Gruppentheorie: kurze Wiederholung

Themen

Gruppen, Untergruppen
Gruppenordnung
Äquivalenzrelationen
Satz von Lagrange
Homomorphismen
Faktorgruppen
Isomorphiesätze
Chinesischer Restsatz
Zyklische Gruppen
Direkte und semidirekte Produkte
Symmetrische Gruppe
Sylowsätze

Einige wichtige Konzepte

Gruppenaxiome

Sei G eine Menge und $\cdot : G \times G \to G$; $(x, y) \mapsto x \cdot y = xy$ eine Abbildung. Wir betrachten folgende Axiome:

(a) Assoziativität: $\forall x, y, z \in G$: $(xy)z = x(yz)$.

(b) Neutrales Element: $\exists! e \in G \forall x \in M$: $ex = x = xe$.

(c) Inverses Element: $\forall x \in G \exists! x' \in G$: $xx' = e = x'x$. Wir setzen $x^{-1} := x'$.

(d) Kommutativität: $\forall x, y \in G$: $xy = yx$.

$(G, \cdot)$ heißt Gruppe, falls (a), (b), (c) gelten, abelsche Gruppe, falls zusätzlich (d) gilt.

Untergruppen

Eine Teilmenge H einer Gruppe $(G, \cdot)$ heißt Untergruppe, falls sie selbst wieder eine Gruppe ist.
Dies ist der Fall, wenn zusätzlich gilt

(a) $e \in H$

(b) $\forall x, y \in H$ ist $xy \in H$

(c) $\forall x \in H : x^{-1} \in H$.

Sie $X \subset G$.

$$\langle X \rangle = \{y \in G \mid \exists n \in \mathbb{N}_0, x_1, \ldots, x_n \in X \cup X^{-1} : y = x_1 \cdots x_n\}$$

ist die von X erzeugte Untergruppe von G.
Ist $X = \{x\}$, so ist

$$\langle x \rangle = \langle \{x\} \rangle = \{x^a \mid a \in \mathbb{Z}\}$$

abelsche Untergruppe (zyklische Gruppe).

Ordnung

Die Zahl $|G| \in \mathbb{N}_0 \cup \{\infty\}$ heißt Ordnung der Gruppe G.
Für $x \in G$ gilt $\mathrm{ord}(x) = |\langle x \rangle| \in \mathbb{N}_0 \cup \infty$.
Sei p eine Primzahl. Eine endliche Gruppe heißt p-Gruppe, falls es $n \in \mathbb{N}$ gibt mit $|G| = p^n$.
Hat $x \in G$ endliche Ordnung, so sind äquivalent:

(a) $n = \mathrm{ord}(x) = |\langle x \rangle|$,

(b) $\langle x \rangle = \{e, x, \ldots, x^{n-1}\}$ und $x_i \neq x_j$ für $i \neq j$,

(c) $\forall z \in \mathbb{Z} : x^z = e \Leftrightarrow n | z$,

(d) $n = \min\{k \in \mathbb{N} \,|x^k = e\}$.

Äquivalenzrelationen

Sei X eine Menge. Eine Relation $\sim$ auf X heißt Äquivalenzrelation falls

(a) $\forall x \in X$: $x \sim x$ (Reflexivität)

(b) $\forall x, y \in X$: $x \sim y \Leftrightarrow y \sim x$ (Symmetrie)

(c) $\forall x, y, z \in X$: $x \sim y, y \sim z \Rightarrow x \sim z$ (Transitivität)

Für $x \in X$ heißt $\overline{x} = \{y \in X \mid x \sim y\}$ die Äquivalenzklasse von x.

Satz von Lagrange

Sei G eine Gruppe, $H \subset G$ eine Untergruppe. Betrachte die Äquivalenzrelation auf G:

$$x \sim y \Leftrightarrow \exists h \in H : xh = y \Leftrightarrow x^{-1}y \in H \Leftrightarrow y^{-1}x \in H.$$

$\overline{x} = xH$ ist die Linksnebenklasse von H in G repräsentiert durch x. Die Menge aller Linksnebenklassen von H in G ist G/H. (Genauso für rechts statt links.)
Die Zahl $[G : H] = |G/H| = |H\backslash G| \in \mathbb{N} \cup \{\infty\}$ heißt Index von H in G.

