$, die Menge aller invertierbaren $n \times n$ Matrizen über K, wirkt auf K^n durch Matrizenmultiplication. Tatsächlich, $A \in GL(n, K)$ dann ist $x \mapsto Ax$ eine bijektive Abbildung $K^n \to K^n$.

   Alternative Möglichkeit, sei $X = M(n, K)$, die Menge aller $n \times n$-Matrizen über K und $M \in X$. Es gibt zwei Wirkungen

   (a) : $M \mapsto AM$ (Multiplikation von links);

   (b) : $M \mapsto AMA^{-1}$ (Konjugation).

   Dann kann Man auf die $GL(n, K)$ einschränken, d.h. $X = GL(n, K)$.

3. Im Allgemeinen, jede Gruppe wirkt auf sich selbst durch

   (a) Multiplikation von links.
   Gegeben G und $X = G, \forall g \in G \quad \alpha(g) \colon x \mapsto gx, \forall x \in G$.

   (b) durch Konjugation.
   Gegeben G und $X = G, \forall g \in G \quad \alpha(g) \colon x \mapsto gxg^{-1}, \forall x \in G$.

4. $X = \mathbb{Z}_n$ (Restklassenring $\mod n$), $\mathbb{Z}_n^*$ die Gruppe der invertierbaren Elemente. $\mathbb{Z}_n^*$ wirkt auf $\mathbb{Z}_n$ durch Multiplikation: $\forall a \in \mathbb{Z}_n^*, \forall x \in \mathbb{Z}_n, \quad \alpha(a) \colon x \mapsto ax$.

5. G eine Gruppe, $H, K \leqslant G$ die Untergruppen, G/H die Menge der Linksnebenklassen nach H. Dann K wirkt auf G/H durch Linksmultiplikation: $k \in K, gH \in G/H$, $k \cdot gH = kgH$.

6. Wenn G auf X wirkt, dann automatisch auch auf Potenzmenge 2^X von X: $g \in G, Z \subseteq X, \quad g \cdot Z = \{g \cdot z \mid z \in Z\} \subseteq X$.

Sei G eine Gruppe die wirkt auf X.

Definition 1.6 (Bahn und Stabilisator)**.** Sei $x \in X$, dann heißt $O_x = G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X$ *Bahn* oder *Orbit* von x unter der Wirkung von G.
Es heißt $G_x = \{g \in G \mid g \cdot x = x\} \subseteq G$ der *Stabilisator* von x unter der Wirkung von G.

Es gilt:
• $G_x \leqslant G$, d.h. G_x ist Untergruppe von G.
• Die Menge der Bahnen bildet eine Zerlegung (oder Partition) von X. D.h. (i) jedes $x \in X$ liegt in einer Bahn; (ii) zwei Bahnen sind entweder disjunkt oder identisch. Die zu dieser Zerlegung gehörige Äquivalenzrelation ist gegeben durch

$$x \sim y \iff \exists g \in G \colon y = g \cdot x \quad (\text{bzw. } O_x = O_y)$$

Satz 1.7. *Seien $G \curvearrowright X$ und $x \in X$. Dann gibt es eine Bijektion zwischen O_x und G/G_x, die Menge aller Linksnebenklassen, gegeben durch $O_x \ni g \cdot x \mapsto g \cdot G_x \in G/G_x$.*
Insbesondere gilt, wenn G endlich ist, daß auch O_x endlich ist und $|O_x| = |G/G_x| = \frac{|G|}{|G_x|}$ und daher gilt auch $|O_x| \cdot |G_x| = |G|$.

Hier, $|U|$ = Anzahl der Elemente von U.

Beweis.

Definition ist sinnvoll: Angenommen $g \cdot x = h \cdot x$, (h^{-1} anwenden) $\Longrightarrow (h^{-1}g) \cdot x = x$, d.h. $h^{-1}g \in G_x \Longrightarrow hG_x = gG_x$.

Injektivität: Dies den Beweis von oben in die andere Richtung.

Surjektivität: Das ist klar, weil g beliebig.

□

Übung 1. Sei $X = M_{n,m}(K)$, die Menge aller $n \times m$-Matrizen über K. Die Gruppe $G = GL(n, K)$ wirkt auf X durch Multiplikation von links. Beschreiben Sie die Bahnen.

Sei $G \curvearrowright X$. Die Bahnen sind paarweise disjunkt, Vereinigung = X. Wenn X endlich,

$$|X| = \sum_{i=1}^{n} |O_i|,$$

wobei $O_1, \ldots, O_n$ alle Bahnen sind.

Unterscheide Bahnen, $Q_1, \ldots, Q_l$ sind jene Bahnen, die aus einem Element bestehen, $P_1, \ldots, P_q$ jene Bahnen, die aus mehr als einem Element bestehen. Bilde

$$X_0 := \sqcup_{i=1}^{l} Q_i \quad \Longrightarrow \quad |X| = |X_0| + \sum_{i=1}^{q} |P_i|.$$

Wir haben daß $X_0 = \{x \in X \mid g \cdot x = x\}$. $\forall i$ sei $x_i \in P_i$, dann $|P_i| = \frac{|G|}{|G_{x_i}|} = [G\colon G_{x_i}]$, der Index von G_{x_i} in G (= die Anzahl der Linksnebenklassen von G_{x_i} in G).

$$|X| = |X_0| + \sum_{i=1}^{q} |P_i|$$

$$|X| = |X_0| + \sum_{i=1}^{q} [G : G_{x_i}]$$

Beispiel 1.8. G endlich, $X = G$ und $G \curvearrowright X$ durch Konjugation: $\forall g, x \in G : g \cdot x = gxg^{-1}$. Dann $X_0 = \{x \in G \mid g \cdot x = x \ \forall g \in G\} = \{x \in G \mid gxg^{-1} = x \ \forall g \in G\} = \{x \in G \mid gx = xg \ \forall g \in G\} = Z(G)$, das *Zentrum* von G.

$G_x = \{g \in G \mid g \cdot x = x\} = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = C_G(x)$, der Zentralisator von x in G.

Definition 1.9 (Zentralisator)**.** G eine Gruppe, $Y \subseteq G$ eine Teilmenge, dann heißt die Menge

$$\{g \in G \mid gy = yg \ \forall y \in Y\} = C_G(Y)$$

der *Zentralisator von Y in G*

Im konkreten Fall, $|G| = |Z(G)| + \sum_{i=1}^{q}[G : C_G(x_i)]$. Zur Erinnerung: $x \sim y \iff \exists g \in G$ so daß $y = gxg^{-1}$ In dieser Situation heißen x und y zueinander *konjugiert*, die $\sim$-Klassen heißen *Konjugiertenklassen* bzw. Klassen konjugierte. Also ergibt sich

$$|G| = |Z(G)| + \sum_{i=1}^{q} |C_i|,$$

wenn C_i sind Konjugiertenklassen, die aus mehr als einem Element bestehen. Obige Formel wird die *Klassengleichung* genannt.

Satz 1.10 (Cauchy)**.** *Sei F endliche Gruppe, p Primzahl, $p \mid |F|$ (p dividiert $|F|$). Dann $\exists g \in F, g \neq 1$ mit $g^p = 1$ ($\implies \exists$ Untergruppen mit p Elementen).*

Beweis. Sei $X = \{(g_1, g_2, \ldots, g_p) \in F^p \mid g_1 g_2 \cdots g_p = 1\}$, es gilt $|X| = |F|^{p-1}$, denn $g_1, \ldots, g_{p-1}$ sind frei wählbar und g_p ist eindeutig gegeben durch $g_p = (g_1 g_2 \cdots g_{p-1})^{-1} \implies p \mid |X|$.

Sei $G = \mathbb{Z}_p$, dann G wirkt auf X via $k \cdot (g_1, \ldots, g_p) = (g_{1+k}, g_{2+k}, \ldots, g_p, g_1, \ldots, g_k)$, um k schiften.

Nebenrechnung: $g_1 \cdots g_p = 1$, dann $(g_1 \cdots g_k)^{-1} g_1 \cdots g_p (g_1 \cdots g_k) = (g_1 \cdots g_k)^{-1} \cdot 1 \cdot (g_1 \cdots g_k) = g_{k+1} g_{k+2} \cdots g_p g_1 \cdots g_k = 1$.

$|X| = |X_0| + \sum_{i=1}^{q} |P_i|$, wenn P_i besteht immer aus p Elementen, weil $|P_i| \mid |\mathbb{Z}_p|$, wobei $|\mathbb{Z}_p| = p$ und $|P_i| > 1$.

$|X_0| = |X| - qp \implies p \mid |X_0|$

$|X_0| = \{(g_1, \ldots, g_p) \in X \mid k \cdot (g_1, \ldots, g_p) = (g_1, \ldots, g_p)\ \forall k \in \mathbb{Z}_p\}$

$X_0 =$ die Menge aller p-Tupel in X für die gilt daß sie sich unter jeglicher zyklischer Vertauschung nicht ändern (alle Einträge gleich).

Es gilt $X_0 = \{(a, \ldots, a) \in X\} \neq \emptyset$, weil $(1, \ldots, 1) \in X_0 \implies$ es gibt $a \neq 1,\ a \in G$ mit $(a, a, \ldots, a) \in X \implies \exists a \neq 1$ mit $a^p = 1$. □

Definition 1.11 (p–Gruppe)**.** Sei p eine Primzahl, eine Gruppe G heißt p–Gruppe, wenn $\forall g \neq 1, g \in G$ gilt $\exists n \in \mathbb{N}, g^{p^n} = 1$, d.h. jedes Element hat endliche Ordnung und diese ist eine Potenz von p.

Korollar 1.12. *Eine endliche Gruppe ist genau dann eine p–Gruppe, wenn $|G| = p^n$ für ein $n \in \mathbb{N}$.*

Korollar 1.13. *Jede endliche p–Gruppe hat ein nicht triviales Zentrum, d.h. $|Z(G)| > 1$.*

Beweis. Sei G eine endliche p–Gruppe. Die Klassengleichung:

$$|G| = |Z(G)| + \sum_{i} [G : C_G(x_i)],$$

aber $|G|$ ist eine Potenz von p, $[G : C_G(x_i)] > 1$ und ein Teiler von $|G|$ (eine lauter Potenzen von p).

$1 \in Z(G) \implies |Z(G)| > 1 \implies |Z(G)| \geqslant p$. □

Korollar 1.14. *Sei p eine Primzahl. Jede Gruppe mit p^2 Elementen ist Abel'sch.*

Beweis. Angenommen G nicht Abel'sch. Dann $Z(G) \neq G$ und $Z(G)$ hat p Elemente. $Z(G) \trianglelefteq G$, die Faktorgruppe $g/Z(G)$ hat p Elemente $\Longrightarrow$ die Faktorgruppe ist zyklisch.

Sei $xZ(G)$ ein erzeugendes Element $\Longrightarrow G/Z(G) = \{xZ(G), x^2Z(G), \ldots, x^pZ(G)\}$. Aber $x^pZ(G) = Z(G)$ da ord(x) = p. Dann $G = xZ(G) \cup x^2Z(G) \cup \ldots \cup x^{p-1}Z(G) \cup Z(G)$.

Sei z ein erzeugendes Element von $Z(G) = \{z, z^2, \ldots, z^{p-1}, 1\}$. Dann

$$G = x\{z, z^2, \ldots, z^{p-1}, 1\} \cup x^2\{z, z^2, \ldots, z^{p-1}, 1\} \cup \ldots \cup x^{p-1}\{z, z^2, \ldots, z^{p-1}, 1\} \cup \{z, z^2, \ldots, z^{p-1}, 1\}$$

und $G = \{x^i z^j \mid 0 \leqslant i, j < p-1\}$. Es gilt $x^i z^j x^k z^l = x^{i+k} z^{j+l} = x^k z^l x^i z^j$, weil $z \in Z(G)$. □

Definition 1.15 (Normalisator)**.** Seien G eine Gruppe, $X \subseteq G$. Die Menge $N_G(X) = \{g \in G \mid gXg^{-1} = X\}$ heißt *Normalisator* von X in G.

Lasse G auf 2^G durch Konjugation wirken, dann ist $N_G(X)$ genau Stabilisator von X bezüglich dieser Wirkung. Es gilt (1) $N_G(X) \leqslant G$ eine Untergruppe, (2) $N_G(X) = \{g \in G \mid g^{-1}Xg = X\}$, (3) wenn $X \leqslant G$ eine Untergruppe, dann ist $N_G(X)$ die größte Untergruppe von G, in welcher X Normalteiler ist. Bahn von X ist $\{gXg^{-1} \mid g \in G\}$.

2 Sylow-Sätze

Sei p eine beliebige aber fix gewählte Primzahl.

Lemma 2.1. *Seien G eine endliche Gruppe, $H \leqslant G$ eine Untergruppe, H eine p–Gruppe. Dann gilt $[G : H] = [N_G(H) : H] (\mod p)$.*

Beweis. Benütze die Klassengleichung $|X| = |X_0| + \sum_i |P_i|$.

Sei $X = G/H = \{gH \mid g \in G\}$. Lassen H auf X wirken durch $H \ni h\colon gH \mapsto hgH$. $|H|$ ist Potenz von p, daher $p \big| |P_i|$

$X_0 = \{gH \mid \forall h \in H\ hgH = gH\}$, aber $hgH = gH$, $\forall h \in H \Leftrightarrow g^{-1}hg \in H\ \forall h \in H \Leftrightarrow g^{-1}Hg \subseteq H \Leftrightarrow g^{-1}Hg = H \Leftrightarrow g^{-1} \in N_G(H) \Leftrightarrow g \in N_G(H)$. Dann gilt $X_0 = \{gH \mid g \in N_G(H)\} = N_G(H)/H \Leftrightarrow g \in N_G(H)$ und $|X_0| = [N_G(H) : H]$ □

Satz 2.2 (1-ter Sylowsatz)**.** *Seien G eine Gruppe, $|G| = p^n r$ mit $(r, p) = 1$ (r relativ prim zu p). Dann gilt $\forall i \in \{0, 1, \ldots, n\}$ gibt es eine Untergruppe von G mit p^i Elementen. Wenn H eine Untergruppe von G mit p^i Elementen für $i < n$ ist, dann ist H normal in einer Untergruppe von G mit p^{i+1} Elementen (daher auch in dieser enthalten).*

Das heißt zu jeder Potenz q von p, die $|G|$ teilt, gibt es eine Untergruppe von G mit q Elementen.

Beweis. Die Behauptung für $i = 0$: $\{1\}$ hat p^0 Elemente. Nach Satz von Cauchy gibt es ein $g \in G$ mit ord(g) = p $\Rightarrow \{1\} \leqslant \langle g \rangle$.

Sei $i \in \{0, \ldots, n\}$, die Behauptung für $i - 1$ richtig. Es gibt eine Untergruppe H mit $|H| = p^{i-1}$ und $H \trianglelefteq K$ mit $|K| = p^i$.

Die Behauptung für i: Es gibt eine Untergruppe mit p^i Elementen. Dies folgt aus Induktionsannahme (= K).

Sei $H \leqslant G$ mit $|H| = p^i$. Zu zeigen: Wenn $i < n$, $\exists K$ mit $|K| = p^{i+1}$ und $H \trianglelefteq K$.

$$p^{n-i}r = \frac{|G|}{p^i} = [G : H] = [N_G(H) : H] \ (\mod p),$$

dann gilt $p \mid [N_G(H) : H] = |N_G(H)/H|$.

Daraus folgt: In $N_G(H)/H$ gibt es eine Untergruppe mit p Elementen, welche von der Form K/H für eine geeignete Untergruppe K von $N_G(H)$. $|K| = |K/H||H| = p \cdot p^i = p^{i+1}$.

H ist Normalteiler in K (Kann auch so geschaut werden $H \leqslant K \leqslant N_G(H)$. Daher H ist normal in K): es gilt $p = [K : H] = [N_K(H) : H] \ (\mod p) \Longrightarrow [N_K(H) : H]$ ist durch p teilbar ($\neq 0$). Dann $H \leqslant N_K(H) \leqslant K \Longrightarrow [N_K(H) : H] \leqslant [K : H] \Longrightarrow [N_K(H) : H] = p$.

$H \leqslant N_K(H) \leqslant K$, mittels Satz von Lagrange:

$$p = [K : H] = [K : N_K(H)][N_K(H) : H] = 1 \cdot p \implies K = N_K(H) \implies H \trianglelefteq K.$$

□

Definition 2.3 (p–Sylowuntergruppe)**.** Die Untergruppe von G ($|G| = p^n r$ mit $(p, r) = 1$) mit p^n Elementen heißen p–Sylowuntergruppen.

Jede p–Untergruppe von G in einer p-Sylowuntergruppe von G enthalten.

Satz 2.4 (2-ter Sylowsatz)**.** *Seien G eine endliche Gruppe, P eine p–Sylowuntergrupe, H eine beliebige p–Untergruppe. Dann gilt: $\exists g \in G$ so daß $gHg^{-1} \subseteq P$.*

Ist H eine p–Sylowuntergruppe, dann gilt $|H| = |P| \Longrightarrow gHg^{-1} = P$.

Beweis. Sei $X = \{gP \mid g \in G\}$. Lassen H auf X wirken, $h\colon gP \mapsto hgP$. Dann gilt $|X| = |X_0| (\mod p)$. Aber

$$\frac{|G|}{|P|} = \frac{p^n r}{p^n} = r \neq 0 (\mod p) \implies X_0 \neq \emptyset$$

Dann gilte: $\exists gP$ so daß $hgP = gP \ \forall h \in H$ und $g^{-1}hgP = P \ \forall h \in H \Longrightarrow g^{-1}hg \in P \ \forall h \in H \Longrightarrow g^{-1}Hg \subseteq P$. □

Proposition 2.5. *Die Anzahl der p–Sylowuntergruppen von G ist ein Teiler von $|G|$:*

$$\# = [G : N_G(P)] \text{ und } [G : N_G(P)] \mid |G|$$

Beweis. Menge der p–Sylowuntergruppen = Bahn von P unter der Konjugationswirkung von G auf 2^G. $|$ Bahn von $(P)| = [G : G_P]$ mit $G_P = \{g \in G \mid g^{-1}Pg\} = N_G(P)$, d.h. $[G : N_G(P)]$ ist die Anzahl der Elemente der Bahn von P. □

Satz 2.6 (3-ter Sylowsatz)**.** *Die Anzahl der p–Sylowuntergruppen von G ist kongruent zu* $1(\mod p)$ *(d.h. $\# = kp + 1$).*

Beweis. $P \leqslant N_G(P) \leqslant G$, dann $[G : P] = [G : N_G(P)][N_G(P) : P]$, also $[G : P] = [G : N_G(P)][N_G(P) : P](\mod p)$.

Wir wissen $[G : P] = [N_G(P) : P](\mod p) \implies [G : P] = r \neq 0(\mod p)$. Dann $1 \cdot [G : P] = [G : N_G(P)][G : P](\mod p)$, kann in $\mathbb{Z}_p$ dividieren: $1 = [G : N_G(P)](\mod p)$.

□

3 Semi-direktes Produkt

Sei $G \curvearrowright X$, wenn X eine Gruppe, wollen wir voraussetzen, daß alle Bijektionen $g\colon X \to X$ Automorphismen von X sind.

Notation: $g \in G, x \in X, \alpha\colon G \to S_X,\ g \mapsto \alpha(g)$ und $\alpha(g)\colon x \to \alpha(g)(x)$.

Wir sagen *G wirkt auf X durch Automorphismen* wenn G auf X wirkt, so daß $\alpha(g)\colon x \to \alpha(g)(x)$ ein Automorphismus von X ist $\forall g \in G$.

