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.

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 $\{f \in \mathrm{Abb(X, X)} \mid f \text{ ist ein Homöomorphismus mit } \pi \circ \mathrm{f} = \pi\}$ 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).

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

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 $X \leqslant$ 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 $i + 1$: 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 $|H| = |P| \Longrightarrow gHg^{-1} = P$.

Proof. 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.

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, $\alpha(h) = \mathrm{id}$ 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 $= H$. 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) besagt, jedes $g \in G$ läßt sich eindeutig darstellen als $g = nh$ mit $n \in N, h \in H$.

Tatsächlich, $g = nh = n_1 h_1 \implies N \ni n_1^{-1} n = h_1 h^{-1} \in H \implies N \cap H \ni n_1^{-1} n = h_1 h^{-1} = 1 \implies n_1 = n$ 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: $h \in H$, $\alpha(h)\colon n \mapsto \alpha(h)(n) = hnh^{-1}$.

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

$(n, h)(n_1, h_1) = n \cdot hn_1h^{-1} \cdot hh_1 = n\alpha(h)(n_1)hh_1$.

Beispiele des Semi-direktes Produktes, Erweiterungen, Exakt Sequenzen, Kranzprodukte: siehe der Kurs am 17.03.2015.

Reihen und Zerlegungen: siehe der Kurs am 24.03.2015.

---

4 Auflösbare, Nilpotente, p-Gruppen

Definition 4.1 (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 4.2.

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 aller 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 besitzt keinen echten nichttrivialen Normalteiler (sie ist einfach). 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 4.3. 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 4.4 (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, d.h. das Bild von H ist wieder in H.
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 2. Für jede Gruppe G ist das Zentrum $Z(G)$ charakteristisch, aber nicht notwendig vollinvariant in G.

Lemma 4.5. *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 dem folgenden Satz:

Proposition 4.6. *(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 4.5 (i) dass alle $G^{(i)}$ sind voll invariante (dann charakteristische) Untergruppen, daher Normalteiler.

Zunächst deshalb einige ergänzende Überlegungen zu höheren Kommutatorgruppen:

Lemma 4.7.

- *(i) Für höhere Kommutatorgruppen ist folgendes richtig: $H \leqslant G$, dann $H^{(n)} \leqslant G^{(n)}$;*
- *(ii) $N \trianglelefteq G$, dann 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 4.8.

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 4.9. *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 $dl(G)$.

Proof. ($\Rightarrow$) 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 4.8 und Satz 4.9, 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 4.10.

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 es Untergruppen H und K gibt so daß $H \trianglelefteq K \trianglelefteq G$ und K/H einfach, nicht abel'sch (c.f. Beispiel 4.2).

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

Sei $X = \{x_1, x_2, \dots, \}$, definiere durch Induktion Wörter $w_n = w_n(x_1, \dots, x_{2^n})$: $w_1(x_1, x_2) = [x_1, x_2]$, ist w_n schon definiert $w_n^* = w_n(x_{2^n+1}, \dots, x_{2^{n+1}})$ 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. $G \models w_i = 1 \iff \forall g_1, \dots, g_{2^i} \in G$ es gilt $w_i(g_1, \dots, g_{2^i}) = 1$ in G.

Wir zeigen per Induktion nach n:

Satz 4.11. *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 beruhmte Sätze auf, werden diese aber nicht beweisen.

Satz 4.12 (von Burnside)**.** *Alle Gruppen der Ordnung $p^k q^l$ mit Primzahlen p, q und $k, l \in \mathbb{N}$ sind auflösbar.*

Satz 4.13 (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 4.14 (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 4.15 (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 4.16 (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 $Z_{i+1}(G)$ 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 4.17. *$\forall i \;\; Z_i(G)$ 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 4.18.

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 4.19. *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 4.20. $\forall n \quad \gamma_n(G) = \langle [g_1, \dots, g_n] \mid g_1, g_2, \dots, g_n \in G \rangle$ *erzeugt von den* $[g_1, \dots, g_n] := [[g_1, \dots, g_{n-1}], g_n]$.

Proof. 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 4.21 (Zentralereihen)**.** *Sei* $\{1\} = G_0 \leqslant G_1 \leqslant \dots \leqslant G_{n-1} \leqslant G_n = G$, *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 folgt wegen $G_{i+1}/G_i \leqslant Z(G/G_i)$ dass $G_{i+1}Z_i(G)/Z_i(G) \leqslant Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G) \Longrightarrow G_{i+1} \leqslant Z_{i+1}(G)$.

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

Wir zeigen per Induktion nach n:

Satz 4.22. *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 4. 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 4.23. *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 5 (3-Untergruppen Lemma). Seien A, B, C normale Untergruppen von G. So gilt

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

Proposition 4.24. *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 richtig $\forall$ p-Gruppen H mit $|H| < |G|$. 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 4.25. *Jede nichttriviale nilpotente Gruppe hat ein nichttriviales Zentrum.*

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

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).