Satz. *Sei G endliche Gruppe, $H \subset G$ Untergruppe. Dann gilt*

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

Insbesondere sind $[G : H]$ und $|H|$ Teiler von $|G|$.

Gruppenoperationen

Sei X eine Menge $\neq \emptyset$, G eine Gruppe. Eine Abbildung

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

heißt (Links)Operation von G auf X, falls

(a) für alle $x \in X$ gilt $ex = x$;

(b) für alle $x \in X$ und $g_1, g_2 \in G$ gilt $g_2(g_1x) = (g_1g_2)x$.

Die Operation heißt transitiv, falls es für alle $x, y \in X$ ein $g \in G$ gibt mit $y = gx$.
Die Bahn von $x \in X$ ist $\overline{x} = Gx = \{gx \mid g \in G\} \subset X$.
Der Stabilisator von $x \in X$ ist $G_x = \mathrm{Stab}_G(x) = \{g \in G \mid gx = x\} \subset G$, eine Untergruppe von G.
Die Fixpunkte von G sind $X^G = \{x \in X \mid gx = x \forall g \in G\} \subset X$.

Bahnengleichung

Sei X endliche Menge, G endliche Gruppe, $G \times X \to X$, $(g, x) \mapsto gx$ eine Operation.

(a) Für alle $x \in X$ gilt $|Gx| = [G : G_x]$.

(b) Ist $T \subset X$ eine Transversale der Bahnen dann ist die Vereinigung $X = \bigcup_{x \in T} Gx$ disjunkt.

(c) Es gilt

$$|X| = \sum_{x \in T} [G : G_x].$$

Ist X_0 die Menge der Fixpunkte, dann gilt

$$|X| = |X_0| + \sum_{x \in T \setminus X_0} [G : G_x].$$

Konjugation

Sei G eine Gruppe. $x, y \in G$ sind zueinander konjugiert $\Leftrightarrow \exists u \in G : uxu^{-1} = y$.
Die Konjugationsklasse (Äquivalenzklasse) von $x \in G$ ist

$$C_x = \{uxu^{-1} : u \in G\} \subseteq G.$$

Der Zentralisator (Stabilisatoruntergruppe) von $x \in G$ ist

$$C_G(x) = \{u \in G : uxu^{-1} = x\} = \{u \in G : ux = xu\} \subseteq G.$$

Das Zentum einer Gruppe ist

$$Z(G) = \{x \in G : ux = xu \forall u \in G\}.$$

Ist C_x die Konjugationsklasse von x, dann gilt

$$|C_x| = [G : C_G(x)].$$

Klassengleichung: Sei S eine Transversale der Konjugationsklassen in $G \backslash Z(G)$, dann gilt

$$|G| = |Z(G)| + \sum_{s \in S} [G : C_G(s)].$$

Homomorphismus

Seien G und G' Gruppen. Eine Abbildung $f : G \to G'$ heißt Homomorphismus, falls für alle $x, y \in G$: $f(xy) = f(x)f(y)$. Dann gilt $f(e) = e'$ und $f(x^{-1}) = f(x)^{-1}$.

— Isomorphismus: f ist bijektiv $\Leftrightarrow$ f hat ein inverses $f' = f^{-1} : G' \to G$
— Endomorphismus $:\Leftrightarrow G = G'$
— Automorphismus $:\Leftrightarrow$ f ist bijektiv und $G = G'$
— f ist injektiv $\Leftrightarrow \ker(f) = e$
— f ist surjektive $\Leftrightarrow \mathrm{im}(f) = G'$
— Sind $H \subset G$ und $H' \subset G'$ Untergruppen, dann sind $f(H) \subset G'$ und $f^{-1}(H') \subset G$ Untergruppen. Insbesondere sind $\ker(f) \subset G$ und $\mathrm{im}(f) \subset G'$ Untergruppen.

Normalteiler

Sei G Gruppe. Eine Untergruppe $N \subset G$ heißt Normalteiler, wenn für alle $x \in G$ $xNx^{-1} = N$, geschrieben $N \triangleleft G$.