Anders formuliert: der Homomorphismus $\alpha\colon G \to S_X$, der die Wirkung definiert, hat die Eigenschaft $\alpha(G) \leqslant \mathrm{Aut(X)} \leqslant \mathrm{S_X}$.

Seien N, H zwei Gruppen und H wirkt auf N durch Automorphismen:

$$\alpha\colon H \to \mathrm{Aut(N)}.$$

Definition 3.1 (Externes semi-direktes Produkt)**.** Die kartesische Produkt $N \times H = \{(n, h) \mid n \in N, h \in H\}$ mit der Komposition

$$(n_1, h_1)(n_2, h_2) = (n_1\alpha(h_1)(n_2), h_1h_2)$$

ist eine Gruppe G, genannt das *externe (oder äußere) semi-direkte Produkt* von N mit H bezüglich α.

Notation: $G = N \rtimes_\alpha H$, das *externe* semi-direkte Produkt von N mit H bezüglich der Wirkung α.

Das neutrale Element ist $(1_N, 1_H)$, das inverse Element ist $(n, h)^{-1} = (\alpha(h^{-1})(n^{-1}), h^{-1})$. Das semi-direkte Produkt hängt von der Wirkung ab, d.h. $\alpha\colon H \to \mathrm{Aut(N)}$. Zum Beispiel, wenn $\alpha(h) = \mathrm{id}$ auf N, d.h. die triviale Wirkung, dann ist das externe semi-direkte Produkt das direkte Produkt.

Die Mengen $\widetilde{N} = \{(n, 1_H) \mid n \in N\}$ und $\widetilde{H} = \{(1_N, h) \mid h \in H\}$ sind Untergruppen dieses semi-direkten Produktes. Wir haben $\widetilde{N} \cong N$ und $\widetilde{H} \cong H$. Dann N, H sind mit Untergruppen von $N \rtimes_\alpha H$ zu identifizieren. N ist Normalteiler, H i.A. kein Normalteiler in G. H ist homomorphes Bild von $N \rtimes_\alpha H$, via Projektion auf 2-te Komponente. Der Kern dieser Projektion $= N$. Also $H \cong (N \rtimes_\alpha H)/N$.

Wir haben

(1) $N \trianglelefteq G$ und $H \leqslant G$;

(2) $G = N \cdot H$ und $N \cap H = \{1\}$.

(2) impliziert, jedes $g \in G$ läßt sich eindeutig darstellen als $g = nh$ mit $n \in N, h \in H$.

Tatsächlich, $g = nh = n_1h_1$ mit $n_1 \in N, h_1 \in H \implies N \ni n_1^{-1}n = h_1h^{-1} \in H \implies N \cap H \ni n_1^{-1}n = h_1h^{-1} = 1 \implies n_1 = n$ and $h_1 = h$. (surjektive: $G = N \cdot H$, injektive: $N \cap H = \{1\}$).

Definition 3.2 (Internes semi-direktes Produkt)**.** Eine Gruppe G heißt *internes semidirektes Produkt* von zwei Untergruppen N und H, falls gilt

1. $G = NH$;
2. $N \cap H = \{1\}$;
3. $N \trianglelefteq G$.

Dann gilt $G \cong N \rtimes_\alpha H$, wobei H auf N durch Konjugation wirkt: $h \in H$, $\alpha(h)\colon n \mapsto \alpha(h)(n) = hnh^{-1}$.

Es gilt $N \rtimes_\alpha H \ni (n, h) \mapsto nh \in G$ ist Bijektion wegen (2).

$(n, h)(n_1, h_1) = n \cdot hn_1h^{-1} \cdot hh_1 = n\alpha(h)(n_1)hh_1$, dann ist diese Abbildung ein Homomorphismus.

Beispiel 3.3 (Diedergruppe). Wir betrachten ein regelmäßiges n-Eck. Die Diedergruppe D_n definieren wir als die Gruppe aller Drehungen und Spiegelungen welche dieses regelmäßige n-Eck auf sich selbst abbilden. Dabei bezeichnen wir mit $d \in D_n$ die Drehung um $\frac{2\pi}{n}$ (gegen den Uhrzeigersinn) und mit $s \in D_n$ die Spiegelung an einer fest gewählten Symmetrieachse. Alle weiteren Drehungen in D_n erhalten wir als Potenzen d^k von d, alle weiteren Spiegelungen als Produkte d^ks einer Drehung und der Spiegelung s, wobei jeweils $k = 1, \ldots, n-1$. Wir haben n Drehungen, um $\frac{k2\pi}{n}, k = 0, \ldots, n-1$ und n Spiegelungen.

Die Diedergruppe D_n können wir also als $D_n = \{1, d, d^2, \ldots, d^{n-1}, s, ds, \ldots, d^{n-1}s\}$ darstellen. Insbesondere hat D_n die Ordnung $|D_n| = 2n$. Weiter bemerken wir $d^n = 1$, $s^2 = 1$ (also $s = s^{-1}$) und $sds = d^{-1}$. Die zyklische Untergruppe $C_n = \langle d \rangle = \{1, d, \ldots, d^{n-1}\}$ ist ein Normalteiler mit $[D_n : C_n] = 2$, da $sd^ks^{-1} = sd^ks = (sds)^k = d^{-k}$. Wir haben also $C_2 = \langle s \rangle$, $\langle s \rangle \cap \langle d \rangle = \{1\}$ und $\langle s \rangle \cdot \langle d \rangle = D_n$. So dass D_n das semidirekte Produkt von $\langle d \rangle$ und $\langle s \rangle$. Mit dem zugehörigen Gruppenhomomorphismus $\alpha\colon \langle s \rangle \to \mathrm{Aut}(\langle d \rangle)$ so dass $\alpha(1) = \mathrm{id}_{\langle d \rangle}$ und $\alpha(s)\colon \langle d \rangle \to \langle d \rangle, d \mapsto sds = d^{-1}$, D_n ist isomorph zum semidirekten Produkt $C_n \rtimes_\alpha C_2$ der zyklischen Gruppen C_n und C_2.

Beispiel 3.4 (Affine Gruppe). Die affine Gruppe $AGL(V)$ eines Vektorraumes V ist das semiderekte Produkt der Translationsgruppe $T(V)$ mit der Gruppe der Vektorraumautomorphismen $GL(V)$. Hier ist $T(V) = \{\tau_v \mid v \in V\}$ und τ_v bezeichnet die Translation $V \to V, x \mapsto v + x$.

Für jeden Vektorraum V operiert die allgemeine lineare Gruppe $GL(V)$ in natürlicher Wiese auf V. Das entsprechende semidirekte Produkt $V \rtimes GL(V)$ mit Verknüpfung

$$(v, f) \cdot (w, g) = (v + f(w), f \circ g)$$

ist durch

$$(v, f) \mapsto \tau_v \circ f$$

isomorph zur affinen Gruppe $AGL(V)$.

Beispiel 3.5 (Affine Gruppe: Dimension 2). Die Bewegungen in der euklidischen Ebene E: $x \mapsto Ox + t, \quad x \mapsto x + t$, eine orthogonale Abbildung O und eine Translation mit t. Dann $(t, O) \in E \times O(E)$.

Seien $(s, P), (t, O) \in E \times O(E)$ und $y = Ox + t$. Dann $y \mapsto Py + s = P(Ox + t) + s = POx + Pt + s$ so daß $PO \in O(E)$ und $Pt + s \in E$. Wir haben $(s, P) \circ (t, O) = (s + Pt, PO)$ und die Gruppe $E \rtimes O(E)$.

Definition 3.6 (Erweiterung / Exakte Sequenz)**.** Eine *Erweiterung* von N durch Q ist eine Gruppe G zusammen mit einem Monomorphismus (= Einbettung) $i\colon N \hookrightarrow G$ und einem Epimorphismus $\pi\colon G \twoheadrightarrow Q$, sodass das Bild von i mit dem Kern von π übereinstimmt. Anders gesagt: Die kurze Sequenz

$$1 \to N \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q \to 1$$

ist exakt.
Eine (längere) Sequenz

$$\cdots \xrightarrow{\phi_{i-1}} G_i \xrightarrow{\phi_i} G_{i+1} \xrightarrow{\phi_{i+1}} G_{i+2} \xrightarrow{\phi_{i+2}} \cdots,$$

G_i sind Gruppen, ϕ_i Homomorphismen, heißt *exakt*, wenn $\operatorname{im} \phi_i = \ker \phi_{i+1}$.

Hat man zwei Erweiterungen G und G' von N durch Q, so heißen diese *äquivalent*, falls es einen Isomorphismus $G \to G'$ gibt, der

$$\begin{array}{ccccc} & & G & \longrightarrow & Q & \longrightarrow & 1 \\ & & \downarrow & \searrow & \uparrow & & \\ 1 & \longrightarrow & N & \longrightarrow & G' & & \end{array}$$

kommutieren lässt.

Semi-direkte Produkte $G \cong N \rtimes_\alpha H$ sind immer Erweiterungen von N durch H. Aber nicht jede Erweiterung von N durch H ist semidirektes Produkt!

Definition 3.7 (Split-Erweiterung)**.** Eine *Erweiterung* G von N durch Q:

$$1 \to N \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q \to 1$$

heißt *spaltend* (oder *split*), wenn gibt es einen Homomorphismus (= eine Spaltung oder der Schnitt) $s\colon Q \to G$ so daß

$$\pi \circ s = \mathrm{id}_G.$$

Wenn die Erweiterung spaltet, dann ist die Gruppe ein semidirektes Produkt.

Übung 2.

(1) Zeige dass nicht jede Erweiterung spaltet.

(2) Zeige dass eine Erweiterung G von N durch Q ist spaltet wenn und nur wenn G ist das semidirekte Produkt von N mit Q.

Das Kranzprodukt ist ein spezielles semidirektes Produkt von Gruppen.

Definition 3.8 (Reguläre Kranzprodukt)**.** Seien G und H Gruppen. Sei

$$H^G := \{f \colon G \to H\}$$

die Menge alle Funktionen von G nach H. Bezüglich punktweiser Operationen: $(f_1 f_2)(x) := f_1(x) f_2(x)$ ist H^G eine Gruppe. Dann G wirkt auf H^G:

$$G \curvearrowright H^G, g \mapsto {}^g f \text{ mit } {}^g f(x) := f(xg).$$

Das *reguläre Kranzprodukt* $H \wr G$ von H mit G ist das semidirekte Produkt von H^G mit G bezüglich ebendieser Wirkung:

$$H \wr G := H^G \rtimes G.$$

Satz 3.9 (Kaluznin-Krasner'1950)**.** *Jede Erweiterung von H durch G kann in $H \wr G$ eingebettet werden.*

Beweis. Sei E eine Erweiterung von H durch G:

$$1 \to H \overset{i}{\hookrightarrow} E \overset{\pi}{\twoheadrightarrow} G \to 1.$$

Wir wollen eine Einbettung $E \hookrightarrow H \wr G = H^G \rtimes G$, die wir mit $E \ni c \mapsto (f_c, \overline{c}) \in H^G \rtimes G$ notieren. Wir haben daß

$$\begin{array}{ccccc} E & \overset{\pi}{\twoheadrightarrow} & G \cong E/H & \rightsquigarrow & E \\ \cup & & \cup & & \cup \\ c & \longmapsto & \overline{c} & \longmapsto & \overline{c}_r, \end{array}$$

wobei $\overline{c}$ ist das Bild von c unter Surjektion π und $\overline{c}_r$ ist Repräsentant der Nebenklasse $\overline{c} \in E/H$, also $\overline{\overline{c}_r} = \overline{c} \quad \forall c \in E$. Dabei wählen wir $\overline{1}_r = 1_H = 1_E$.

Wir definieren $f_c \colon G \to H$ durch $f_c(\overline{g}) := \overline{g}_r \cdot c \cdot \left(\overline{\overline{g}_r \cdot c}_r\right)^{-1}$. Nach Definition, $\overline{g}_r \in E$, $c \in E$, $\overline{\overline{g}_r \cdot c}_r \in E$.

- (1) Wir beweisen, daß $f_c(\overline{g}) \in H$.

Wir haben $f_c(\overline{g}) \in H \iff \overline{f_c(\overline{g})} = \overline{1}$. Tatsächlich, $\overline{\overline{g}_r \cdot c \cdot (\overline{\overline{g}_r \cdot c}_r)^{-1}} = \overline{\overline{g}_r \cdot c} \cdot \left(\overline{\overline{\overline{g}_r \cdot c}_r}\right)^{-1} = \overline{g \cdot c} \cdot \left(\overline{\overline{g}_r \cdot c}\right)^{-1} = \overline{g \cdot c} \cdot (\overline{g} \cdot \overline{c})^{-1} = \overline{1}$.

- (2) Wir beweisen, daß $c \longmapsto (f_c, \overline{c})$ ist ein Homomorphismus.

Wir haben $d \longmapsto (f_d, \overline{d})$ und $cd \longmapsto (f_{cd}, \overline{cd})$ und möchten beweisen, daß $(f_c, \overline{c})(f_d, \overline{d}) = (f_{cd}, \overline{cd})$ als Produkt in $H \wr G$. Nach Definition von Kranzprodukt, $(f_c, \overline{c})(f_d, \overline{d}) = (f_c {}^{\overline{c}} f_d, \overline{c}\overline{d})$. Aber haben wir $f_c {}^{\overline{c}} f_d \stackrel{?}{=} f_{cd}$. Dies ist äquivalent zu

$$f_c(\overline{g})^{\overline{c}} f_d(\overline{g}) \stackrel{?}{=} f_{cd}(\overline{g}) \quad \forall g \in E$$

Dies ist äquivalent zu

$$f_c(\overline{g}) f_d(\overline{gc}) \stackrel{?}{=} f_{cd}(\overline{g}) \quad \forall g \in E$$

und zu

$$\overline{g}_r \cdot c \cdot \left(\overline{\overline{g}_r \cdot c}_r\right)^{-1} \cdot \overline{gc}_r \cdot d \cdot \left(\overline{\overline{gc}_r \cdot d}_r\right)^{-1} \stackrel{?}{=} \overline{g}_r \cdot cd \cdot \left(\overline{\overline{g}_r cd}_r\right)^{-1} \quad \forall g \in E.$$

Aber

$$\left(\overline{\overline{g}_r \cdot c}_r\right)^{-1} \cdot \overline{gc}_r = \left(\overline{gc}_r\right)^{-1} \cdot \overline{gc}_r = 1_E = 1_H.$$

Dann müssen wir zeigen

$$\overline{g}_r \cdot cd \cdot \left(\overline{\overline{gc}_r \cdot d}_r\right)^{-1} \stackrel{?}{=} \overline{g}_r \cdot cd \cdot \left(\overline{\overline{g}_r cd}_r\right)^{-1} \quad \forall g \in E$$

und dies ist äquivalent zu

$$\overline{\overline{gc}_r \cdot d}_r \stackrel{?}{=} \overline{\overline{g}_r cd}_r \quad \forall g \in E.$$

Wir benutzen die Definition von Repräsentant: $\overline{gcd}_r = \overline{gcd}_r \quad \forall g \in E$.

• (3) Wir beweisen, daß $E \to H^G \rtimes G, c \longmapsto (f_c, \overline{c})$ ist injektive.

Angenommen, $(f_c, \overline{c}) = (\mathbf{1}, \overline{1})$ mit $\mathbf{1} \in H^G$ und $\overline{1} \in G$. Dann

$$(f_c, \overline{c}) = (\mathbf{1}, \overline{1}) \Longleftrightarrow f_c(\overline{g}) = 1_H, \quad \forall g \in E \text{ und } \overline{c} = \overline{1} \Longleftrightarrow f_c(\overline{g}) = 1_H, \quad \forall g \in E \text{ und } c \in H.$$

Für $g := 1$,

$$1_H = f_c(\overline{1}) = \overline{1}_r \cdot c \left(\overline{\overline{1}_r \cdot c}_r\right)^{-1} = c \cdot 1_E = 1_H \Longleftrightarrow c = 1.$$

□

Eigentlich das Kranzprodukt $H \wr G$ ist das reguläre Kranzprodukt. Es gibt auch das eingeschränkte Kranzprodukt und uneingeschränkte Kranzprodukt. Die folgende Definition ist allgemein.

Definition 3.10 (Uneingeschränkte Kranzprodukt)**.** Seien G und H zwei Gruppen, X eine Menge und $G \curvearrowright X$. Sei

$$H^X := \{f \colon X \to H\}$$

die Gruppe aller Abbildungen von X nach H mit punktweiser Verknüpfung (das direkte Produkt, die Menge aller $|X|$-tupel mit Elementen von H).
Dann G wirkt auf H^X:

$$G \curvearrowright H^X, g \stackrel{\alpha}{\longmapsto} {}^g f \text{ mit } {}^g f(x) := f(g^{-1}x).$$

Das *uneingeschränkte Kranzprodukt* $H \wr_X G$ (oder $H \operatorname{Wr}_X G$) von H mit G bezüglich $G \curvearrowright X$ ist das semidirekte Produkt von H^X mit G bezüglich ebendieser Wirkung:

$$H \wr_X G := H^X \rtimes_\alpha G.$$

Definition 3.11 (Eingeschränkte Kranzprodukt)**.** Seien G und H Gruppen, X eine Menge und $G \curvearrowright X$.
Sei

$$\bigoplus_X H := \{f\colon X \to H \text{ fast überall verschwinden, d.h. } f(x) = 1_H \text{ für fast alle } x \in X\}$$

die Gruppe aller Abbildungen von X nach H die fast überall verschwinden, mit punktweiser Verknüpfung. (Bemerkung: $\bigoplus_X H$ ist die Untergruppe von H^X). Dann G wirkt auf $\bigoplus_X H$:

$$G \curvearrowright \bigoplus_X H, g \overset{\alpha}{\longmapsto} {}^g f \text{ mit } {}^g f(x) := f(g^{-1}x).$$

Das *eingeschränkte Kranzprodukt* $H \wr_X G$ (oder $H \operatorname{wr}_X G$) von H mit G bezüglich $G \curvearrowright \bigoplus_X H$ ist das semidirekte Produkt von $\bigoplus_X H$ mit G bezüglich ebendieser Wirkung:

$$H \wr_X G := \bigoplus_X H \rtimes_\alpha G.$$

Jede Gruppe auf sich selbst durch Linksmultiplikation operiert. Dann für $X := G$ und $G \curvearrowright X$ durch Linksmultiplikation, $H \wr_X G = H \wr_r G = H \wr G$ das reguläre Kranzprodukt.

Die Gruppe H^X ist ein Normalteiler in $H \wr G$, da H^X ist der Kern der Projektion: $H \wr G \twoheadrightarrow G, (f, g) \longmapsto g$. Dieser Normalteiler heißt die *Basis(unter)gruppe des Kranzproduktes*. Ein Komplement der Basisgruppe in Kranzprodukte ist die *Topgruppe*.

Übung 3. Ist das direkte Produkt $H \times G$ eine normale Untergruppe von $H \wr_X G$? Bemerkung: wir haben die Diagonaleinbettung $\delta\colon H \hookrightarrow H^X, h \mapsto \delta_h$ mit $\delta_h\colon x \mapsto h$ (die konstante Funktion auf X); $\delta(H)$ ist eine normale Untergruppe in der Basisgruppe H^X, die auch normale im Kranzprodukt $H \wr_X G$.

Eigenschaften:

• Seien G und H endlichen Gruppen, $G \curvearrowright X, |X| < \infty$.