— Ist $f : G \to G'$ Homomorphismus, dann ist $\ker(f) \triangleleft G$.
— Ist $N' \triangleleft G'$, dann ist $f^{-1}(N') \triangleleft G$.
— Ist f surjektiv und $N \triangleleft G$, dann ist $f(N) \triangleleft G'$.
— Ist $N \triangleleft G$, so ist G/N eine Gruppe (Faktorgruppe von G modulo N. Kanonische Abbildung $\pi : G \to G/N$ mit $\ker(\pi) = N$.

Isomorphiesätze

Sei $f : G \to G'$ Gruppenhomomorphismus.

Homomorphiesatz: Es gibt genau einen injektiven Homomorphismus $f' : G/Ker(f) \to G'$ mit $f = f' \circ \pi$ wobei π der kanonische Homomorphismus ist, das heißt, das Diagramm

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & G' \\ & G/\ker(f) \arrow[ur, "f'"'] & \end{tikzcd}$$

kommutiert. Insbesondere ist

$$f' : G/\ker(f) \to \mathrm{im}(f), x\ker(f) \mapsto f(x)$$

Isomorphismus.

1. **Isomorphiesatz:** Sei $H \subset G$ Untergruppe und $N \triangleleft G$ Normalteiler. Dann ist $HN = NH$ Untergruppe von G, $N \triangleleft HN$. $H \cap N \triangleleft H$, und die Abbildung
$$H/H \cap N \to HN/N, hH \cap N \mapsto hN$$
ist Isomorphismus.
2. **Isomorphiesatz:** Seien $M \triangleleft G$, $N \triangleleft G$ Normalteiler mit $M \subset N$. Dann sind $M \triangleleft N$, $N/M \triangleleft G/M$ Normalteiler, und die Abbildung
$$G/N \to (G/M)/(N/M), xN \mapsto (xM)(N/M)$$
ist Isomorphismus.

Zyklische und einfache Gruppen

Sei G Gruppe. G ist genau dann zyklisch, wenn es $n \in \mathbb{N}_0$ gibt, mit $G \cong \mathbb{Z}/\mathbb{Z}n$. Ist G zyklisch, dann sind auchdie Unter- und Faktorgruppen von G zyklisch.
G heißt einfach, wenn $G \neq \{e\}$ und G außer G und $\{e\}$ keine Normalteiler enthält.

Direktes Produkt

Seien $G_1, \dots, G_r$ Gruppen. Das kartesische Produkt $G := \prod_{i=1}^r G_i$ mit komponentenweiser Multiplikation heißt auch direktes Produkt der G_i.
Sei G eine Gruppe und $H_1, \dots, H_r$ Untergruppen. G ist direktes Produkt der H_i, wenn
$$f : \prod_{i=1}^r H_i \to G, (x_1, \dots, x_r) \mapsto x_1 \cdots x_r$$
ein Isomorphismus ist.
Dann sind $H_1, \dots, H_r$ sind Normalteiler mit
$$G = H_1 \cdots H_r \quad \text{und} \quad H_i \cap (H_{i+1} \dots H_r) = \{e\}$$
für $1 \leqslant i \leqslant r$.
Man schreibt
$$G = H_1 \times \cdots \times H_r = \times_{i=1}^r H_i.$$
oder falls G abelsch ist
$$G = H_1 \oplus \cdots \oplus H_r = \bigoplus_{i=1}^r H_i.$$

Hauptsatz für endliche abelsche Gruppen

Sei A endliche abelsche Gruppe, $|A| = n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, $r \in \mathbb{N}_0$, Primzahlen $p_1 < \cdots < p_r$, und $\nu_i \in \mathbb{N}$. Dann gibt es $b_{ij} \in A$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s_i$, und natürliche Zahlen $k_{i1} \geqslant \ldots \geqslant k_{is_i} \geqslant 1$ mit
$$A = \bigoplus_{i=1}^r \bigoplus_{j=1}^{s_i} \mathbb{Z}\, b_{ij} \quad \text{und } \operatorname{ord}(b_{ij}) = p_i^{k_{ij}} \text{ für } 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s_i.$$
Diese Zerlegung ist eindeutig.

Semidirektes Produkt

Seien G_1, G_2 Gruppen und $\tau : G_2 \to \operatorname{Aut}(G_1)$ ein Homomorphismus. Die Menge $G_1 \times G_2$ ist Gruppe:
— Multiplikation: $(x, y)(x', y') = (x\tau(y)(x'), yy')$
— Neutrales Element: (e, e)
— Inverses: $(x, y)^{-1} = (\tau(y^{-1})(x^{-1}), y^{-1})$
Sie heißt äußeres Semidirektes Produkt $G_1 \times_\tau G_2$.
Sei G eine Gruppe, $N \triangleleft G$, $H \subset G$ Untergruppe mit $G = NH = HN$ und $N \cap H = \{e\}$, sei $H \to \operatorname{Aut}(N)$ definiert durch $\kappa(y)(x) = yxy^{-1}$ für $x \in N$, $y \in H$. Dann ist
$$f : N \times_\kappa H \to G, (x, y) \mapsto xy$$
ein Isomorphismus.
G heißt inneres semidirektes Produkt von N und H.

Symmetrische Gruppen

Zykel: $\sigma = (a_1 \dots a_k) \in \mathfrak{S}_n$ = Zykel der Länge k: $a_1, \dots, a_k \in \{1, \dots, n\}$ paarweise verschieden mit

$$\begin{aligned} \sigma(a_i) &= a_{i+1} \quad \text{für } 1 \leqslant i < k, \\ \sigma(a_k) &= a_1, \\ \sigma(x) &= x \quad \text{für } x \in \{1, \dots, n\} \backslash \{a_1, \dots, a_k\} \end{aligned}$$

Zweizykel heißen Transpositionen.
Jedes Element $\sigma \in \mathfrak{S}_n$ ist Produkt von endlich vielen disjunkten Zykeln $\sigma = \sigma_1 \cdots \sigma_r$.
Es gilt $\operatorname{ord}(\sigma) = \operatorname{kgV}(\operatorname{ord}(\sigma_i))$.
Typ einer Permutation: Sei $\sigma = \sigma_1 \cdots \sigma_r$ Zerlegung in paarweise disjunkte Zyklen, $k_i = \operatorname{ord}(\sigma_i)$, $k_1 \geqslant \cdots \geqslant k_r$. Dann heißt $(k_1, \dots, k_r)$ Typ von σ.
Zwei Permutationen sind genau dann konjugiert, wenn sie denselben Typ haben.
Signum einer Permutation:

$$\varepsilon : \mathfrak{S}_n \to \{-1, 1\}, \varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Ist $\sigma = \tau_1 \cdots \tau_n$ Produkt von Transpositionen, dann gilt

$$\varepsilon(\sigma) = (-1)^n.$$

Ist $\sigma = \sigma_1 \cdots \sigma_r$ Produkt von disjunkten Zyklen, $\operatorname{ord}(\sigma_i) = k_i$, dann gilt

$$\varepsilon(\sigma) = (-1)^{\sum (k_i - 1)}.$$

σ heißt gerade (bzw. ungerade) falls $\varepsilon(\sigma) = 1$ (bzw. $\varepsilon(\sigma) = -1$).
Alternierende Gruppe: Man setzt

$$A_n = \ker \varepsilon.$$

Dies ist die Menge der geraden Permutationen und der einzige Normalteiler vom Index 2 von $\mathfrak{S}_n$. Es gilt

$$\begin{aligned} \mathfrak{S}_n / A_n &\cong \{-1, 1\} \\ |A_n| &= \frac{n!}{2}. \end{aligned}$$

$\mathfrak{S}_n$ ist semidirektes Produkt von A_n und jeder von einer Transposition erzeugten Untergruppe.
Wir wissen $A_2 = \{\mathrm{id}\}$, $A_3 = \langle (123) \rangle$, A_4 ist nicht einfach, A_3 schon. Für $n \geqslant 5$ ist A_n einfach.