(1) Das Kranzprodukt $H \wr_X G$ ist eine Gruppe der Ordnung

$$|H \wr_X G| = |H|^{|X|} \cdot |G|.$$

(2) Ist P_H eine p-Sylowgruppe von H und P_G eine p-Sylowgruppe von G, so ist $P_H \wr_X P_G$ eine p-Sylowgruppe von $H \wr_X G$.

Tatsächlich, die Ordnung $|P_H \wr_X P_G| = |P_H|^{|X|}|P_G|$ ist die maximal in $H \wr_X G$.

• Sind $G_1 \leqslant G$ und $H_1 \leqslant H$ Untergruppen, so hat man $H_1 \wr_X G_1 \leqslant H \wr_X G$.

Speziell ist für die Basisgruppe $H^X \cong H \wr_X 1_G$ und für die Topgruppe $G \cong \mathbf{1}_{H^X} \wr G$.

• Ist $\pi\colon H \twoheadrightarrow \overline{H}$ ein Epimorphismus, so ist $\pi_\wr\colon H \wr_X G \twoheadrightarrow \overline{H} \wr_X G$ ein Epimorphismus mit $H \wr_X G \ni (f, g) \mapsto (\overline{f}, g)$ so daß $\overline{f}(x) := \pi(f(x))$ für $x \in X$.

Übung 4. Das Kranzprodukt ist assoziativ:

$$(H_1 \wr H_2) \wr H_3 \cong H_1 \wr (H_2 \wr H_3)$$

Hinweise:

1) $H_1 \curvearrowright X_1, H_2 \curvearrowright X_2, H_3 \curvearrowright X_3$, zu zeigen:

$$(H_1 \wr_{X_2} H_2) \wr_{X_3} H_3 \cong H_1 \wr_{X_2 \times X_3} (H_2 \wr_{X_3} H_3)$$

2) Seien G und H Gruppen, $G \curvearrowright X$ und $H \curvearrowright Y$. Dann $H \wr_X G \curvearrowright Y \times X$.
Zwar:

$$G \curvearrowright X \Longrightarrow G \curvearrowright Y \times X, g \longmapsto \{(y,x) \mapsto (y, g \cdot x)\}$$

$$H \curvearrowright Y \Longrightarrow H^X \curvearrowright Y \times X, f \longmapsto \{(y,x) \mapsto (f(x) \cdot y, x)\}$$

Dann: $H \wr_X G \curvearrowright Y \times X, (f,g) \longmapsto \{(y,x) \mapsto (f(x) \cdot y, g \cdot x\}$.
Achtung: für das reguläre Kranzprodukt gilt das Assoziativegesetz nicht!

4 Reihen und Zerlegungen

Definition 4.1 (Reihe oder Subnormalreihe)**.** Sei G eine Gruppe. Eine *Reihe* von G ist eine endliche Folge von Untergruppen von G so daß

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_l = G.$$

Die G_i heißen Terme, Elemente, Mitglieder der Reihe.
Wenn $G_i \ncong G_{i+1}, \ \forall i$, dann heißt l die *Länge* der Reihe.
Die Quotienten G_{i+1}/G_i heißen *Faktoren* der Reihe.

$\{1\} \trianglelefteq G$ ist, für jede Gruppe, immer eine Reihe.
Man kann daher für jede Gruppe die nichtleere Menge aller Reihen betrachten.

Definition 4.2 (Verfeinerung)**.** Eine Reihe $\mathcal{S}$ ist eine *Verfeinerung* der Reihe $\mathcal{T}$, wenn jedes Element von $\mathcal{T}$ auch Element von $\mathcal{S}$ ist.
Eine Reihe $\mathcal{S}$ ist *echte Verfeinerung*, wenn sie Verfeinerung ist und mindestens ein Element, das nicht in der ursprünglichen Reihe $\mathcal{T}$ vorkommt besitzt.

Beispiel 4.3. $\{1\} \trianglelefteq G \trianglelefteq G$ ist eine Verfeinerung von $\{1\} \trianglelefteq G$ aber keine echte.

Definition 4.4 (Isomorphe Reihen)**.** Zwei Reihen heißen *isomorph*, wenn es eine Bijektion zwischen den Faktoren der Reihen gibt, die jedem Faktor der einen Reihe einen isomorphen Faktor der anderen Reihe zuordnet.

Beispiel 4.5. Sei $G = \mathbb{Z}/6\mathbb{Z} = \{0,1,2,3,4,5\}$. Seien $\mathcal{S}\colon \{0\} \trianglelefteq \{0,2,4\} \trianglelefteq G$ und $\mathcal{T}\colon \{0\} \trianglelefteq \{0,3\} \trianglelefteq G$. Dann Faktoren von $\mathcal{S}\colon \{0,2,4\}/\{0\} \cong \mathbb{Z}/3\mathbb{Z},\ G/\{0,2,4\} \cong \mathbb{Z}/2\mathbb{Z}$ und Faktoren von $\mathcal{T}\colon \{0,3\}/\{0\} \cong \mathbb{Z}/2\mathbb{Z},\ G/\{0,3\} \cong \mathbb{Z}/3\mathbb{Z}$. Dann beiden Reihen sind isomorph.

Definition 4.6 (Kompositionsreihe)**.** Eine Reihe heißt *Kompositionsreihe*, wenn sie keine echte Verfeinerung besitzt. Die Faktoren heißen dann *Kompositionsfaktoren*.

Lemma 4.7. *Seien $H, K, L \leqslant G$ Untegruppen von G mit $K \leqslant L$, dann gilt*

$$(HK) \cap L = (H \cap L)K.$$

Beweis. '$\supseteq$': $H \cap L \subseteq H$ und $K \subseteq K \implies (H \cap L)K \subseteq HK$; Also $H \cap L \subseteq L$ und $K \leqslant L \Longrightarrow (H \cap L)K \subseteq L \cdot L = L$. Dann gilt auch, $(H \cap L)K \subseteq (HK) \cap L$.

'$\subseteq$': Sei $x \in (HK) \cap L$, also $L \ni x = hk \in HK \implies L \supseteq LK \ni xk^{-1} = h \in H$, daher $h \in H \cap L$. Wir haben daß $h \in H \cap L, k \in K$, daher $x = hk \in (H \cap L)K$. □

Lemma 4.8. *Seien $H, K, N \leqslant G$ Untergruppen von G mit $H \trianglelefteq K, N \trianglelefteq G$, dann gilt: $NH \trianglelefteq NK$.*

Beweis. Wir bemerken, daß NH und NK sind Untergruppen. Seien $n, m \in N$ und $k \in K, h \in H$, dann $(mk)(nh)(mk)^{-1} = m \cdot knk^{-1} \cdot khk^{-1} \cdot m^{-1} \in N \cdot N \cdot H \cdot N = 1_H \cdot N \cdot H \cdot N \in NH$ (Wir benutzen, daß $H \trianglelefteq K, N \trianglelefteq G$ und NH ist eine Untergruppe.) □

Lemma 4.9 (Lemma von Zassenhaus'1934)**.** *Seien $A_1 \trianglelefteq A_2 \leqslant G$ und $B_1 \trianglelefteq B_2 \leqslant G$. Dann gilt*

$$A_1(A_2 \cap B_1) \trianglelefteq A_1(A_2 \cap B_2) \text{ und } B_1(A_1 \cap B_2) \trianglelefteq B_1(A_2 \cap B_2)$$

und auch

$$A_1(A_2 \cap B_2)/A_1(A_2 \cap B_1) \cong B_1(B_2 \cap A_2)/B_1(A_1 \cap B_2).$$

Beweis. $B_1 \trianglelefteq B_2 \implies A_2 \cap B_1 \trianglelefteq A_2 \cap B_2$.

Es folgt aus $A_1 \trianglelefteq A_2$ und Lemma 4.8, daß $A_1(A_2 \cap B_1) \trianglelefteq A_1(A_2 \cap B_2)$. Aus Symmetrie, $B_1(A_1 \cap B_2) \trianglelefteq B_1(A_2 \cap B_2)$.

Für $N := A_1(A_2 \cap B_1)$ und $H := A_1(A_2 \cap B_2)$, nach Isomorphiesatz, $NH/N \cong H/(N \cap H)$.

Nach Lemma 4.7, $A_1(A_2 \cap B_1) \cap (A_2 \cap B_2) = (A_1 \cap A_2 \cap B_2)(A_2 \cap B_1) = (A_1 \cap B_2)(A_2 \cap B_1)$.

Daher, nach Isomorphiesatz,

$$A_1(A_2 \cap B_2)/A_1(A_2 \cap B_1) = A_1(A_2 \cap B_1)(A_2 \cap B_2)/A_1(A_2 \cap B_1) =$$

$$= NH/N \cong H/(N \cap H) = (A_2 \cap B_2)/\left(A_1(A_2 \cap B_1) \cap (A_2 \cap B_2)\right) =$$

$$= (A_2 \cap B_2)/\left((A_1 \cap B_2)(A_2 \cap B_1)\right).$$

Aus Symmetrie gilt dann auch

$$B_1(B_2 \cap A_2)/B_1(A_1 \cap B_2) \cong (A_2 \cap B_2)/(A_1 \cap B_2)(A_2 \cap B_1),$$

daraus folgt die behauptete Isomorphie. □

Satz 4.10 (Schreierscher Verfeinerungssatz'1928)**.** *Zwei beliebige Reihen einer Gruppe G besitzen isomorphe Verfeinerungen.*

Beweis. Seien

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_l = G$$

und

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq K_2 \trianglelefteq \cdots \trianglelefteq K_m = G$$

zwei Reihen von G. Setzen $H_{ij} := H_i(H_{i+1} \cap K_j)$ und $K_{ij} := K_j(H_i \cap K_{j+1})$ für alle i, j wo sinnvoll $0 \leqslant i \leqslant l-1$ und $0 \leqslant j \leqslant m-1$.

Für $A_1 := H_i \trianglelefteq H_{i+1} =: A_2$ und $B_1 := K_j \trianglelefteq K_{j+1} =: B_2$, nach Lemma von Zassenhaus, gilt $H_{ij} \trianglelefteq H_{i(j+1)}$, analog, $K_{ij} \trianglelefteq K_{(i+1)j}$, und die Faktoren sind isomorph:

$$H_{i(j+1)}/H_{ij} \cong K_{(i+1)j}/K_{ij}.$$

Die Extremfälle stimmen gerade mit den ursprünglichen Elementen überein:

$$H_{i0} = H_i = H_{(i-1)m} \text{ und } K_{0j} = K_j = K_{l(j-1)}.$$

Betrachte zu den $\{H_i\}_i$ und $\{K_j\}_j$ die folgenden Reinhen:

$$\{H_{ij} \mid (i,j) = (0,0), (0,1), \ldots, (0,m-1), (1,0), \ldots, (1,m-1), \ldots, (l-1,m-1)\},$$

insgesamt sind $l \cdot m$ Indizes in lexikographischer Ordnung;

$$\{1\} = H_{00} \trianglelefteq H_{01} \trianglelefteq \ldots \trianglelefteq H_{0(m-1)} \trianglelefteq H_{10} = H_1 \trianglelefteq \ldots$$

Analog,

$$\{K_{ij} \mid (i,j) = (0,0), (1,0), \ldots, (l-1,0), (0,1), \ldots, (l-1,1), \ldots, (l-1,m-1)\},$$

insgesamt sind $l \cdot m$ Indizes in inverser lexikographischer Ordnung.

Diese beiden Reihen sind isomorph nach Lemma von Zassenhaus. □

Definition 4.11 (Einfach Gruppe)**.** Eine Gruppe $G \neq \{1\}$ heißt *einfach*, wenn G keinen nicht trivialen Normalteiler hat (gilt genau dann, wenn 1_G und G die einzigen Normalteiler sind, oder wenn $\{1\} \trianglelefteq G$ eine Kompositionsreihe ist).

Eine Reihe ist genau dann Kompositionsreihe, wenn alle Faktoren einfach oder trivial.

Beispiele 4.12*.*

- $\mathbb{Z}$ hat keine Kompositionsreihe;
- Eine Kompositionsreihe hat maximal Länge.

Lemma 4.13. *Jede endliche Gruppe besitzt eine Kompositionsreihe.*

Beweis. Induktion nach Kardinalität von G.

1. $|G| = 1, G \cong \{1\} \implies G$ besitzt eine triviale Kompositionsreihe.
2. Induktionannahme: gilt $\forall G$ mit $|G| \leqslant n$.
3. Induktionschluss: sei G eine Gruppe mit $|G| = n + 1$.

a) G ist einfach $\implies \{1\} \trianglelefteq G$ ist eine Kompositionsreihe.

b) G ist nicht einfach $\implies \exists N \trianglelefteq G, N \neq \{1\}$. Dann $|N| \leqslant n$ und $|G/N| \leqslant n$, daher zwei Kompositionsreihe

$$\{1\} = H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_{k-1} \trianglelefteq H_k \cong N,$$

und

$$\{1\} = K_1/N \trianglelefteq K_2/N \trianglelefteq \ldots \trianglelefteq K_{l-1}/N \trianglelefteq K_l/N \cong G/N.$$

Daher

$$\{1\} \trianglelefteq = H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_{k-1} \trianglelefteq H_k \cong N = K_1 \trianglelefteq K_2 \trianglelefteq \ldots \trianglelefteq K_{l-1} \trianglelefteq K_l \cong G.$$

□

Satz 4.14 (Jordan'1868-Hölder'1889)**.** *Sei G eine endliche Gruppe. Wenn G eine Kompositionsreihe besitzt, dann läßt sich jede Reihe zu einer Kompositionsreihe verfeinern. Je zwei Kompositionsreihen sind isomorph.*

Bemerkung 4.15.

Jordan'1868: die Anzahl von Faktoren der Kompositionsreihe hängt nur ab von G.

Hölder'1889: die Faktoren der Kompositionsreihe hängen nur ab von G.

Beweis. Sei $\mathcal{S}$ eine Kompositionsreihe und $\mathcal{T}$ eine beliebige Reihe. Nach Schreierscher Verfeinerungssatz, es gibt isomorph Verfeinerugen $\mathcal{S}'$ und $\mathcal{T}'$ (von $\mathcal{S}$ und $\mathcal{T}$). Aber $\mathcal{S}$ ist eine Kompositionsreihe, dann $\mathcal{S}'$ und $\mathcal{S}$ sind isomorph. Wir haben

$$\mathcal{S} \cong \mathcal{S}' \cong \mathcal{T}'.$$

Dann gilt $\mathcal{T}'$ ist eine Kompositionsreihe. □

Die Kompositionsfaktoren von G sind bis auf Isomorphie nur von G aber nicht von der Reihe abhängig. Sei $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots$ eine Kompositionsreihe von G. Dann $G_0, G_1/G_0, G_2/G_1, \ldots$ sind einfach und G_1 ist Erweiterung von G_0 nach $G_1/G_0, G_2$ ist Erweiterung von G_1 nach G_2/G_1, etc.

Beispiel 4.16 (Jordan-Hölder Satz $\Rightarrow$ Fudamentalsatz der Arithmetik).

Fudamentalsatz der Arithmetik: Jede natürliche Zahl eine Primfaktorzerlegung besitzt und daß diese bis auf Reihenfolge der Faktoren eindeutig ist.

Beweis. Sei $\mathbb{N} \ni n = p_1 p_2 \cdots p_t$, wenn p_i nicht notwendigerweise verschieden primzahlen. Sei $G = \langle x \rangle \cong \mathbb{Z}/n\mathbb{Z}$. Dann

$$G = \langle x \rangle \geqslant \langle x^{p_1} \rangle \geqslant \langle x^{p_1 p_2} \rangle \geqslant \cdots \geqslant \langle x^{p_1 p_2 \cdots p_t} \rangle \geqslant \{1\}$$

ist eine Kompositionsreihe. Nach Jordan-Hölder Satz $p_1, p_2, \ldots, p_t$ hängen nur ab von n. □

5 Auflösbare, Nilpotente, p-Gruppen

Definition 5.1 (Auflösbar Gruppe)**.** Eine Gruppe G heißt *auflösbar*, wenn eine Reihe existiert

$$\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \ldots \trianglelefteq G_1 \trianglelefteq G_0 = G$$

mit G_i/G_{i+1} abel'sch.

Beispiele 5.2.

1. Jede abelsche Gruppe ist in trivialer Weise auflösbar.
2. Die symmetrische Gruppe S_4 ist auflösbar. Eine Reihe ist $\{1\} \trianglelefteq \mathbb{Z}_2 \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$. Hier sind
$$V_4 := \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$
die Kleinsche Vierergruppe, die kleinste nicht-zyklische Gruppe, und A_4 die alternierende Gruppe vom Grad 4 allen geraden Permutationen einer 4 elementigen Menge. Es gilt $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ und $A_4/V_4 \cong \mathbb{Z}_3$ und $S_4/A_4 \cong \mathbb{Z}_2$.
3. Die alternierende Gruppe $A_n, n \geqslant 5$ ist nicht auflösbar. Diese Gruppe keinen echten nichttrivialen Normalteiler besitzt (einfach ist). Also kann es keine Reihe mit abelschen Faktoren geben.

Sei G eine Gruppe. Für $x, y \in G$ nennt man $[x, y] = xyx^{-1}y^{-1}$ den Kommutator von x und y. (In manchen Büchern definiert man $[x, y] = x^{-1}y^{-1}xy$.) Seien $X, Y \subseteq G$,

$$[X, Y] = \langle [x, y] \mid x \in X, y \in Y \rangle$$

die Teilmenge von G erzeugt von den Kommutatoren.

Bemerkung 5.3. Es sei G eine Gruppe, $S \subseteq G$ eine Teilmenge. Hier ist $\langle S \rangle$ die kleinste Untergruppe von G, die S enthält. Mit anderen Worten, wenn $H \subseteq G$ eine Untergruppe mit $S \subseteq H$ ist, so ist auch $\langle S \rangle \subseteq H$. $\langle S \rangle$ heißt die von S *erzeugte Untergruppe* oder kurz das *Erzeugnis* von S.

Es gilt:

- $[X, Y] = [Y, X]$ (weil $[x, y]^{-1} = [y, x]$);
- Für jeden Gruppen homomorphismus $f\colon G \to H$ ist $f([X, Y]) = [f(X), f(Y)]$;
- Sind X und Y normale oder charakteristische (siehe unten) Untergruppen von G, so ist der Kommutator $[X, Y]$ eine normale oder charakteristische Untergruppe von G;
- Für Untergruppen X und Y einer Gruppe G gilt stets $[X, Y] \trianglelefteq \langle X, Y \rangle \leqslant G$.

  Beweis. Für beliebige $x, x' \in X, y \in Y$, gilt $x[x', y]x^{-1} = xx'y(x')^{-1}y^{-1}x^{-1} = xx'y(x')^{-1} \cdot x^{-1}y^{-1}yx \cdot y^{-1}x^{-1} = [xx', y][x, y]^{-1} \in [X, Y]$. Analog ist $y[X, Y]y^{-1} \subseteq [X, Y]$. □

Definition 5.4 (Vollinvarianten/charakteristischen Untergruppen)**.** Seien G eine Gruppe, $H \leqslant G$ eine Untergruppe.
H heißt *voll invariant*, wenn die unter jedem Endomorphismus (surjektiven Homomorphismus von G nach G) fest bleibt.
H heißt *charakteristische*, wenn die jedem Automorphismus (bijektiven Gruppenhomomorphismus von G nach G) von G fest bleibt.

Jede charakteristische Untergruppe ist Normalteiler, denn sie bleibt insbesondere fest unter jedem inneren Automorphismus. Jede vollinvariant Untergruppe ist also charakteristisch, jedoch nicht umgekehrt.