Sylow-Sätze

Normalisator: Sei $H \subset G$ Untergruppe einer endlichen Gruppe:

$$N_G(H) = \{x \in G \mid xHx^{-1} = H\}$$

heißt Normalisator von H in G. $N_G(H)$ ist die größte Untergruppe von G, in der H als Normalteiler enthalten ist.
p-Sylowuntergruppe: Seien G eine endliche Gruppe, p eine Primzahl, $|G| = p^a m$ mit $a \in \mathbb{N}_0$, $m \in \mathbb{N}$ und $p \nmid m$. Eine Untergruppe der Ordnung p^a von G heißt p-Sylowuntergruppe.

Satz 0.1 (Sylow)**.** *Sei G eine endliche Gruppe, p Primzahl, $|G| = p^a m = n$ mit $p \nmid m$.*

(a) G enthält mindestens eine p-Sylowuntergruppe, und jede p-Untergruppe ist in einer solchen enthalten.

(b) Je zwei p-Sylowuntergruppen sind zueinander konjugiert.

(c) Sei s_p die Anzahl der p-Sylowgruppen, sei P eine p-Sylowgruppe. Dann gilt

$$s_p = [G : N_G(P)] \quad , \quad s_p \big| m \quad \textit{und} \quad s_p \equiv 1 \mod p.$$

Sei G eine endliche Gruppe, p Primzahl; dann sind folgende Aussagen äquivalent:

(a) G ist p-Gruppe.

(b) Für alle $x \in G$ ist $\operatorname{ord}(x)$ p-Potenz.

Die Sylowsätze haben viele wichtige Anwendungen!

Nilpotente Gruppen

Kommutator: Für $x, y \in G$ heißt $[x, y] = xyx^{-1}y^{-1}$ Kommutator von x und y. Es gilt

$$[x, y] = e \quad \Leftrightarrow \quad xy = yx.$$

Für Untergruppen $H, K \subset G$ ist $[H, K]$ die Kommutatoruntergruppe. $[G, G]$ ist die Kommutatoruntergruppe von G.

Absteigende Zentralreihe:

$$\begin{aligned} C^1(G) &= G \\ C^{i+1}(G) &= [C^i(G), G] \end{aligned}$$

— $C^i(G) \triangleleft G$, $i \geqslant 1$,
— $G = C^1(G) \supset C^2(G) \supset \dots$
— Da $C^i(G)/C^{i+1}(G) \subset Z(G/C^{i+1}(G))$ ist, ist $C^i(G)/C^{i+1}(G)$ abelsch.
— Die Folge $\left(C^i(G)\right)_{i \geqslant 1}$ heißt absteigende Zentralreihe von G.

Nilpotente Gruppen: Eine endliche Gruppe heißt nilpotent, falls folgende äquivalente Bedingungen erfüllt sind:

(a) Es gibt $n \in \mathbb{N}$ mit $C^n(G) = \{e\}$.
(b) Es gibt eine Folge von Untergruppen $G = H_1 \supset H_2 \supset \dots \supset H_m = \{e\}$ mit $[H_i, G] \subset H_{i+1}$, $1 \leqslant i \leqslant m - 1$. (Dann gilt $H_i \triangleleft G$.)

— p-Gruppen sind nilpotent.
— Untergruppen, Faktorgruppen und endliche direkte Produkte endlicher nilpotenter Gruppen sind nilpotent.
— Ist G endlich, $H \subset Z(G)$ eine Untergruppe und ist G/H nilpotent, dann ist G nilpotent.

Auflösbare Gruppen

Abgeleitete Reihe:

$$\begin{aligned} D^0(G) &= G \\ D^1(G) &= [G, G] \\ D^{n+1}(G) &= D^1(D^n(G)) = [D^n(G), D^n(G)] \quad \text{für } n \geqslant 1 \end{aligned}$$

— $D^n(G) \triangleleft G$, $n \geqslant 0$
— $G = D^0(G) \supset D^1(G) \supset D^2(G) \supset \dots$
— Die Faktorgruppe $D^n(G)/D^{n+1}(G)$ ist abelsch aber im Allgemeinen nicht zentrale Untergruppe von $G/D^{n+1}(G)$, $n \geqslant 0$.
— Die Folge $\left(D^i(G)\right)_{i \geqslant 1}$ heißt abgeleitete Reihe von G.

Auflösbare Gruppen: Eine Gruppe G heißt auflösbar, wenn folgende äquivalente Bedingungen erfüllt sind:

(a) Es gibt $n \in \mathbb{N}_0$ mit $D^n(G) = \{e\}$.
(b) Es gibt eine Folge von Normalteilern $G = H_0 \supset H_1 \supset \dots \supset H_m = \{e\}$, $m \geqslant 0$, so daß H_i/H_{i+1} abelsch ist für $0 \leqslant i < m$.
(c) Es gibt eine Folge von Untergruppen $G = H_0 \supset H_1 \supset \dots \supset H_m = \{e\}$, $m \geqslant 0$, so daß $H_{i+1} \triangleleft H_i$ und H_i/H_{i+1} abelsch ist für $0 \leqslant i < m$. (Normalreihe mit abelschen Faktoren)

— Ist G auflösbar, so auch jede Untergruppe und jedes epimorphe Bild von G.
— Ist $N \triangleleft G$, so daß N und G/N auflösbar sind, dann ist G auflösbar.
— Endliche direkte Produkte auflösbarer Gruppen sind auflösbar.

Beispiele

Beispiele für Gruppen:

(a) Sei K ein Körper, dann ist $(K, +)$ abelsche Gruppe, $(K, \cdot)$ abelsches Monoid und $(K \backslash \{0\}, \cdot)$ abelsche Gruppe.

(b) $(\mathbb{Z},+)$ abelsche Gruppe, $(\mathbb{Z},\cdot)$ abelsches Monoid, $(\mathbb{Z}\setminus\{0\},\cdot)$ abelsches Monoid, $(\{1,-1\},\cdot)$ abelsche Gruppe.

(c) Sei $\mathcal{X}\neq\emptyset$ eine Menge. Die Menge $\mathfrak{S}_{\mathcal{X}}$ aller Bijektionen von $\mathcal{X}$ nach $\mathcal{X}$ ist bezüglich der Komposition eine Gruppe, die symmetrische Gruppe von $\mathcal{X}$. Ist $\mathcal{X}=\{1,\dots,n\}$, dann setzt man $\mathfrak{S}_n:=\mathfrak{S}_{\mathcal{X}}$. Es gilt $|\mathfrak{S}_n|=n!$. $\mathfrak{S}_n$ ist nur für $n=1,2$ abelsch. Die Elemnte der $\mathfrak{S}_n$ werden in der Gestalt $\sigma=\binom{1\dots n}{\sigma(1)\dots\sigma(n)}$ geschrieben.

(d) Ist $(M,\cdot)$ Monoid, dann ist $M^\times=\{x\in M\mid\exists x'\in M: xx'=e='x\}$ eine Gruppe; sie heißt Einheitengruppe von $(M,\cdot)$. Speziell $(\mathbb{Z},\cdot)^\times=\{1,-1\}$.

(e) Sind $G_1,\dots,G_n$ Gruppen (Monoide), dann ist das kartesische Produkt $G_1\times\cdots\times G_n$ mit komponentenweiser Multiplikation eine Gruppe (ein Monoid) $(x_1,\dots,x_n)\cdot(y_1,\dots,y_n)=(x_1y_1,\dots,x_ny_n)$.

(f) Weitere Beispiele: $\mathbf{GL}_n(K)$, $\mathbf{SL}_n(K)$, $\mathbf{O}_n$, $\mathbf{SO}_n$, $\mathbf{U}_n$, $\mathbf{SU}_n$,...

(g) Abelsche Gruppen bis auf Isomorphie:

$$\begin{array}{rl} n=4 & \mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}2 \quad,\quad \mathbb{Z}/\mathbb{Z}4\\ n=6 & \mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}3\cong\mathbb{Z}/\mathbb{Z}6\\ n=8 & \mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}2 \quad,\quad \mathbb{Z}/\mathbb{Z}4\times\mathbb{Z}/\mathbb{Z}2 \quad,\quad \mathbb{Z}/\mathbb{Z}8\\ n=12 & \mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}3\cong\mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}6 \quad,\quad \mathbb{Z}/\mathbb{Z}4\times\mathbb{Z}/\mathbb{Z}3\cong\mathbb{Z}/\mathbb{Z}12 \end{array}$$