Übung 5. Für jede Gruppe G ist das Zentrum $Z(G)$ charakteristisch, aber nicht notwendig vollinvariant in G.

Lemma 5.5. *Für Untergruppen H, K einer Gruppe G mit $K \leqslant H \leqslant G$ gilt:*
(i) K ist charakteristisch (vollinvariant) in H und H ist charakteristisch (vollinvariant) in G, dann folgt K ist charakteristisch (vollinvariant) in G.
(ii) K ist charakteristisch in H und $H \trianglelefteq G$, dann folgt $K \trianglelefteq G$.

Beweis. (i) Sei K charakteristisch in H, H charakteristisch in G und $f \in Aut(G)$. Dann ist $f(H) \subseteq H = f(f^{-1}(H)) \subseteq f(H)$, also $f(H) = H$. Daher ist die Einschränkung f' von f ein Automorphismus von H. Folglich ist $f(K) = f'(K) \subseteq K$. Analog für vollinvariante Untergruppen.

(ii) Sei K charakteristisch in H, $H \trianglelefteq G$ und $g \in G$. Dann ist die Abbildung $f\colon H \to H$, $h \mapsto ghg^{-1}$ ein Automorphismus von H. Also ist $gKg^{-1} = f(K) \subseteq K$. □

Die von allen Kommutatoren $[x, y] = xyx^{-1}y^{-1}$ erzeugte Untergruppe $G^{(1)} = [G, G] = G'$ heißt *Kommutatorgruppe* von G (manchmal auch "abgeleitete Gruppe", englisch "derived group"). Wegen $[x, y]^{-1} = [y, x]$ ist das Inverse eines Kommutators wieder ein Kommutator; deshalb besteht die Kommutatorgruppe von G aus allen Produkten (beliebiger Länge) von Kommutatoren (beim Erzeugnis werden keine Inversen der Erzeuger benötigt).

Die Bedeutung der Kommutatorgruppe für die Auflösbarkeit von Gruppen ergibt sich aus des folgenden Satzes:

Proposition 5.6. *(i) Die Kommutatorgruppe G' einer Gruppe G ist eine charakteristische Untergruppe von G, insbesondere ein Normalteiler.*
(ii) Es sei $N \trianglelefteq G$ ein Normalteiler. Dann ist die Faktorgruppe G/N abel'sch genau dann, wenn $G' \subseteq N$ ist. Insbesondere, $G^{(1)}$ ist der kleinste Normalteile mit abelscher Faktorgruppe $G/G^{(1)}$.
(iii) Es sei $f\colon G \to A$ ein Homomorphismus, wobei A abel'sch ist. Dann ist $G' \subseteq \operatorname{Ker} f$.

Iteriert man die Kommutatorgruppenbildung: höhere Kommutatoruntergruppen

$$G^{(i+1)} = [G^{(i)}, G^{(i)}]$$

und

$$G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \dots$$

abgeleitete Reihe.

Wir zeigen per Induktion nach i und nach Lemma 5.5 (i) dass alle $G^{(i)}$ sind voll invariante (dann charakteristische) Untergruppen, daher Normalteiler.

Zunächst deshalb einige ergänzende Überlegungen zu höheren Kommutatorgruppen:

Lemma 5.7.

- *(i) Für höhere Kommutatorgruppen ist folgendes richtig: $H \leqslant G$, dann $H^{(n)} \leqslant G^{(n)}$;*
- *(ii) $N \trianglelefteq G$, dann es gilt $(G/N)^{(n)} = (G^{(n)} \cdot N)/N \cong G^{(n)}/(G^{(n)} \cap N)$;*
- *(iii) $(G \times H)^{(n)} = G^{(n)} \times H^{(n)}$.*

Beweis. (i) und (iii) sind mit Induktion sofort klar.
(ii) Induktion nach n:
(1) $n = 0$: dieser Fall ist klar wegen $G^{(0)} = G$.
(2) $n > 0$:

$$\begin{aligned}
(G/N)^{(n)} &= [(G/N)^{(n-1)}, (G/N)^{(n-1)}] \\
&= [(G^{(n-1)}N)/N, (G^{(n-1)}N)/N] \\
&= [\{gN \mid g \in G^{(n-1)}\}, \{gN \mid g \in G^{(n-1)}\}] \\
&= \langle [g_0N, g_1N] \mid g_i \in G^{(n-1)} \rangle \\
&= \langle [g_0, g_1]N \mid g_i \in G^{(n-1)} \rangle \\
&= (G^{(n)} \cdot N)/N.
\end{aligned}$$

□

Dann folgt

Proposition 5.8.

1. *Gibt es $n \in \mathbb{N}$ mit $G^{(n)} = \{1\}$, dann gilt auch für jede ihrer Untergruppen $H^{(n)} = \{1\}$, und auch für jede Faktorgruppe ist $(G/N)^{(n)} = \{1\}$.*
2. *Sind $G_1, \ldots, G_m$ Gruppen mit $G_i^{(n_i)} = \{1\}$, $n = kgV\{n_i \mid 1 \leqslant i \leqslant m\}$, dann ist*
$$(G_1 \times \cdots \times G_m)^{(n)} = \{1\}.$$
3. *Ist $N \trianglelefteq G$ und $N^{(r)} = (G/N)^{(n)} = \{1\}$, dann ist $G^{(n+r)} = \{1\}$.*

Satz 5.9. *Eine Gruppe G ist genau dann auflösbar, wenn und nur wenn ein $n \in \mathbb{N}$ existiert derart, dass die höhere Kommutatorgruppe $G^{(n)} = \{1\}$ ist.*

Das kleinste n, für welches das gilt, heißt die *abgeleitete Länge* ("derived length") der auflösbaren Gruppe G, bezeichnet durch $dl(G)$.

Beweis. ($\Rightarrow$) Sei zunächst G auflösbar. Es gibt also eine Reihe

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}, \text{ mit abel'schen Faktoren } G_i/G_{i+1}.$$

Wir zeigen $G^{(i)} \subseteq G_i$: da $G_n = \{1\}$ folgt dann die Behauptung. Wir verfahren per Induktion nach $i, 0 \leqslant i \leqslant n$. Für $i = 0$ ist $G^{(0)} = G = G_0$. Sei also $i > 0$. Nun ist G_{i-1}/G_i abel'sch, womit $G^{(i-1)} \subseteq G_i$ gilt. Weiterhin ist nach Induktionsvoraussetzung $G^{(i-1)} \subseteq G_{i-1}$, womit

$$G^{(i)} = (G^{(i-1)})' \subseteq (G_{i-1})' \subseteq G_i$$

ist.

($\Leftarrow$) Ist umgekehrt $G^{(n)} = \{1\}$, dann bilden die höheren Kommutatorgruppen die Reihe

$$G = G_0 = G^{(0)} \trianglerighteq G_1 = G^{(1)} \trianglerighteq \cdots \trianglerighteq G_n = G^{(n)} = \{1\}, \text{ mit abel'sch Faktoren } G_i/G_{i+1}.$$

□

Nach Proposition 5.8 und Satz 5.9, die Klasse aller auflösbaren Gruppen ist abgeschlossen unter $\mathcal{S}$ (Untergruppen), $\mathcal{H}$ (homomorphe Bilder), $\mathcal{E}$ (Erweiterungen), unter Bildung von endlichen direkten Produkten und beliebige Potenzen ($\prod_{i\in I} G$).

Wir haben
$dl(H) \leqslant dl(G)$ für $H \leqslant G$,
$dl(G/N) \leqslant dl(G)$ für $N \trianglelefteq G$,
$dl(G) \leqslant dl(N) + dl(G/N)$ für eine Erweiterung von N durch G/N.

Bemerkung 5.10.

1. Jede Verfeinerung von eine Reihe mit abel'schen Faktoren ist auch mit abel'schen Faktoren. Dann jede auflösbar Gruppe G mit eine Kompositionreihe endlich ist.

2. Eine endliche Gruppe G ist genau dann auflösbar wenn die Faktoren einer (jeder) Kompositionreihe zyklisch mit Primzahlordnung sind.

3. G ist genau dann nicht auflösbar, wenn gibt es Untergruppen H und K so daß $H \trianglelefteq K \trianglelefteq G$ und K/H einfach, nicht abel'sch (c.f. Beispiel 5.2).

4. Jede endliche p-Gruppe ist auflösbar. Tatsächlich, per Induktion nach $|G|$. G hat ein nichttriviales Zentrum (nach Klassengleichung), dann folgt $|G/Z(G)| < |G|$. $Z(G)$ ist abel'sch, dann auflösbar. $G/Z(G)$ ist eine p-Gruppe, dann auflösbar nach Induktion. G ist eine Erweiterung von $Z(G)$ durch $G/Z(G)$, dann folgt G ist auflösbar.

Übung 6. $GL(n, K)$ ist nicht auflösbar (außer wenn $n = 2$ und $|K| = 2, 3$).

Sei $X = \{x_1, x_2, \ldots, \}$, definieren durch Induktion Wörter $w_n = w_n(x_1, \ldots, x_{2^n})$: $w_1(x_1, x_2) = [x_1, x_2]$, ist w_n schon definiert $w_n^* = w_n(x_{2^n+1}, \ldots, x_{2^{n+1}})$ und $w_{n+1} = [w_n, w_n^*]$.

Zum Beispiel $w_2 = [[x_1, x_2], [x_3, x_4]]$, $w_3 = [[[x_1, x_2], [x_3, x_4]], [[x_5, x_6], [x_7, x_8]]]$, etc.

Notation. $G \models w_i = 1 \iff \forall g_1, \ldots, g_{2^i} \in G$ es gilt $w_i(g_1, \ldots, g_{2^i}) = 1$ in G.

Wir zeigen per Induktion nach n:

Satz 5.11. *Eine Gruppe G ist genau dann auflösbar (mit abgeleiteter Länge $\leqslant n$), wenn und nur wenn ein $n \in \mathbb{N}$ existiert derart, dass $G \models w_n = 1$ gilt.*

Abschließend führen wir noch zwei weitere berühmte Sätze auf, werden diese aber nicht beweisen.

Satz 5.12 (von Burnside)**.** *Alle Gruppen der Ordnung $p^k q^l$ mit Primzahlen p, q und $k, l \in \mathbb{N}$ sind auflösbar.*

Satz 5.13 (von Feit-Thompson)**.** *Alle Gruppen ungerader Ordnung sind auflosbar.*

Der letzte Satz wurde im Jahr 1963 von Feit und Thompson bewiesen, der Originalbeweis ist inklusive aller Hilfssätze 274 Seiten lang. Ein kurzer Beweis dieses Satzes wird nach wie vor dringend gesucht.

Definition 5.14 (Zentralreihe)**.** Eine Normalreihe

$$\{1\} = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_{n-1} \leqslant G_n = G,$$

(d.h. $\forall i \;\; G_i \trianglelefteq G$) heißt *Zentralreihe* wenn $\forall i \;\; G_i/G_{i-1} \leqslant Z(G/G_{i-1})$.
Eine Gruppe G heißt *nilpotent* wenn G eine Zentralreihe besitzt.
Die Länge der kürzesten Zentralreihe von G heißt *Nilpotenzklasse* von G.

Definition 5.15 (Absteigende Reihe)**.** Die *absteigende* Zentralreihe

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

wird rekursiv definiert durch $\gamma_1(G) = G$ und $\gamma_{i+1}(G) = [\gamma_i(G), G]$.

Nach Definition: $\gamma_1(G) = G$ und $\gamma_2(G) = G^{(1)} = G'$.
Per Induktion nach i: $\gamma_{i+1}(G) \leqslant \gamma_i(G)$. Das ist klar für $i = 1$. Dann $[\gamma_{i-1}(G), G] \leqslant \gamma_{i-1}(G)$ und es folgt $\gamma_{i+1}(G) = [\gamma_i(G), G] = [[\gamma_{i-1}(G), G], G] \leqslant [\gamma_{i-1}(G), G] = \gamma_i(G)$.

Definition 5.16 (Aufsteigende Reihe)**.** Die *aufsteigende* Zentralreihe

$$\{1\} = Z_0(G) \leqslant Z_1(G) \leqslant Z_2(G) \leqslant Z_3(G) \leqslant \ldots$$

wird rekursiv definiert durch $Z_1(G) = Z(G)$ und Z_{i+1} ist definiert durch

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)).$$

Die aufsteigende Reihe ist sicher eine Zentralreihe, nach Definition.

Lemma 5.17. $\forall i \;\; Z_i(G)$ *ist charakteristisch in* G.

Beweis. Per Induktion nach i: $i = 0, i = 1$ sind klar. Ist $Z_{i-1}(G) \subseteq G$ charakteristisch für ein i, so induziert jedes $f \in \mathrm{Aut(G)}$ ein $\overline{f} \in \mathrm{Aut(G/Z_{i-1}(G))}$ mit $\overline{f}(gZ_{i-1}(G)) = f(g)Z_{i-1}(G) \;\; \forall g \in G$. Da $Z(G/Z_{i-1}(G)) \subseteq G/Z_{i-1}(G)$ charakteristisch ist, folgt:

$$\overline{f}(Z_i(G)/Z_{i-1}(G)) = Z_i(G)/Z_{i-1}(G).$$

Folglich: $f(g) \in Z_i(G)$ für $g \in Z_i(G)$. □

Lemma 5.18.

1. $H \leqslant G \Longrightarrow \gamma_i(H) \leqslant \gamma_i(G) \;\; \forall i$;
2. *Sei* $f\colon G \to H$ *ein Homomorphismus. Es gilt* $f(\gamma_i(G)) = \gamma_i(f(G)) \leqslant \gamma_i(H) \;\; \forall i$.

Insbesondere ist $\forall i \;\; \gamma_i(G)$ voll invariant in G. Es folgt: $\gamma_i(G) \trianglelefteq G \;\; \forall i$.

Proposition 5.19. *Die absteigende Reihe ist eine Zentralreihe.*

Beweis. Per Induktion nach i. Sei $\gamma_{i+1}(G) \ni x = y_1 \dots y_k$ mit $y_j = a^{-1}b^{-1}ab, a \in \gamma_i(G), b \in G$.

Sei $z \in G$. Es gilt $z^{-1}y_jz = z^{-1}a^{-1}b^{-1}abz = z^{-1}a^{-1}z \cdot z^{-1}b^{-1}z \cdot z^{-1}az \cdot z^{-1}bz \in [\gamma_i(G), G]$ weil $z^{-1}a^{-1}z \in \gamma_i(G)$. Dann $\gamma_i(G) \trianglelefteq G \;\; \forall i$. (siehe auch oben). Wir haben auch $\gamma_{i+1}(G) \leqslant \gamma_i(G)$.

Das folgt: $[G/\gamma_{i+1}(G), \gamma_i(G)/\gamma_{i+1}(G)] = [G, \gamma_i(G)]\gamma_{i+1}(G)/\gamma_{i+1}(G) = 1_{G/\gamma_{i+1}(G)}$. Es gilt: $\gamma_i(G)/\gamma_{i+1}(G) \leqslant Z(G/\gamma_{i+1}(G))$. Das heißt die absteigende Reihe ist eine Zentralreihe. □

Proposition 5.20. $\forall n \;\; \gamma_n(G) = \langle [g_1, \dots, g_n] \mid g_1, g_2, \dots, g_n \in G \rangle$ *erzeugt von den* $[g_1, \dots, g_n] := [[g_1, \dots, g_{n-1}], g_n]$.

Beweis. Wir führen Induktion nach n durch. $n = 1, n = 2$ sind klar. Sei $N := \langle [g_1, \dots, g_n] \mid g_1, g_2, \dots, g_n \in G \rangle$. Wir haben $N \trianglelefteq G$ und $N \leqslant \gamma_n(G)$. Nach Induktion dürfen wir $\gamma_{n-1}(G) = \langle [g_1, \dots, g_{n-1}] \mid g_i \in G \rangle$ voraussetzen. Dann ist $\gamma_{n-1}(G)/N = \langle [g_1, \dots, g_{n-1}]N \mid g_i \in G \rangle$ und für $g_i \in G$ gilt: $[[g_1, \dots, g_{n-1}]N, g_nN] = [[g_1, \dots, g_{n-1}], g_nN] = [g_1, \dots, g_nN] = 1$. Das folgt $\gamma_{n-1}(G)/N \leqslant Z(G/N)$ und $\gamma_n(G)/N = [\gamma_{n-1}(G), G]/N = [\gamma_{n-1}(G), G/N] = 1$, d.h. $\gamma_n(G) = N$. □

Satz 5.21 (Zentralereihen)**.** *Sei* $\{1\} = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_{n-1} \leqslant G_n = G$, *eine Zentralreihe einer nilpotenten Gruppe* G, *dann gilt*

(1) $\gamma_i(G) \leqslant G_{n-i+1} \;\; \forall i$, *daher* $\gamma_{n+1}(G) = 1$;

(2) $G_i \leqslant Z_i(G) \;\; \forall i$, *daher* $Z_n(G) = G$ *und insbesondere* $1 \neq \gamma_n(G) \leqslant Z(G)$;

(3) Die nilpotenz-Klasse von G = *Länge der absteigenden Zentralreihe = Länge der aufsteigende Zentralreihe.*

Beweis. Induktion nach i.

(1): $G = \gamma_1(G) = G_n$ und hat man $\gamma_i(G) \leqslant G_{n-i+1}$ so folgt, nach Induktion, $\gamma_{i+1}(G) = [\gamma_i(G), G] \leqslant [G_{n-i+1}, G] \leqslant G_{n-i}$ weil $G_{n-i+1}/G_{n-i} \leqslant Z(G/G_{n-i})$.

(2): Für $i = 0$, haben wir $1 = Z_0(G) = G_0$ und $Z_i(G) \geqslant G_i$, dann $G_{i+1}/G_i \leqslant Z(G/G_i)$ folgt $G_{i+1}Z_i(G)/Z_i(G) \leqslant Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G) \Longrightarrow G_{i+1} \leqslant Z_{i+1}(G)$.

(3) folgt aus (1) und (2). □

Sei $X = \{x_1, x_2, \dots, \}$, definieren durch Induktion Wörter $v_n = v_n(x_1, \dots, x_{n+1})$: $v_1(x_1, x_2) = [x_1, x_2]$, ist v_n schon definiert, $v_n = [v_{n-1}, x_{n+1}]$. Zum Beispiel, $v_2 = [[x_1, x_2], x_3]$, $v_3 = [[[x_1, x_2], x_3], x_4]$, etc.

Notation. $G \models v_i = 1 \iff \forall g_1, \dots, g_{i+1} \in G$ es gilt $v_i(g_1, \dots, g_{i+1}) = 1$ in G.

Wir zeigen per Induktion nach n:

Satz 5.22. *Eine Gruppe G ist genau dann nilpotent mit nilpotenz-Klasse $\leqslant n$ (d.h. $\gamma_n(G) = 1$), wenn und nur wenn ein $n \in \mathbb{N}$ existiert derart, dass $G \models v_{n+1} = 1$ gilt.*

Übung 7. Die Klasse aller nilpotenten Gruppen ist abgeschlossen unter $\mathcal{S}$ (Untergruppen), $\mathcal{H}$ (homomorphe Bilder), unter Bildung von endlichen direkten Produkten und beliebige Potenzen. Die ist nicht abgeschlossen unter Erweiterungen.

Satz 5.23. *Für $m, n \in \mathbb{N}$ und jede Gruppe G gilt:*

(i) $[\gamma_m(G), \gamma_n(G)] \leqslant \gamma_{m+n}(G)$;

(ii) $G^{(n)} \leqslant \gamma_{2^n}(G)$.

Insbesondere jede nilpotente Gruppe ist auflösbar. Hat G die Nilpotenzklasse c, dann hat G abgeleitete Länge $\leqslant [\log_2 c] + 1$.

Beweis. Wir führen Induktion nach n durch.

(i): $[\gamma_m(G), G] = \gamma_{m+1}(G)$. Sei $n \geqslant 2$ und die Aussage für $n-1$ bereits bewiesen. Mit $H := G/\gamma_{m+n}(G)$ gilt dann $[\gamma_m(G), \gamma_n(G)]\gamma_{m+n}(G)/\gamma_{m+n}(G) =$

$= [\gamma_m(G)/\gamma_{m+n}(G), \gamma_n(G)/\gamma_{m+n}(G)] = [\gamma_m(H), \gamma_n(H)] = [\gamma_m(H), [H, \gamma_{n-1}(H)]] = 1_H$ wegen $[H, [\gamma_{n-1}(H), \gamma_m(H)]] = [H, [\gamma_m(H), \gamma_{n-1}(H)]] \subseteq [H, \gamma_{m+n-1}(H)] = \gamma_{m+n}(H) =$

$= \gamma_{m+n}(G)/\gamma_{m+n}(G) = 1_H$ und $[\gamma_{n-1}(H), [\gamma_m(H), H]] = [[\gamma_m(H), H], \gamma_{n-1}(H)] =$

$= [[H, \gamma_m(H)], \gamma_{n-1}(H)] = [\gamma_{m+1}(H), \gamma_{n-1}(H)] \subseteq \gamma_{m+n}(H) = 1$ nach dem 3-Untergruppen Lemma (siehe unten).

(ii): $G^{(0)} = G = \gamma_1(G) = \gamma_{2^0}(G)$. Sei n eine natürliche Zahl und bereits gezeigt, daß $G^{(n-1)} \subseteq \gamma_{2^{n-1}}(G)$ gilt. Dann folgt aus der obigen Aussage, daß $G^{(n)} = [G^{(n-1)}, G^{(n-1)}] \leqslant [\gamma_{2^{n-1}}(G), \gamma_{2^{n-1}}(G)] \leqslant \gamma_{2^n}(G)$. □

Übung 8 (3-Untergruppen Lemma). Seien A, B, C normale Untergruppen von G. So gilt

$$[A, B, C] \leqslant [B, C, A][C, A, B].$$

Proposition 5.24. *Jede endliche p-Gruppe ist nilpotent.*

Beweis. Jede endliche p-Gruppe G besitzt ein nichttriviales Zentrum $Z = Z(G)$.

Beweis mit Induktion nach $|G|$. Die Behauptung ist klar für $|G| = 1$ und $\forall$ p-Gruppen H mit $|H| < |G|$ ist richtig. D.h. die Behauptung für G/Z ist richtig. Es gibt die Zentralreihe

$$\{1_{G/Z}\} \trianglelefteq G_1/Z \trianglelefteq G_2/Z \trianglelefteq \ldots \trianglelefteq G_n/Z = G/Z$$

damit ist

$$\{1_G\} \trianglelefteq Z \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G$$

eine Zentralreine für G. □

Der Satz ist nicht richtig für nicht endliche p-Gruppen (Warum?).

Lemma 5.25. *Jede nichttriviale nilpotente Gruppe ein nichttriviales Zentrum hat.*

Beweis. Sei n so daß $\gamma_n(G) = 1$ aber $\gamma_{n-1}(G) \neq 1$ (hat G die Nilpotenzklass n).

$\gamma_n = [\gamma_{n-1}, G] = 1 \iff \forall x \in \gamma_{n-1}(G), \forall g \in G, \quad x^{-1}g^{-1}xg = 1 \iff xg = gx$, dann $\gamma_{n-1}(G) \leqslant Z(G)$. Es folgt $Z(G) \neq \{1\}$.

□

Beispiele 5.26. $S_3, D_n(n \neq 2^k)$ sind auflösbar aber nicht nilpotent. Zum Beispiel S_3 hat kein nichttriviales Zentrum.

Lemma 5.27. *Sei G endliche Gruppe, P eine p-Sylow Untergruppe von G, H eine Untergruppe von G. Dann gilt für $N_G(P) \leqslant H \leqslant G$, daß $N_G(H) = H$.*

Beweis. Sei $x \in N_G(H)$, es gilt

$$P \leqslant H \trianglelefteq N_G(H) \implies x^{-1}Px \leqslant H.$$

P ist p-Sylow Untergruppe von H, daher auch $x^{-1}Px$. Dann $\exists h \in H$, so daß $h^{-1}Ph = x^{-1}Px$ und $xh^{-1}Phx^{-1} = (hx^{-1})^{-1}P(hx^{-1}) = P$. Das bedeutet, daß $hx^{-1} \in N_G(P) \leqslant H$. Aber $h, hx^{-1} \in H$, dann $x \in H$. Wir schließen, daß $N_G(H) = H$. □

Definition 5.28 (Normalisatoreigenschaft)**.** Eine Gruppe G hat die *Normalisatoreigenschaft* wenn $\forall H \leqslant G, H \neq G$ gilt, daß $H \neq N_G(H)$.

Definition 5.29 (Subnormal Untergruppe)**.** Eine Untergruppe $H \leqslant G$ heißt *subnormal*, wenn gibt es eine Reihe $H = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$.

Satz 5.30. *Für eine endliche Gruppe G sind äquivalent:*

(1) G ist nilpotent;

(2) Jede Untergruppe von G ist subnormal;

(3) G hat die Normalisatoreigenschaft;

(4) Jede maximale Untergruppe von G ist normal;

(5) G ist das direkte Produkt ihrer Sylow Untergruppen.

Beweis. (1) $\Rightarrow$ (2):

Sei G nilpotent mit Klasse c, und $H \leqslant G$. Dann gilt $\forall i,\ HZ_i(G) \trianglelefteq HZ_{i+1}(G)$ denn $HZ_i(G) \leqslant HZ_{i+1}(G)$. Es gilt, nach Definition, $Z_{i+1}(G)/Z_i(G) = Z\left(G/Z_i(G)\right)$. Es gilt

$$HZ_i(G)/Z_i(G) \trianglelefteq HZ_{i+1}(G)/Z_i(G).$$

Seien $h, h_1 \in H,\ g_1 \in Z_{i+1}(G)$, dann

$$hZ_i(G) \in HZ_i(G)/Z_i(G) \text{ und } h_1 g_1 Z_i(G) \in HZ_{i+1}(G)/Z_i(G).$$

Wir konjugieren

$$(h_1 g_1)^{-1} h (h_1 g_1) Z_i(G) = g_1^{-1} h_1^{-1} h h_1 g_1 Z_i(G),$$
$$h_1^{-1} h h_1 g_1^{-1} g_1 Z_i(G) \in HZ_i(G)/Z_i(G).$$

Dann gilt $HZ_i(G) \trianglelefteq HZ_{i+1}(G)\ \forall i$ und wir haben

$$H = HZ_0(G) \trianglelefteq HZ_1(G) \trianglelefteq \cdots \trianglelefteq HZ_c(G) = G.$$

(2) $\Rightarrow$ (3):

Sei $H \subsetneqq G$, H subnormal: $H = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$. Sei i der kleinste Index mit $H \neq H_i$:

$$H = H_{i-1} \trianglelefteq H_i \implies H_i \leqslant N_G(H) \Longrightarrow H \neq N_G(H).$$

(3) $\Rightarrow$ (4):

Sei $M \subsetneqq G$ maximal, es gilt $N_G(M) \geqslant M$ dann $N_G(M) = G$. Das bedeutet, daß $M \trianglelefteq G$.

(4) $\Rightarrow$ (5):

Sei P eine Sylow Untergruppe. Wollen zeigen: $P \trianglelefteq G$. Angenommen $N_G(P) \neq G$, dann $N_G(P)$ ist enthalten in einer maximalen Untergruppe M.

$$P \leqslant N_G(P) \leqslant M \trianglelefteq G \overset{\text{Lemma } 5.27}{\Longrightarrow} N_G(M) = M.$$

Anderseits $M \trianglelefteq G \implies N_G(M) = G$ ist ein Widerspruch. Dann gilt $P \trianglelefteq G$ für alle Sylow Untergruppen.

Seien $p_1, \ldots, p_n$ die Primteiler von $|G|$, S_{p_i} die zugehörigen Sylow Untergruppen. Zu jedem Primteiler p von $|G|$ gibt es daher genau eine p-Sylow Untergruppe; S_{p_i} besteht aus allen Elementen mit Ordnung eine Potenz von p_i und dem 1-Element. Dann gilt

$$S_{p_1} \cap S_{p_2} = \{1\} \Longrightarrow S_{p_1} \cdot S_{p_2} \cong S_{p_1} \times S_{p_2}.$$

Weiters gilt $S_{p_1} S_{p_2} \trianglelefteq G$.

Analog:

$$S_{p_1} S_{p_2} \cap S_{p_3} = \{1\} \Longrightarrow S_{p_1} S_{p_2} S_{p_3} \cong S_{p_1} S_{p_2} \times S_{p_3} \cong S_{p_1} \times S_{p_2} \times S_{p_3}.$$

Mit Induktion:

$$S_{p_1} S_{p_2} \cdots S_{p_{n-1}} \cap S_{p_n} = \{1\} \Longrightarrow S_{p_1} S_{p_2} \cdots S_{p_n} \cong S_{p_1} \times S_{p_2} \times \cdots \times S_{p_n} \cong G,$$

weil $|G| = |S_{p_1}| \cdot |S_{p_2}| \cdot \ldots \cdot |S_{p_n}|$.

(5) $\Rightarrow$ (1):

Jede p-Gruppe ist nilpotent für jedes p. Dann jedes endliche direkte Produkt solcher Gruppen ist wieder nilpotent. $\square$

Wir wollen eine allgemeine Konstruktion nilpotenten Gruppen haben.
Seien R ein Ring mit 1, N ein Unterring, ohne 1,

$$N^{(i)} = \{ \text{ Summen von Produkten von } i \text{ Elementen von } N \}.$$

Insbesondere $N^{(1)} = N$. Jedes $N^{(i)}$ ist ein Unterring und $N = N^{(1)} \geqslant N^{(2)} \geqslant \dots$

Definition 5.31 (Nilpotent Ring)**.** Ein Ring N heßt *nilpotent* falls $\exists n \in \mathbb{N}$ mit

$$N^{(n)} = \{0\} \iff x_1 \cdot \ldots \cdot x_n = 0 \ \forall x_1, \dots, x_n \in N.$$

Sei $U = \{1 + x \mid x \in N\}$ mit Multiplikation von R.
Die Menge U ist eine Gruppe:
$(1+x)(1+y) = 1 + (x + y + xy) \in U$ und
$(1+x)^{-1} = 1 - x + x^2 - \dots + (-1)^{n-1}x^{n-1}$, weil

$$(1+x)(1 - x + x^2 - \dots + (-x)^{n-1}) = 1 - x^n = 1 \text{ weil } x^n = 0.$$

Sei

$$U_i = \left\{1 + x \mid x \in N^{(i)}\right\} \text{ für } i = 1, 2, \dots, n.$$

Dann gilt

$$\{1\} \leqslant U_n \leqslant U_{n-1} \leqslant \dots \leqslant U_1 = U.$$

Jedes U_i ist Untergruppe, weil $N^{(i)}$ ist Unterring.
Seien $x \in N^{(r)}, y \in N^{(s)}$,

$$[1+x, 1+y] = ((1+y)(1+x))^{-1}(1+x)(1+y) = (1+y+x+yx)^{-1}(1+x+y+xy),$$

mit $v = y + x + yx \in N^{(r+s)}$ und $u = x + y + xy \in N^{(r+s)}$. Dann

$$[1+x, 1+y] = (1+v)^{-1}(1+u) = (1 - v + v^2 - \ldots + (-1)^{n-1}v^{n-1})(1+u) =$$

$$= 1 + (1 - v + v^2 - \ldots + (-1)^{n-2}v^{n-2})(u - v) + (-1)^{n-1}v^{n-1}u.$$

Dann gilt $v^{n-1}u = 0$ und $u - v = x + y + xy - x - y - yx = xy - yx \in N^{(r+s)}$, daher

$$[1+x, 1+y] \in U_{r+s}.$$

Wir haben gezeigt $[U_r, U_s] \leqslant U_{r+s}$. Insbesondere für $s = 1$, wir haben $[U_r, U] \leqslant U_{r+1} \leqslant U_r$, dann gilt $U_r \trianglelefteq U$. Anders, seien $a \in U_{r+1}, b \in U_r$, dann gilt $b^{-1}aba^{-1} \in [U_r, U] \leqslant U_r$ und $b^{-1}ab \in U_{r+1} \implies U_{r+1} \trianglelefteq U_r$.

$[U_r, U] \leqslant U_{r+1}$, das heißt jedes Element von U_r kommutiert mit jedem Element von U modulo U_{r+1}.

Seien $a \in U, b \in U_r$, dann $b^{-1}a^{-1}ba \in U_{r+1} \implies baU_{r+1} = abU_{r+1}$

$$\implies U_r/U_{r+1} \leqslant Z\left(U/U_{r+1}\right)$$

$$\{1\} \leqslant U_n \leqslant U_{n-1} \leqslant \dots \leqslant U_1 = U$$

ist eine Zentralreihe. Das heißt die Nilpotentzklasse von U ist $\leqslant n$.

Sei S ein kommutativer Ring mit 1 und $n \in \mathbb{N}$, $R = M_{n,n}(S)$ $n \times n$-Matrizen über S.
$N =$ der Unterring der oberen Dreiecks Matrizen mit 0 auf der Diagonalen.

Wir bilden Unterring mit

$N^{(2)} =$ alle Matrizen, die auf der ersten Nebendiagonalen, ebenfalls 0 haben.

$N^{(i)} =$ alle Matrizen, die auf den ersten $i-1$ Nebendiagonalen lauter 0 haben.

$N^{(n)} = \{0\}$.

$U =$ Menge aller oberen Δ-Matrizen mit 1'-en auf der Hauptdiagonale

$U(n, S)$ ist eine nilpotente Gruppe, bezüglich Matrizenmultiplikation.

Wir haben die Zentralreihe

$$\{1\} = U_n = U_n(n, S) \leqslant U_{n-1} = U_{n-1}(n, S) \leqslant \cdots \leqslant U_1 = U_1(n, S) = U(n, S),$$

so mit Nilpotenzklasse $\leqslant n$. Es gilt $U_i =$ Gruppe aller oberen Δ-Matrizen mit 1en auf Hauptdiagonale und 0 auf den ersten $(i-1)$ Nebendiagonalen. Kann sich überlegen: die Nilpotenzklasse von $U(n, S)$ ist genau $= n$, weil

$$[\cdots[[[[[I + E_{1,2}, I + E_{2,3}], I + E_{3,4}], I + E_{4,5}], \cdots], I + E_{n-1,n}]].$$

Zu jedem n gibt es eine nilpotente Gruppe mit Nilpotenzklasse n.

Wenn $S = \mathbb{Z}$ erhält man mit $U(n, \mathbb{Z})$ eine Torsion freie Gruppe mit Nilpotenzklasse $= n$.

Eine Gruppe ist *torsions freie* wenn jedes $x \neq 1$ hat unendliche Ordnung.

Wenn $S = \mathbb{F}_p$, $U(n, \mathbb{F}_p) \leqslant GL(n, \mathbb{F}_p)$ mit

$$(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = (p^n - 1)(p^{n-1} - 1) \cdots (p - 1) \cdot p \cdot p^2 \cdot \ldots \cdot p^{n-1} =$$

$$= (p^n - 1)(p^{n-1} - 1) \cdots (p - 1) \cdot p^{\binom{n}{2}}$$

Elementen in $GL(n, \mathbb{F}_p)$.

$$|U(n, \mathbb{F}_p)| = p^{\binom{n}{2}}$$

das heißt $U(n, \mathbb{F}_p)$ ist eine p-Sylow Untergruppe von $GL(n, \mathbb{F}_p)$.

Satz 5.32. *Jede endliche p-Gruppe ist isomorph zu einer Untergruppe von $U(n, \mathbb{F}_p)$.*

Jede endliche p-Gruppe läßt sich als Gruppe von Δ-Matrizen über $\mathbb{F}_p$ realisieren.

Satz 5.33. *Zu jedem Körper $\mathbb{K}$ und jeder endlichen Gruppe G gibt es ein n, sodaß G zu einer Untergruppe von $GL(n, \mathbb{K})$ isomorph ist.*

Beweis von Satz 5.33. Wähle $n := |G|$, sei $\mathbb{K}^n \cong$ Vektorraum über $\mathbb{K}$ mit Basis G, d.h. betrachten $\mathbb{K}G = \{\sum_{g \in G} \lambda_g \cdot g,\ \lambda_g \in \mathbb{K}\}$. G wirkt auf $\mathbb{K}G$ durch

$$g \circ \sum_{h \in G} \lambda_h \cdot h := \sum_{h \in G} \lambda_h \cdot gh.$$

Die Wirkung ist *treu* (oder *effektiv*), d.h. wenn $g \circ \sum_{h \in G} \lambda_h \cdot h = \sum_{h \in G} \lambda_h \cdot h$, dann $g = 1_G$.

Daher ist $G \leqslant \mathrm{Aut}(\mathbb{K}G) \cong GL(n, \mathbb{K})$. □

Beweis von Satz 5.32. Sei G eine endliche p-Gruppe, $\mathbb{K} = \mathbb{F}_p$, dann ist G isomorph zu einer Untergruppe H von $GL(n, \mathbb{F}_p)$ für geeignetes n. Wir haben $H \leqslant P$ mit P eine p-Sylow Gruppe von $GL(n, \mathbb{F}_p)$. Aber P und $U(n, \mathbb{F}_p)$ sind zueinander konjugiert, d.h. $\exists x \in GL(n, \mathbb{F}_p)$ mit $x^{-1}Px = U(n, \mathbb{F}_p)$. Dann gilt $x^{-1}Hx \leqslant U(n, \mathbb{F}_p)$. □

6 Freie Gruppen

Seien $X \neq \emptyset$ eine Menge, $\mathcal{K} \neq \emptyset$ eine Klasse von Gruppen.

Definition 6.1. Eine Gruppe $F \in \mathcal{K}$, zusammen mit einer Abbildung $i\colon X \to F$ heißt *$\mathcal{K}$-frei über X* (oder *frei in $\mathcal{K}$ über X)* wenn gilt: $\forall G \in \mathcal{K},\ \forall f\colon X \to G,\ \exists!$ (eindeutig) Homomorphismus $\overline{f}\colon F \to G$ sodaß das Diagramm:

$$\begin{array}{ccc} X & \xrightarrow{f} & G \\ {\scriptstyle i}\downarrow & \nearrow_{\overline{f}} & \\ F & & \end{array}$$

kommutiert.

Folgerungen (falls F exisitiert):

(1) Wenn $\mathcal{K}$ eine Gruppe mit mehr als einem Element enthält, ist i injektiv und X wird mit $i(X)$ identifiziert. X kann dann als Teilmenge von F angesehen werden.

(2) F ist bis auf Isomorphie eindeutig durch $|X|$ und $\mathcal{K}$ bestimmt.

(3) F wird von $X = i(X)$ erzeugt.

Beweis. (1): $G \in \mathcal{K}, |G| > 1$, seien $x \neq y \in X,\ \exists f\colon X \to G$ mit $f(x) \neq f(y)$. Dann gilt $\overline{f}(i(x)) = f(x) \neq f(y) = \overline{f}(i(y)) \implies i(x) \neq i(y)$.

(2): Seien F_1, F_2 zwei $\mathcal{K}$-freie Objekte über X. Ohne Beschränkung der Allgemeinheit, $X \subseteq F_1$ und $X \subseteq F_2$. Wir haben die Diagramme

$$\begin{array}{ccc} X & \xrightarrow{\mathrm{id}_X} & X \subseteq F_2 \\ {\scriptstyle i_1}\downarrow & \nearrow_{\overline{f}_1} & \\ F_1 & & \end{array}$$

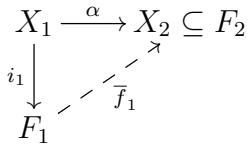
und

$$\begin{array}{ccc} X & \xrightarrow{\mathrm{id}_X} & X \subseteq F_1 \\ {\scriptstyle i_2}\downarrow & \nearrow_{\overline{f}_2} & \\ F_2 & & \end{array}$$

$\overline{f}_1$ ist ein Homomorphismus $F_1 \to F_2$ mit $\overline{f}_1\big|_X = \mathrm{id}_X$ und $\overline{f}_2$ ist ein Homomorphismus $F_2 \to F_1$ mit $\overline{f}_2\big|_X = \mathrm{id}_X$. Dann $\overline{f}_2 \circ \overline{f}_1$ ist ein Homomorphismus $F_1 \to F_1$ mit $(\overline{f}_2 \circ \overline{f}_1)\big|_X = \mathrm{id}_X$ und $\overline{f}_1 \circ \overline{f}_2$ ist ein Homomorphismus $F_2 \to F_2$ mit $(\overline{f}_1 \circ \overline{f}_2)\big|_X = \mathrm{id}_X$.

Es kann nur einen solchen Homomorphismus geben, id_{F_1} ist ein solcher, dann gilt $\overline{f}_2 \circ \overline{f}_1 = \mathrm{id}_{F_1}$ und $\overline{f}_1 \circ \overline{f}_2 = \mathrm{id}_{F_2}$.

Falls $|X_1| = |X_2|$ mit $\alpha\colon X_1 \to X_2$ und $\alpha^{-1}\colon X_2 \to X_1$, analoge Vorgehensweise, nur statt id_X mit α und α^{-1} arbeiten:



(3): Siehe unten. □

Beispiele 6.2. (1) $\mathcal{K} = Ab$ = Klasse der abel'schen Gruppen, $X = \{x_1, x_2, \ldots, x_n\}$, die Ab-freie Gruppe über X ist isomorph zu $\mathbb{Z}^n$.

(2) X beliebig, dann betrachtet man $\mathbb{Z}^X = \{f\colon X \to \mathbb{Z}\}$ mit punktweisen Verknüpfung. Sei $F = \{f \in \mathbb{Z}^X \mid f(n) = 0 \text{ bis auf endlich vielen } \} \leqslant \mathbb{Z}^X$. Dann $i\colon X \to F, x \mapsto f_x$ mit $f_x(y) = 1$ für $x = y$, 0 sonst.

(3) Die Klasse der endlichen Gruppen besitzt keine freie Gruppe..

Definition 6.3 (Absolut freie Gruppe/Rang)**.** Eine Gruppe F, zusammen mit einer Abbildung $i\colon X \to F$ heißt *absolut frei über* X (oder *frei über* X*)* wenn gilt: F ist $\mathcal{K}$-frei über X mit $\mathcal{K} =$ Klasse aller Gruppen.
Der *Rang* einer freien Gruppe über X ist die Mächtigkeit $|X|$ von X: $\mathrm{rang}(F) = |X|$.

Man müsste beweisen dass es existiert zu jedem X eine absolute freie Gruppe über X.

Beweise (Existenz von absolut freie Gruppe). Gegeben sei die Erzeugermenge X. Wir wählen für jedes $x \in X$ ein neues Symbol x^{-1} und betrachten nun das Wortmonoid $(X \sqcup X^{-1})^*$ (d.h. die Halbgruppe mit Einselement, von $X \sqcup X^{-1}$ erzeugt) über dem Alphabet $X \sqcup X^{-1}$:

$(X \sqcup X^{-1})^* =$ Menge aller endlichen Wörter über $X \sqcup X^{-1}$, inklusive dem leeren Wort 1,

und zwei Operationen:

$$(u, v) \mapsto u \cdot v \quad \text{die Konkatenation (eine assoziative Verknüpfung) und}$$

$$u \mapsto u^{-1} \quad \text{die inverse Element, definiert durch}$$

$u = y_1 \ldots y_n$ mit $y_i \in X \sqcup X^{-1}$, dann $u^{-1} := y_n^{-1} \ldots y_1^{-1}$ und $1^{-1} := 1$. Wir haben, daß $(u^{-1})^{-1} = u, (uw)^{-1} = w^{-1}u^{-1}$.

Wir betrachten Äquivalenzrelation $\sim$ auf $(X \sqcup X^{-1})^*$, wenn sich u durch endliche Streichungen und / oder Einfügungen von Segmenten der Form xx^{-1} oder $x^{-1}x$, für x ein beliebiges Element von X, in v umformen läßt.

$\sim$ ist eine Äquivalenzrelation, die mit $\cdot$ und $^{-1}$ verträglich ist, d.h.

$$u \sim v, u_1 \sim v_1 \Longrightarrow uu_1 \sim vv_1$$

$$u \sim v \Longrightarrow u^{-1} \sim v^{-1}.$$

Mann kann auf die Quotientenmenge $(X \sqcup X^{-1})^* / \sim$ die Operationen $\cdot$ und -1 definieren durch

$$[u][v] := [u \cdot v],\ [u]^{-1} := [u^{-1}].$$

Die Multiplikation ist assoziativ und die Involution (= die Inversenbildung) erfüllt

$$([u][v])^{-1} = [v]^{-1}[u]^{-1} \text{ und } ([u]^{-1})^{-1} = [u], \quad [1] \text{ ist Einselement.}$$

$^{-1}$ ist eine Inversion: für $u \in (X \sqcup X^{-1})^*, u = y_1 \dots y_n$,

$$[u][u]^{-1} = [u \cdot u^{-1}] = [y_1 \dots y_n y_n^{-1} \dots y_1^{-1}] = [1].$$

Dann $(X \sqcup X^{-1})^* / \sim$ ist eine Gruppe, genannt $F(X)$ oder F, und gibt es eine Abbildung $X \to F(X)$, z.B. $x \mapsto [x]$ (eine Bijektion).

F wird als Gruppe von $\{[x] \mid x \in X\}$ erzeugt. Sei G beliebig, $f\colon X \to G$ gesucht ist Homomorphismus $\overline{f}\colon F(X) \to G$ mit $\overline{f}|_X = f$. Dieser ist dann notwendig eindeutig, weil $F(X)$ von X erzeugt wird. Sei $[w] \in F(X)$ beliebig $w = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ mit $x_i \in X, \varepsilon_i = \pm 1$

$$\overline{f}(x_i) := f(x_i) \text{ ist vorgegeben, wir definieren } \overline{f}(x_i^{-1}) := (\overline{f}(x_i))^{-1} = (f(x_i))^{-1},$$

dann $\overline{f}(x_i^{\varepsilon_i}) = (f(x_i))^{\varepsilon_i}$ und wir definieren $\overline{f}(w) = \overline{f}(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}) := (f(x_1))^{\varepsilon_1} \dots (f(x_n))^{\varepsilon_n}$.

Bemerkung 6.4. Sei X eine Teilmenge von eine Gruppe G erzeugte von X, d.h. $G = \langle X \rangle$, und $f\colon X \to H$ (eine beliebige Gruppe H), dann hat f höchstens eine Fortsetzung $\overline{f}\colon G \to H$.

Bleibt zu zeigen: wohldefiniertheit, daher unabhängig vom Repräsentanten in $[w]$. Definiere $g\colon (X \sqcup X^{-1})^* \to G, \quad g(w) := g(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}) = (f(x_1))^{\varepsilon_1} \dots (f(x_n))^{\varepsilon_n}$ ist ein Monoidhomomorphismus, der mit der Involution verträglich ist.

$$\begin{array}{ccc} X & \hookrightarrow & (X \sqcup X^{-1})^* \\ {\scriptstyle f}\downarrow & \overset{\overline{g}}{\swarrow} & \downarrow{\scriptstyle w \mapsto [w]} \\ G & \underset{\overline{f}}{\leftarrow} & F(X) = (X \sqcup X^{-1})^* / \sim \end{array}$$

Wenn $w \sim u$, d.h. $w = w_0 = w_1 = \dots = w_n = u$ und (jeweils eine Elementare Operation) auf der rechten Seite ändert sich nichts, da dort 1 eingefügt oder rausgestrichen wird, dann

$$w \sim u \Longrightarrow g(w) = g(u)$$

und g kann für Äquivalenzklassen definiert werden. □

Man kann einen anderen Beweis für die Existenz von $F(X)$ geben. Ein Wort $w \in (X \sqcup X^{-1})^*$ heißt *reduziert*, wenn w kein Segment der Form $x \cdot x^{-1}$ oder $x^{-1} \cdot x$, mit x ein Buchstabe, enthält.

$w \in (X \sqcup X^{-1})^*$ kann durch sukzessives Streichen solcher Segmente in ein reduziertes Wort überführt werden. Dieses reduzierte Wort ist nur von w abhängig, unabhängig davon in welcher Reihenfolge die Reduktionen (= Streichungen) vorgenommen werden.

Bezeichnung: $w \to red(w)$.

Wir haben, daß $u \sim v \Longrightarrow red(u) = red(v)$. Jede $\sim$-Klasse besitzt genau ein reduziertes Wort. $F(X) =$ Menge aller endlichen reduzierten Wörter über $X \sqcup X^{-1}$, inklusive dem leeren Wort 1, mit zwei Operationen: 'Involution' und 'Konkatenation + Reduktion'.

Proposition 6.5. *$G = \langle X \rangle$ ist genau dann frei über X wenn in G, $w \neq 1$ für jedes nicht leere reduzierte Wort w in $X \sqcup X^{-1}$. Äquivalent: für $u, v \in (X \sqcup X^{-1})^*$, dann gilt $u = v$ in G nur dann, wenn $red(u) = red(v)$.*

Zu zeigen: die universelle Eigenschaft. Sei H eine Gruppe, $f\colon X \to H$ eine Abbildung. Dann $\exists!\ \overline{f}\colon G \to H$ mit $\overline{f}|_X = f$. Wir definieren $\overline{f}(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}) := (f(x_1))^{\varepsilon_1} \dots (f(x_n))^{\varepsilon_n}$.

Beispiel 6.6. $A, B \in GL(2,\mathbb{R})$, so daß $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ und $B = \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix}$ mit $a, b \in \mathbb{R}, |a|, |b| \geqslant 2$. Sei $H = \langle A, B\rangle \leqslant GL(2,\mathbb{R})$. Wir haben $H = \{A^{n_1}B^{n_2} \dots A^{n_{l-1}}B^{n_l} \mid n_i \in \mathbb{Z}\}$. Behauptung: H is frei, $\operatorname{rang}(H) = 2$.

Wir haben, daß $A^n = \begin{bmatrix} 1 & na \\ 0 & 1 \end{bmatrix}$. Also $A^n \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + nay \\ y \end{bmatrix}$. Seien $M_1 = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \mid |x| > |y| \right\}$ und $M_2 = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \mid |x| < |y| \right\}$. Wir bemerken, daß $M_1 \cap M_2 = \emptyset$. Wir haben, daß für jedes reduzierte Wort $B^{n_2} \dots A^{n_{l-1}}B^{n_l} \neq 1$ mit $n_2 \neq 0, n_l \neq 0$ und für jedes reduzierte Wort $A^{n_1}B^{n_2} \dots A^{n_{l-1}} \neq 1$ mit $n_1 \neq 0, n_{l-1} \neq 0$, weil für $v \in M_2$ und $n \neq 0$, $A^n v = v' \in M_1$ (weil $|x + nay| \geqslant |na||y| - |x| \geqslant 2|y| - |x| > |y|$) und für $v \in M_1$ und $n \neq 0$, $B^n v = v' \in M_2$. Aber jedes reduzierte Wort $A^{n_1}B^{n_2} \dots A^{n_{l-1}}B^{n_l}$ mit $n_1 \neq 0, n_l \neq 0$ und jedes reduzierte Wort $B^{n_2} \dots A^{n_{l-1}}$ mit $n_2 \neq 0, n_{l-1} \neq 0$ sind konjugiert mit Worten wie oben (dann $\neq 1$). Nach Proposition 6.5, H ist frei und $\operatorname{rang}(H) = 2$.

Offene Frage 6.7. Gibt es $a, b \in \mathbb{Q}$ mit $|a| < 2$ (oder $|b| < 2$) so daß H ist frei und $\operatorname{rang}(H) = 2$?

Beispiel 6.8. Sei R ein Ring, $R[[x_1, \dots, x_k]] = \{\sum_{i=0}^{\infty} u_i \mid \ u_i \text{ ein homogen Polynom }\}$. Ein Polynom, mit nicht kommutierende Variablen $x_1, \dots, x_k$, heißt *homogen*, falls alle Monome, aus denen das Polynom besteht, den gleichen Grad haben. Z.B. $x_1x_2x_1$ ist ein Monom und $x_1x_2x_1 - 2x_3^2x_1$ ist ein homogen Polynom.

Sei $G[[x_1, \dots, x_k]] \subset R[[x_1, \dots, x_k]]$ so daß Elementen von $G[[x_1, \dots, x_k]]$ haben konstante Term $= 1$, d.h. $1 + u \in G[[x_1, \dots, x_k]]$ mit $u \in R[[x_1, \dots, x_k]]$ und u hat kein konstante Term. Wir sehen, daß $(1+u)^{-1} = (1 - u + u^2 - u^3 + \dots) \in G[[x_1, \dots, x_k]]$.

Sei $H = \langle 1 + x_1, \dots, 1 + x_k\rangle \leqslant G[[x_1, \dots, x_k]]$.

Behauptung: H is frei, $\operatorname{rang}(H) = k$.

Wir haben daß $(1 + x_i)^n = (1 + nx_i + \dots),\ \forall n \in \mathbb{Z}$. Dann gilt

$$(1 + x_{i_1})^{n_1}(1 + x_{i_2})^{n_2} \cdots (1 + x_{i_l})^{n_l} = (1 + nx_{i_1} + u_1)(1 + nx_{i_2} + u_2) \cdots (1 + nx_{i_l} + u_l)$$

und $\forall j, u_j$ hat kein konstante Term und Grad 1 Term. Dann für jedes nicht leere reduzierte Wort w in $1 + x_1, \dots, 1 + x_k, (1 + x_1)^{-1}, \dots, (1 + x_k)^{-1}$ wir haben:

$$w = (1 + x_{i_1})^{n_1}(1 + x_{i_2})^{n_2} \cdots (1 + x_{i_l})^{n_l} = 1 + (n_{i_1}n_{i_2} \dots n_{i_l})x_{i_1}x_{i_2} \dots x_{i_l} + \dots \neq 1,$$

$\forall n_j \in \mathbb{Z} \setminus \{0\}$ so daß w ist nicht leere reduzierte Wort. Nach Proposition 6.5, H ist frei und $\operatorname{rang}(H) = k$.

Übung 9. Beweise das Ping-Pong Lemma.

Sei X ein Erzeugendensystem einer Gruppe G mit $|X| \geqslant 2$. Dann sind äquivalent:

(i) Es existieren eine Gruppenwirkung $G \times Y \to Y$ und paarweise disjunkte Teilmengen $Y_x, Z_x, x \in X$, von Y, so daß

$$x(Y \setminus Y_x) \subseteq Z_x \text{ und } x^{-1}(Y \setminus Z_x) \subseteq Y_x$$

für alle $x \in X$.

(ii) Die Abbildung $\mathrm{id_X}$ setzt zu einem Gruppenisomorphismus von $F(X)$ nach G fort.

Übung 10. Sei $\overline{\mathbb{C}} := \mathbb{C} \cup \infty$. Betrachte Bijektionen α, β, γ auf $\overline{\mathbb{C}}$ mit $\alpha(z) = z + 2, \beta(z) = \frac{z}{2z+1}, \gamma(z) = \frac{1}{z}$. Beweise daß $\langle \alpha, \beta \rangle$ ist frei über α, β.

Satz 6.9 (Nielsen, 1921: endlich erzeugt, Schreier, 1926: beliebig)**.** *Untergruppen freier Gruppen sind frei.*

Übung 11.

- Falls F_2 von x, y *frei erzeugt* wird (d.h. F_2 ist absolut frei über X mit $X = \{x, y\}$), so bilden die $z_n := y^{-n}xy^n$ ein *freies System* (zu zeigen: $w \neq 1$ für jedes nicht leere reduzierte Wort w in $\{z_n, z_n^{-1} \mid n \in \mathbb{N}\}$); So F_∞ und F_k sind Untergruppen von F_2;
- Alle freien Gruppen sind linear, d.h. Untergruppe von einem $GL(n, \mathbb{K})$;
- Für $k > 1$ gilt $Z(F_k) = \{1\}$, das Zentrum von F_k ist trivial.

7 Relativ freie Gruppen

Sei $\mathcal{K}$ eine Klasse von Gruppen. Wir definieren die Klassenoperatoren $\mathcal{P}, \mathcal{S}, \mathcal{H}$:

$\mathcal{PK}$ = Klasse aller Gruppen, die isomorph zu (vielleicht unendlichen) direkten Produkten von $\mathcal{K}$ sind.

$\mathcal{SK}$ = Klasse aller Gruppen, die isomorph zu Untergruppen von Mietgliedern von $\mathcal{K}$ sind.

$\mathcal{HK}$ = Klasse aller Gruppen, die isomorph zu homomorphen Bilden von Mitgliedern von $\mathcal{K}$ sind.

$\mathcal{X} \in \{\mathcal{P}, \mathcal{S}, \mathcal{H}\}, \mathcal{K}$ eine Klasse von Gruppen. $\mathcal{K}$ ist *abgeschlossen unter* $\mathcal{X}$, wenn $\mathcal{XK} \subseteq \mathcal{K}$. Beispiel: abel'sche Gruppen ($\mathcal{X}$ beliebig).

Satz 7.1. *Zu jeder Klasse $\mathcal{K}$ von Gruppen, die abgeschlossen unter $\mathcal{P}$ und $\mathcal{S}$ gibt es über jeder Menge X eine $\mathcal{K}$-freie Gruppe über X.*

Beweis. Sei $\mathcal{K}$ eine Klasse mit $\mathcal{PK} \subseteq \mathcal{K}, \mathcal{SK} \subseteq \mathcal{K}, X \neq \emptyset$. Wir definieren

$$W_\mathcal{K} := \{w \in F(X) \mid \mathcal{K} \not\models w = 1\}.$$

O.B.d.A. die Klasse $\mathcal{K}$ enthält nicht triviale Mitglieder, dann gilt $W_\mathcal{K} \neq \emptyset$. Wir definieren

$$K_\mathcal{K} := F(X) \setminus W_\mathcal{K} = \{w \in F(X) \mid \mathcal{K} \models w = 1\}.$$

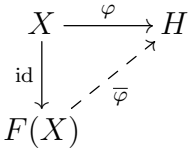
Die Untergruppe $K_\mathcal{K}$ ist voll-invariante Untergruppe (siehe Definition 5.4; m. a. W. abgeschlossen unter allen Substitutionen: Variable $\mapsto$ Wort).

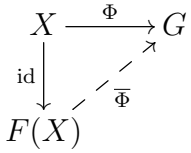
Zu jedem $w \in W_\mathcal{K}$, $\exists G_w \in \mathcal{K}$ und $f_w \colon X \to G_w$ sodaß $\overline{f}_w(w) \neq 1$ wobei $\overline{f}_w \colon F(X) \to G_w$ von die universelle Eigenschaft ist. Betrachten $\prod_{w \in W_\mathcal{K}} G_w$ mit $\Phi \colon X \to \prod_{w \in W_\mathcal{K}} G_w$ so daß $\Phi(x) := (f_w(x))_{w \in W_\mathcal{K}}$. Die Abbildung Φ is injektiv (wenn $x \neq y$, dann $xy^{-1} \in W_\mathcal{K}$).

Sei $G := \langle \Phi(X) \rangle \leqslant \prod_{w \in W_\mathcal{K}} G_w, G \in \mathcal{K}$ und wird von $\Phi(X)$, welches mit X identifiziert werden kann, erzeugt.

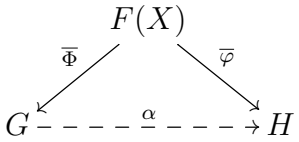
Behauptung: $G = F_{\mathcal{K}}(X)$.

Sei $H \in \mathcal{K}$ beliebig mit $\varphi\colon X \to H$ beliebig. Dann kann φ zu einem Homomorphismus $\overline{\varphi}\colon F(X) \to H$ fortgesetzt werden und $\Phi\colon X \to G$ kann zu Homomorphismus $\overline{\Phi}\colon F(X) \to G$ fortgesetzt werden.

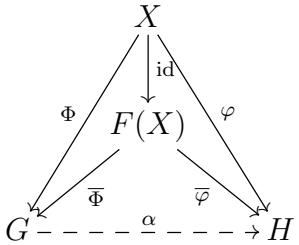




Es gilt $\overline{\Phi}(u) = (\overline{f}_w(u))_{w \in W_{\mathcal{K}}}$. Wir möchten zeigen, daß gibt es $\alpha\colon G \to H$ sodass das folgende Diagramm kommutiert:



Zu zeigen $\operatorname{Ker}\overline{\Phi} \subseteq \operatorname{Ker}\overline{\varphi}$. Das ergibt zusammen

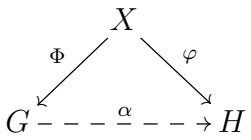


Es gilt $\operatorname{Ker}\overline{\Phi} = K_{\mathcal{K}} = F(X) \setminus W_{\mathcal{K}}$:

• Wenn $w \in K_{\mathcal{K}} \Longrightarrow G \models w = 1 \Longrightarrow \overline{\Phi}(w) = 1$. Dann $K_{\mathcal{K}} \subseteq \operatorname{Ker}\overline{\Phi}$.

• Wenn $w \in W_{\mathcal{K}}$ dann gilt $\overline{f}_w(w) \neq 1 \Longrightarrow \overline{\Phi}(w) \neq 1$. Dann $\operatorname{Ker}\overline{\Phi} \subseteq K_{\mathcal{K}}$.

Wenn $w \in K_{\mathcal{K}}$, da $H \models w = 1 \Longrightarrow \overline{\varphi}(w) = 1 \Longrightarrow K_{\mathcal{K}} \subseteq \operatorname{Ker}\overline{\varphi}$. Es gibt daher $\alpha\colon G \to H$ mit $\alpha \circ \overline{\Phi} = \overline{\varphi}$. Es gilt $\forall x \in X\ \alpha(\Phi(x)) = \alpha(\overline{\Phi}(x)) = \overline{\varphi}(x) = \varphi(x)$. Daher



□

Seien $F(X)$ ein absolut freie Gruppe, $K \subseteq F(X)$. Wir definieren

$$\mathcal{K}_K := \{G \mid \ G \models w = 1 \text{ für alle } w \in K\}.$$

Die Klasse $\mathcal{K}_K$ wird durch die Menge der *Identitäten* $\{w = 1 \mid w \in K\}$ definiert.

z.B. $K = \{xyx^{-1}y^{-1}\}$ bzw $K = \{xyx^{-1}y^{-1}uvu^{-1}v^{-1}\}$ dann $\mathcal{K}_K =$ abelsche Gruppen.

Definition 7.2 (Garrett Birkhoff'35, Philip Hall'49)**.** Eine Klasse $\mathcal{K}$ von Gruppen kann durch *Identitäten* definiert werden, wenn es ein X und ein $K \subseteq F(X)$ gibt mit $\mathcal{K} = \mathcal{K}_K$. In diesem Fall $\mathcal{K}$ heißt eine *Varietät von Gruppen.*

Frage 7.3 (Birkhoff)**.** Welche Klassen von Gruppen können durch Identitäten definiert werden?

Satz 7.4 (Birkhoff'35)**.** *Eine Klasse $\mathcal{K}$ kann genau dann durch Identitäten definiert werden, wenn und nur wenn $\mathcal{K}$ abgeschlossen unter $\mathcal{P}, \mathcal{S}$ und $\mathcal{H}$ ist.*

Beweis. Es ist klar, daß jede solche Klasse ist abgeschlossen unter $\mathcal{P}, \mathcal{S}$ und $\mathcal{H}$.

Sei $\mathcal{K}$ abgeschlossen unter $\mathcal{P}, \mathcal{S}$ und $\mathcal{H}$. Sei $X = \{x_1, x_2, \ldots\}$ eine abzählbar unendliche Menge, wir bilde die absolut freie Gruppe $F(X)$.

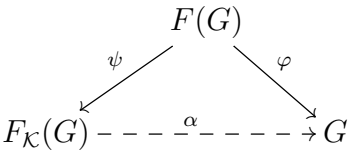
Seien $K := \{w \in F(X) \mid \mathcal{K} \models w = 1\}$, wir bilden $\mathcal{K}_K$:

$$\mathcal{K}_K := \{G \mid \ G \models w = 1 \text{ für alle } w \in K\}.$$

Dann gilt $\mathcal{K} \subseteq \mathcal{K}_K$.

Zu zeigen: $\mathcal{K}_K \subseteq \mathcal{K}$.

Sei $G \in \mathcal{K}_K$, bilde $F(G)$ und $F_{\mathcal{K}}(G)$ (existieren nach Satz 7.1). Die Abbildung $\mathrm{id}\colon G \to G$ kann zu einem Homomorphismus $\varphi\colon F(G) \to G$ und zu einem Homomorphismus $\psi\colon F(G) \to F_{\mathcal{K}}(G)$ fortgesetzt werden. Beide Homomorphismen sind surjektiv:



Wir zeigen die Existenz von α, also ist zu zeigen $\operatorname{Ker}\psi \subseteq \operatorname{Ker}\varphi$.

Sei $u \notin \operatorname{Ker}\varphi$, u ist ein Wort in den Symbolen $g_1, \ldots, g_k, g_1^{-1}, \ldots, g_k^{-1}$ mit $g_i \in G$.

$u \notin \operatorname{Ker}\varphi$ heißt $\varphi(u) \neq 1 \implies G \not\models u(x_1, \ldots, x_k) = 1$, betrachte $u(x_1, \ldots, x_k) \in F(X)$, die g_j's werden durch x_j's substituiert. Dann $u(x_1, \ldots, x_k) \notin K \implies F_{\mathcal{K}}(G) \not\models u(x_1, \ldots, x_k) = 1 \implies \psi(u) \neq 1 \implies \operatorname{Ker}\psi \subseteq \operatorname{Ker}\varphi$.

Dann gilt $\exists\alpha\colon F_{\mathcal{K}}(G) \to G$ mit $\alpha\psi = \varphi$. Insbesondere gilt $\forall g \in G, \alpha(g) = g$ und α ist surjektiv. G ist Homomorphes Bild von $F_{\mathcal{K}}(G)$, dann $G \in \mathcal{K}$ weil $\mathcal{HK} \subseteq \mathcal{K}$. □

Sei $\mathcal{K}$ eine beliebige Klasse von Gruppen. Dann gilt

$$\mathcal{PSK} \subseteq \mathcal{SPK} \quad \mathcal{PHK} \subseteq \mathcal{HPK} \qquad \mathcal{SHK} \subseteq \mathcal{HSK}$$

Daraus folgt $\mathcal{HSPK}$ ist die kleinste Klasse, die $\mathcal{K}$ enthälte und abgeschlossen unter $\mathcal{P}, \mathcal{S}$ und $\mathcal{H}$ ist. Die ist die kleinste Klasse, die $\mathcal{K}$ enthält und durch Identitäten definiert werden kann, $= \mathcal{K}_K$ wobei $K := \{w \in F(X) \mid \mathcal{K} \models w = 1\}$.

Übung 12. Sei $\mathcal{K} = \{G\}$ mit G endlich und $\forall H \in \mathcal{K}_K$ endlich erzeugt. Dann gilt $\forall H \in \mathcal{K}_K$, dass $|H| < \infty$.

Übung 13. Finden Klassen von Gruppen $\mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3$, etc. so daß: $\mathcal{SK}_1 \neq \mathcal{K}_1, \mathcal{HK}_1 = \mathcal{K}_1, \mathcal{PK}_1 = \mathcal{K}_1$ aber $\mathcal{SK}_2 = \mathcal{K}_2, \mathcal{HK}_2 \neq \mathcal{K}_2, \mathcal{PK}_2 \neq \mathcal{K}_2$, etc.

Satz 7.5. *Für eine Gruppe F sind äquivalent:*

1. *F ist $\mathcal{K}$-frei für eine geeignete Klasse $\mathcal{K}$;*
2. *F ist $\mathcal{K}$-frei für eine geeignete Varietät $\mathcal{K}$;*
3. *F ist $\{F\}$-frei;*
4. *F ist $\mathcal{HSP}\{F\}$-frei.*

Wenn $|X_1| = |X_2|$ dann sind $F_{\mathcal{K}}(X_1) \cong F_{\mathcal{K}}(X_2)$ zueinander. Es gilt auch die Umkehrung (für freie erzeugten Systeme X_1 und X_2). Beispiel: sei F frei über $\{x, y\}$ dans ist F auch frei über $\{xy, y\}$.

Definition 7.6 (Verbale Untergruppe)**.** Sei $K \subseteq (X \sqcup X^{-1})^*$,

$$V_K := \langle w(g_1, \ldots, g_l) \mid w \in K, g_i \in G \rangle \leqslant G$$

ist *verbale Untergruppe* von G.

Sei $w \in (X \sqcup X^{-1})^*$ und G, H zwei Gruppen. Dann $\forall \varphi \colon G \to H$,

$$\varphi(w(g_1, \ldots, g_l)) = w(\varphi(g_1), \ldots, \varphi(g_n)).$$

Es folgt $\varphi(\langle w(g_1, \ldots, g_l), g_i \in G \rangle) \subseteq \langle w(\varphi(g_1), \ldots, \varphi(g_l)), g_i \in G \rangle$. Insbesondere,

Lemma 7.7. *Jede verbale Untergruppe ist voll-invariant.*

Satz 7.8. *Eine Untergruppe $N \leqslant F(X)$ ist eine verbale Untergruppe wenn und nur wenn*

1. *$u, v \in N \Rightarrow uv^{-1} \in N$;*
2. *$\forall u = u(x_1, \ldots, x_l) \in N$ und $v_1, \ldots, v_l \in F(X) \Rightarrow u(v_1, \ldots, v_l) \in H$.*

Übung 14. Voll-invariant Untergruppe $\not\Longrightarrow$ verbale Untergruppe.

Satz 7.9. *Sei G eine relativ freie Gruppe. Dann ist jede voll-invariante Untergruppe $H \leqslant G$ verbal.*

Beweis. Sei H voll-invariante Untergruppe von G. Sei

$$K_H := \{w = w(x_1, \ldots, x_l) \in F(X) \mid w(g_1, \ldots, g_l) \in H, \forall g_i \in G\}.$$

Zu zeigen: $H = V_{K_H}$.

$\bullet V_{K_H} \leqslant H$ ist klar.
$\bullet H \leqslant V_{K_H}$:
Sei $h \in H$. Dann $\exists w \in G$ sodaß $h = w(f_{i_1}, \ldots, f_{i_n})$, $f_i, i \in I$ ist eine freie Erzeugendensystem: $G = \langle f_i \mid i \in I \rangle$. H ist voll-invariant $\Longrightarrow w(x_1, \ldots, x_n) \in K_H$ weil $\forall g_1, \ldots, g_n$ die Abbildung $f_{i_l} \mapsto g_{i_l}$ ist ein Endomorphismus und $w(g_1, \ldots, g_n) \in H$. □

Übung 15. Die quaternion Gruppe ist nicht relative freie Gruppe.

Die Burnside-Varietät $\mathcal{B}(m, n)$ ist mit Identität $x^n = 1$ definiert (zwischen den Gruppen mit $m \geqslant 2$ erzeugte Elementen).

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

Klassisches Burnside-Problem: 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),
$n = 3$ (endlich: Burnside, 1902, die Kardinalität: 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 $n = 5$ und $n = 7$ und $n = 8$ ist bis jetzt offen.

Satz 7.10 (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 $\mathbb{Z}/p\mathbb{Z}$ 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 7.11 (Golod, 1964)**.** *Fur jede Primzahl p existiert eine 2-erzeugte unendliche Gruppe G, so dass die Ordnungen der Elemente von G Potenzen von p sind.*

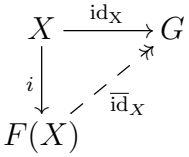
Satz 7.12 (Grigorchuk, 1980, Gupta-Sidki, 1983)**.** *Fur jede ungerade Primzahl p existiert ein Baum X, so dass $Aut(X)$ eine Untergruppe G enthält, für die folgendes gilt:*
(1) G ist von 2 Elementen erzeugt.
(2) G ist eine p-Gruppe.
(3) G ist unendlich.

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 Identität $x^n = 1$ nicht größer als $f(n, m)$ ist?

Die Antwort ist positiv: Zelmanov, Fields-Medaille 1994.

8 Präsentationen von Gruppen

Jede Gruppe ist homomorphes Bild einer freien Gruppe. Sei nämlich X ein Erzeugendensystem von G. Nach die universelle Eigenschaft, setzt sich die Identität auf X zu einem *surjektiven* Homomorphismus $\overline{\mathrm{id}}_X \colon F(X) \twoheadrightarrow G$ fort:



Sei $\pi \colon F(X) \twoheadrightarrow G$ eine Surjektion und $R \subseteq F(X)$ erzeuge $\operatorname{Ker}\pi$ als Normalteiler, d.h. $\langle\langle R\rangle\rangle = \operatorname{Ker}\pi$ und $\langle\langle R\rangle\rangle$ ist die normal Hülle von R in $F(X)$, die Menge aller endlichen Produkte von konjugierten von Elementen von R.

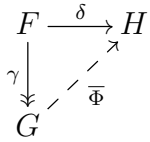
Definition 8.1 (Präsentation)**.** $G = \langle X \mid R\rangle$ ist eine *Präsentation* von G.
Die Elemente aus X nennt man *Erzeuger,* die Elemente aus R nennt man *Relatoren* von G, die Elemente aus $\langle\langle R\rangle\rangle$ (oder aus $\operatorname{Ker}\pi$) nennt man *Relationen* von G.
Eine Präsentation ist endlich wenn $|X| < \infty, |R| < \infty$.

- Jede Gruppe besitzt eine Präsentation;
- Jede endliche Gruppe sogar eine endliche Präsentation.

Lemma 8.2. *Seien* $\gamma \colon F \to G, \delta \colon F \to H$ *Homomorphismen mit:*

- $\operatorname{Bild}\gamma = G$*, d.h.* $\gamma \colon F \twoheadrightarrow G$;
- $\operatorname{Ker}\gamma \subseteq \operatorname{Ker}\delta$.

Dann gibt es einen Homomorphismus $\Phi \colon G \to H$ *sodaß* $\delta = \Phi \circ \gamma$:



Beweis. Wir definieren $\Phi(g) := \delta(\gamma^{-1}(g))$.
Die Abbildung ist wohldefiniert: seien $f, f' \in \gamma^{-1}(g)$,

$$\gamma(f) = \gamma(f') \Longrightarrow f'f^{-1} \in \operatorname{Ker}\gamma \subseteq \operatorname{Ker}\delta \Longrightarrow \delta(f') = \delta(f).$$

Die Abbildung ist Homomorphismus: seien $g, g' \in G, f, f' \in F, \gamma(f) = g, \gamma(f') = g'$,

$$\gamma(ff') = \gamma(f)\gamma(f') = gg', \quad \Phi(gg') = \delta(ff') = \delta(f)\delta(f') = \Phi(g)\Phi(g').$$

Das Dreieck kommutiert:

$$\Phi(\gamma(f)) = \delta(\gamma^{-1}(\gamma(f))) = \delta(f).$$

□

Satz 8.3 (Satz von Walther von Dyck'1882)**.** *Seien $G = \langle X \mid R\rangle$ und $H = \langle X \mid S\rangle$ zwei Gruppen mit $R \subseteq S$. Dann gibt es einen surjektiven Homomorphismus $\Phi\colon G \twoheadrightarrow H$ mit:*

(i) $\Phi|_X = \mathrm{id}_X$;

(ii) $\operatorname{Ker}\Phi = \langle\langle S \setminus R\rangle\rangle$.

Umgekehrt hat jede Faktorgruppe G eine Präsentation der Form $\langle X \mid S\rangle$ mit $S \supseteq R$.

Beweis. Sei F die freie Gruppe mit Basis X, $\gamma\colon F(X) \twoheadrightarrow G$ und $\delta\colon F(X) \twoheadrightarrow H$ die durch die Abbildungen $X \to G, x \mapsto x$ und $X \to H, x \mapsto x$ induzierten surjektiven Homomorphismen. Aus

$$\operatorname{Ker}\gamma = \langle\langle R\rangle\rangle, \quad \operatorname{Ker}\delta = \langle\langle S\rangle\rangle$$

und $R \subseteq S$ folgt: $\operatorname{Ker}\gamma \subseteq \operatorname{Ker}\delta$. Nach dem vorangegangenen Lemma gibt es einen Homomorphismus $\Phi\colon G \to H$ mit $\delta = \Phi \circ \gamma$. Da δ surjektiv ist, ist es auch Φ und für alle $x \in X$ gilt $\delta(x) = x$ sowie $\gamma(x) = x$ und damit $\Phi(x) = x$.

Es gilt $\operatorname{Ker}\Phi = \gamma(\operatorname{Ker}\delta)$ denn:

$$\operatorname{Ker}\delta = \delta^{-1}(1) = \gamma^{-1}(\Phi^{-1}(1)) \Longrightarrow \operatorname{Ker}\delta = \gamma^{-1}(\operatorname{Ker}\Phi) \Longrightarrow \operatorname{Ker}\Phi = \gamma(\operatorname{Ker}\delta).$$

Daraus folgt $\operatorname{Ker}\Phi = \langle\langle S \setminus R\rangle\rangle$.

Sei umgekehrt Q eine Faktorgruppe von G und π die kanonische Projektion auf Q:

$$\pi\colon G \twoheadrightarrow Q.$$

Dann ist $\pi \circ \gamma\colon F(X) \twoheadrightarrow Q$ ein Homomorphismus mit $R \subseteq \operatorname{Ker}\pi \circ \gamma$ und $\langle X \mid \operatorname{Ker}\pi \circ \gamma\rangle$ eine Präsentation von Q.

□

Beispiele 8.4 (Präsentationen).

1. Die zyklische Gruppe der Ordnung n kann offenbar wie folgt präsentiert werden $\mathbb{Z}/n\mathbb{Z} = \langle a \mid a^n\rangle$;

2. $F(X) = \langle X \mid \emptyset\rangle$ und $F_k = \langle x_1, \ldots, x_k \mid \emptyset\rangle$ sind Präsentationen von absolute freie Gruppen, über X und von rang $k > 0$;

3. Die Diedergruppe, die Gruppe aller Symmetrien des regelmäßigen n-Ecks (n Drehungen und n Spiegelungen) hat eine Präsentation

   $$D_n = \langle \sigma, \tau \mid \sigma^2 = \tau^n = 1, \sigma^{-1}\tau\sigma = \tau^{-1}\rangle \cong C_n \rtimes C_2$$

   und andere Präsentation

   $$D_n = \langle x, y \mid x^2, y^2, (xy)^n\rangle$$

   via $x = \sigma, y = \tau\sigma$.

4. Seien $G_1 = \langle X_1 \mid R_1\rangle, G_2 = \langle X_2 \mid R_2\rangle, X_1 \cap X_2 = \emptyset$. Das *freie Produkt* von G_1 und G_2 ist

   $$G_1 * G_2 = \langle X_1 \sqcup X_2 \mid R_1, R_2\rangle.$$

- $F_k * F_l \cong F_{k+l}$;
- $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} \cong D_\infty$ ($x \mapsto -x$ und $x \mapsto 1-x$ sind freie Erzeuger der Ordnung 2);
- $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z} \cong PSL(2,\mathbb{Z})$ [siehe Robinson 6.2].

Gegeben eine Familie von Gruppen $\{G_\alpha\}_{\alpha\in I}$, dann mit $*_\alpha G_\alpha$ bezeichnen wir das freie Produkt von Gruppen $G_\alpha, \alpha \in I$.

5. Seien $G_1 = \langle X_1 \mid R_1\rangle, G_2 = \langle X_2 \mid R_2\rangle, X_1 \cap X_2 = \emptyset, A \leqslant G_1$ und $\varphi\colon A \to G_2$ injektiv. Nehmen $W = \{w^{-1}\varphi(w) \mid w \in A\}$.

   Das *amalgamierte (freie) Produkt von Gruppen G_1 und G_2 nach der Untergruppe A* oder *das freie Produkt der Gruppen G_1 und G_2 mit der amalgamierten Untergruppe A* ist
   $$G_1 *_A G_2 = \langle X_1 \sqcup X_2 \mid R_1, R_2, W\rangle.$$

   - Seien $G_1 = \langle a \mid \emptyset\rangle, G_2 = \langle b \mid \emptyset\rangle, A = \langle a^2 \mid \emptyset\rangle, \varphi(a) = b^3$.
     Dann $G_1 *_A G_2 = \langle a, b \mid a^2 = b^3\rangle$.

6. Sei $G_0 = \langle X_0 \mid R_0\rangle$ eine Gruppe, $A, B \leqslant G_0$ Untergruppen, $\varphi\colon A \to B$ ein Isomorphismus; G_0 ist die *Basisgruppe*, A, B sind die *assoziierten Untergruppen* und t das *stabile Symbole.*

   Die *HNN-Erweiterung* (benannt nach Graham Higman, Bernhard H. Neumann und Hanna Neumann) ist eine Konstruktion, die für die Gruppe G_0 eine größere Gruppe G liefert, die G_0 als Untergruppe enthält: die HNN-Erweiterung ist die Gruppe
   $$G = G_0{*_A} = \langle X_0, t \mid R_0, t^{-1}at = \varphi(a), a \in A\rangle.$$

   Bemerkung (ohne Beweis): die Abbildung $G_0 \to G_0{*_A},\ g \mapsto g$ ist injektiv.

   - Seien $m, n \in \mathbb{Z},\ G_0 = \langle a \mid \emptyset\rangle, A = \langle a^m\rangle \leqslant G_0, B = \langle a^n\rangle \leqslant G_0$. Dann
     $$BS(m,n) = G_0{*_A} = \langle a, t \mid t^{-1}a^m t = a^n\rangle$$
     die Baumslag-Solitar Gruppen.

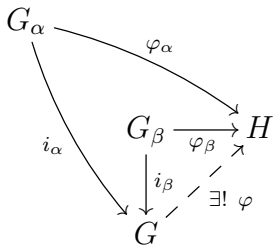
Wir können diese Produkte und HNN-Erweiterung mit Universelle Eigenschaften definieren.

Das freie Produkt von Gruppen erfüllt die folgende Universelle Eigenschaft: Ist $\{\varphi_\alpha\colon G_\alpha \to H\}_{\alpha\in I}$ eine Familie von Homomorphismen, so gibt es genau einen eindeutigen Homomorphismus
$$\varphi\colon *_\alpha G \to H \text{ so daß}$$
$\forall\alpha \in I$ die Identitäten $\varphi \circ i_\alpha = \varphi_\alpha$ gelten. Dabei ist $i_\alpha\colon G_\alpha \to *_\alpha G_\alpha$ die Identifikation von G_α mit der Untegruppe im freien Produkt.

Im Allgemeinen, sei $\mathcal{K}$ eine Klasse von Gruppen und $G_\alpha, \alpha \in I$, Gruppen von $\mathcal{K}$.

Definition 8.5 ($\mathcal{K}$-freie Produkt)**.** Eine Gruppe G von $\mathcal{K}$ zusammen mit Homomorphismen $i_\alpha\colon G_\alpha \to G$ heißt *$\mathcal{K}$-freies Produkt der Gruppen G_α*, wenn gilt $\forall H \in \mathcal{K}, \forall$ Homomorphismus $\varphi_\alpha\colon G_\alpha \to H$,
$$\exists!\text{ Homomorphismus } \varphi\colon G \to H \text{ sodaß } \varphi \circ i_\alpha = \varphi_\alpha,\ \forall\alpha \in I.$$

Mit anderen Worten, gibt es eindeutig die gestrichelte Abbildung, so dass das ganze Diagramm kommutiert:



Wenn G existiert, dann i_α injektiv, G_α können daher als Untegruppen von G aufgefasst werden. Tatsächlich, sei α fix, wähle $H := G_\alpha$ und $\varphi_\beta \colon G_\beta \to H = G_\alpha$ mit

$$\varphi_\beta = \begin{cases} \mathrm{id}_{G_\alpha} & \text{für } \alpha = \beta \\ 1_{G_\alpha} & \text{für } \alpha \neq \beta \end{cases}$$

wegen $\varphi \circ i_\beta = \mathrm{id}_{G_\alpha}$ folgt, daß i_β injektiv.

Sei $\mathcal{K}$ eine Klasse von Gruppen, A und $G_\alpha, \alpha \in I$, Gruppen von $\mathcal{K}$, $\psi_\alpha \colon A \to G_\alpha$ Monomorphismen.

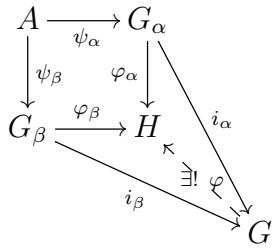
Definition 8.6 ($\mathcal{K}$-freie amalgamierte Produkt)**.** Eine Gruppe G von $\mathcal{K}$ zusammen mit Homomorphismen $i_\alpha \colon G_\alpha \to G$ mit

$$i_\alpha \circ \psi_\alpha = i_\beta \circ \psi_\beta,\ \forall \alpha, \beta \in I$$

heißt *über A amalgamiertes $\mathcal{K}$-freies Produkt der Gruppen G_α*, wenn gilt $\forall H \in \mathcal{K}, \forall$ Homomorphismus $\varphi_\alpha \colon G_\alpha \to H$ mit $\varphi_\alpha \circ \psi_\alpha = \varphi_\beta \circ \psi_\beta\ \forall \alpha, \beta \in I$,

$$\exists! \text{ Homomorphismus } \varphi \colon G \to H \text{ sodaß } \varphi \circ i_\alpha = \varphi_\alpha,\ \forall \alpha \in I.$$

Mit anderen Worten, wenn das durchgezogene Diagramm unten kommutiert, dann gibt es eindeutig die gestrichelte Abbildung, so dass das ganze Diagramm kommutiert.



Übung 16. Sei $\mathcal{K}$ eine Varietät, dann gibt es das amalgamiertes $\mathcal{K}$-freies Produkt.

Seien G_0, A, B, und $\varphi \colon A \to B$ wie oben.

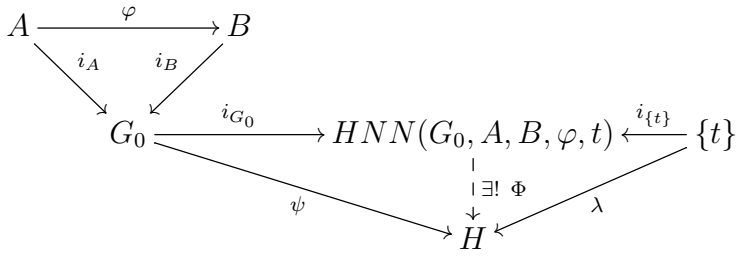
Gegeben H und der Homomorphismus $\psi \colon G_0 \to H$, sowie ein Element in H (aufgefasst als Bild unter einer Abbildung $\lambda \colon \{t\} \to H$) derart dass

$$\psi \circ \varphi(a) = \lambda(t)^{-1} \psi(a) \lambda(t)$$

für alle $a \in A$ gilt. Dann gibt es genau einen eindeutigen Homomorphismus

$$\Phi \colon G_0 *_A = HNN(G_0, A, B, \varphi, t) \to H$$

so daß das Diagram kommutiert ($i_A, i_B, i_{G_0}, i_{\{t\}}$ sind Injektionen).



Übung 17. Sei G die Baumslag-Solitar Gruppe mit $m = 2, n = 3$,

$$BS(2,3) = \langle a, t \mid t^{-1}a^2t = a^3 \rangle,$$

Sei $f\colon G \to G, t \mapsto t, a \mapsto a^2$. Die Elementen t, a^2 und dann a^3 und a sind in das Bild von f. Das folgt f ist surjektiv. Aber f ist nicht injektive: $w = a^{-1}t^{-1}ata^{-1}t^{-1}ata^{-1}$ ist in $\operatorname{Ker} f$ (d.h. $f(w) = 1_G$) und $w \neq 1_G$ nach Fakt:

Fakt (ohne beweis): sei u ist ein reduziert Wort in $a^{\pm 1}, t^{\pm 1}$ so daß $u = 1_G$. Dann u hat als ein Unterwort $t^{-1}a^kt$ mit $m|k$ oder ta^kt^{-1} mit $n|k$.

Das folgt: $w \neq 1_G$.

Analog: Man kann zeigen $|m|, |n| \neq 1 \Longrightarrow F_2 \leqslant BS(m,n)$.

Beispiele 8.7 (Präsentationen).

1. $T = \langle x, y \mid x^{-3}y^{-1}x^2y, y^{-3}x^{-1}y^2x \rangle$;
2. $G_n = \langle x_1, \ldots, x_{n-1} \mid R, S \rangle$ mit $R = \{x_1^2, \ldots, x_{n-1}^2, (x_1x_2)^3, \ldots, (x_{n-2}x_{n-1})^3\}$, $S = \{x_ix_jx_i^{-1}x_j^{-1} \mid 1 \leqslant i < j - 1 \leqslant n-2\}$;
3. $H = \langle a, b, c \mid c^{-1}a^{-1}b^{-1}ab, a^{-1}c^{-1}ac, b^{-1}c^{-1}bc \rangle$.

Proposition 8.8.

- *T ist isomorph zur trivialen Gruppe;*
- *G_n ist isomorph zur symmetrischen Gruppe $Sym(n)$;*
- *H ist isomorph zur Heisenberggruppe.*

Beweis. Siehe die Vorlesung. □

Definition 8.9. Eine Gruppe G ist endlich präsentierbar, wenn $\exists X$ endlich, $\exists R \subseteq (X \sqcup X^{-1})^*$ endlich mit $G \cong \langle X \mid R \rangle$.

Proposition 8.10. *Sei $G = \langle X \rangle$, wenn G eine endliche Präsentation besitzt, dann $\exists X_0 \subseteq X$, X_0 endlich, sodaß G eine endliche Präsentation bezüglich X_0 besitzt.*

Beweis. Siehe die Vorlesung.

□

Proposition 8.11. *Sei G endlich präsentierbar und $G = \langle x_1, \ldots, x_m \mid r_n, n \in \mathbb{N} \rangle$, dann sind alle bis auf endlich viele der Relatoren überflüssig.*

Beweis. Nach Proposition 8.10, G hat bezüglich $x_1, \ldots, x_m$ eine endliche Präsentation

$$G \cong \langle x_1, \ldots, x_m \mid w_1, \ldots, w_k \rangle.$$

Sei $F = F(x_1, \ldots, x_m)$. Dann gilt $G = F/N$ wobei $N = \langle\langle r_n, n \in \mathbb{N} \rangle\rangle = \langle\langle w_1, \ldots, w_k \rangle\rangle$. Jedes w_i ist ein Produkt von Konjugierten von r_n, dazu werden für alle w_i's nur endlich viele der r_n's gebraucht, d.h. $\exists L$ sodaß $w_i \in \langle\langle r_1, \ldots, r_L \rangle\rangle,\ \forall i$. Dann

$$\langle\langle r_1, \ldots, r_L \rangle\rangle \geqslant \langle\langle w_1, \ldots, w_k \rangle\rangle = \langle\langle r_n, n \in \mathbb{N} \rangle\rangle \geqslant \langle\langle r_1, \ldots, r_L \rangle\rangle,$$

Dann $G = \langle x_1, \ldots, x_m \mid r_1, \ldots, r_L \rangle$. □

Beispiel 8.12. $G = \langle x, y, t \mid t^{-1}(x^{-n}yx^n)t = y^{-n}xy^n, n = 1, 2, \ldots \rangle$ ist nicht präsentierbar.

Beweis. Annehmen $G = \langle x, y, t \mid t^{-1}(x^{-n}yx^n)t = y^{-n}xy^n, n = 1, 2, \ldots, N \rangle$.

Verwenden HNN-Erweiterungen. Seien $F = F(x, y), A = \{x^{-n}yx^n \mid n = 1, 2, \ldots\}, B = \{y^{-n}xy^n \mid n = 1, 2, \ldots\} \setminus \{y^{-N}xy^N\}$. Beide Mengen sind freie Erzeugendensysteme. Wir definieren eine Bijektion von A nach B:

$$\varphi = \begin{cases} x^{-n}yx^n \mapsto y^{-n}xy^n, & n < N \\ x^{-n}yx^n \mapsto y^{-(n+1)}xy^{n+1}, & n \geqslant N \end{cases}$$

φ setzt sich zu einem Homomorphismus $\langle A \rangle \to \langle B \rangle$ fort. Nach Universelle Eigenschaft, gibt es $H = \langle x, y, t \rangle$, sodaß $F \leqslant H$ und $\varphi(a) = t^{-1}at,\ \forall a \in \langle A \rangle$. In H gilt

$$\begin{aligned} t^{-1}(x^{-n}yx^n)t &= y^{-n}xy^n, \ n \leqslant N - 1 \\ t^{-1}(x^{-n}yx^n)t &= y^{-(n+1)}xy^{n+1}, \ n \geqslant N \end{aligned}$$

Nach Annahme gilt in H auch $t^{-1}(x^{-n}yx^n)t = y^{-n}xy^n,\ n \geqslant N$. Dann erfüllt $y^{-(N+1)}xy^{N+1} = y^{-N}xy^N \Longrightarrow y^{-1}xy = x \Longrightarrow xy = yx$ in H. Das ist ein Widerspruch dazu, daß $\langle x, y \rangle = F$ ist. □

Proposition 8.13. *Sei $N \trianglelefteq G$, wenn N und G/N endlich präsentierbar sind, dann auch G.*

Beweis. Annahmen $N = \langle x_1, \ldots, x_n \mid r_1, \ldots, r_k \rangle$ und
$G/N = \langle y_1N, \ldots, y_nN \mid s_1(y_1N, \ldots, y_nN), \ldots, s_l(y_1N, \ldots, y_nN) \rangle$

□

9 Die Dehn'schen Entscheidungsprobleme

• Das *Wortproblem*: Sei $\langle X \mid R \rangle$ eine Präsentation einer Gruppe G und F die absolut freie Gruppe mit Basis X. Das *Wortproblem* ist die Frage, ob es einen Algorithmus gibt, der entscheiden kann, ob zwei Wörter $u, v \in F$ in G das selbe Element repräsentieren. Eine äquivalente Frage ist, ob es einen Algorithmus gibt, der entscheidet, ob ein Wort $w \in F$ in $\langle\langle R \rangle\rangle$ liegt. Gibt es einen solchen Algorithmus, so nennt man das Wortproblem für diese Präsentation entscheidbar.

• Das *Konjugationsproblem*: Sei $\langle X \mid R \rangle$ eine Präsentation einer Gruppe G und F die freie Gruppe mit Basis X. Das Konjugationsproblem ist die Frage, ob es einen Algorithmus gibt, der entscheiden kann, ob zwei Wörter $u, v \in F$ in G konjugiert sind.

Hat eine Präsentation ein entscheidbares Konjugationsproblem, so ist auch das Wortproblem entscheidbar. Umgekehrt gibt es allerdings Präsentationen, die ein entscheidbares Wortproblem haben, aber ein unentscheidbares Konjugationsproblem.

• Das *Isomorphieproblem*: Das Isomorphieproblem ist die Frage, ob es einen Algorithmus gibt, der entscheiden kann, ob zwei endliche Präsentationen isomorphe Gruppen definieren.

Beispiele 9.1.

1. $F(X)$ hat entscheidbares Wortproblem;
2. Freie abelsche Gruppe hat entscheidbares Wortproblem;
3. Die Diedergruppe hat entscheidbares Wortproblem.

Proposition 9.2. *Hat eine endliche Präsentation einer Gruppe ein entscheidbares Wort– oder Konjugationsproblem, so gilt dies für jede endliche Präsentation dieser Gruppe.*

Beweis. Seien $\langle X \mid R\rangle$ und $\langle Y \mid S\rangle$ zwei endliche Präsentationen der selben Gruppe G, F_1 und F_2 die freien Gruppen mit Basis X bzw. Y. Die Präsentation $\langle X \mid R\rangle$ habe ein entscheidbares Wort oder Konjugationsproblem. Definiere eine Abbildung $\varphi\colon Y \to F_1$, sodass für alle $x \in Y, \varphi(x)$ und x in G das selbe Element repräsentieren. Diese setzt sich zu einem Homomorphismus $\Phi\colon F_2 \to F_1$ fort. Φ ist berechenbar: Sei $w \in F_2, w = y_1 \cdots y_n$ mit $y_1, \ldots, y_n \in Y$. Dann ist $\Phi(w) = \Phi(y_1) \cdots \Phi(y_n)$, wobei die Werte von $y \in Y$ in einer endlichen Wertetabelle hinterlegt werden können. Das Wort oder Konjugationsproblem für zwei Wörter $u, v \in F_2$ lässt sich nun entscheiden, indem man den Algorithmus für $\langle X \mid R\rangle$ auf $\Phi(u)$ und $\Phi(v)$ anwendet. □

Bibliography

[Rot95] Joseph J. Rotman, *An introduction to the theory of groups*, 4th ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995. MR1307623 (95m:20001)

[Ros10] Stephan Rosebrock, *Geometrische Gruppentheorie: Ein Einstieg mit dem Computer*, Basiswissen für Studium und Mathematikunterricht, Vieweg+Teubner Verlag, 2010 (German).

[KM96] M. I. Kargapolov and Yu. I. Merzlyakov, *Osnovy teorii grupp*, 4th ed., Fizmatlit "Nauka", Moscow, 1996 (Russian, with Russian summary). (requested by Russian speaking students).