Beispiele für endlich erzeugte Gruppen:

(a) Die symmetrische Gruppe

$$G=\mathfrak{S}_3=\left\{e, a=\begin{pmatrix}123\\231\end{pmatrix}, a^2=\begin{pmatrix}123\\312\end{pmatrix}, b=\begin{pmatrix}123\\132\end{pmatrix}, c=\begin{pmatrix}123\\321\end{pmatrix}, d=\begin{pmatrix}123\\213\end{pmatrix}\right\}$$

mit den Relationen $a^3=e$, $a^{-1}=a^2$, $b^2=c^2=d^2=e$, $b^{-1}=b$, $c^{-1}=c$, $d^{-1}=d$, $ab=d$, $a^2b=c$.

$$\begin{aligned}\langle a\rangle &= \langle a^2\rangle=\{e,a,a^2\}\\ \langle b\rangle &= \{e,b\}\\ \langle c\rangle &= \{e,c\}\\ \langle d\rangle &= \{e,d\}\end{aligned}$$

ergibt

$$\begin{aligned}\mathrm{ord}(e) &= 1\\ \mathrm{ord}(a) &= 3\\ \mathrm{ord}(b)=\mathrm{ord}(c)=\mathrm{ord}(d) &= 2\end{aligned}$$

Also: $G=\{e,a,a^2,b,ab,a^2b\}$. Kommutatorrelation: $ba=c=a^2b$.

(b) Sei $n\geqslant 2$, $a=\begin{pmatrix}\cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n}\\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n}\end{pmatrix}$, $b=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ in $\mathbf{O}_2$. Es gilt

$$\begin{aligned}a^n &= e\\ a^i &= a^j \quad \text{für } 0\leqslant i<jn\\ b^2 &= e\end{aligned}$$

Relation: $ba=a^{n-1}b$
Untergruppen:

$$\begin{aligned}\langle a\rangle &= \{e,a,\dots a^{n-1}\} \quad \text{also } \mathrm{ord}(a)=n\\ \langle b\rangle &= \{e,b\} \quad \text{also } \mathrm{ord}(b)=2\\ D_n &= \{e,a,a^2\dots,a^{n-1},b,a^2b\dots,a^{n-1}b\} \quad \text{ist Gruppe der Ordnung } 2n\end{aligned}$$

Jede zu D_n isomorphe Gruppe heißt Diedergruppe der Ordnung $2n$.
Für $n = 2$:

$$D_2 = \{e, a, b, ab\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \cos\pi & -\sin\pi \\ \sin\pi & \cos\pi \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} \cos\pi & \sin\pi \\ \sin\pi & -\cos\pi \end{pmatrix} \right\}$$

ist abelsche Gruppe der Ordnung 4. Jede dazu isomorphe Gruppe heißt Kleinsche Vierergruppe.
Für $n = 3$:

$$D_3 \cong S_3.$$

(c) Sei $a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in $\mathbf{U}_2$. Dann

$$\begin{aligned} a^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ a^4 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e \\ a^3 &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = a^{-1} \\ b^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = a^2 \\ b^4 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e \\ b^3 &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = b^{-1} \end{aligned}$$

Relationen: $b^2 = a^2$, $ba = a^3 b$

$$Q = \langle a, b \rangle = \{e, a, a^2, a^3, b, ab, a^2 b, a^3 b\}$$

hat Ordnung 8 und heißt Quaternionengruppe.

(d) Jede Untergruppe von $(\mathbb{Z}, +)$ ist von der Gestalt $\mathbb{Z}n$ mit eindeutigem $n \in \mathbb{N}_0$.

Beispiele für Gruppenoperationen

(a) Sei $X \neq \emptyset$ eine Menge, $G \subset \mathfrak{S}_X$ eine Untergruppe. Dann ist

$$G \times X \to X, (\sigma, x) \mapsto \sigma(x)$$

eine Operation.
Speziell $X = \{1, 2, 3\}$, $G = S_3$. Dann ist $G.1 = G.2 = G.3 = X$, also ist die Operation transitiv. Sie ist fixpunktfrei.

$$\begin{aligned} G_1 &= \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} \\ G_2 &= \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} \\ G_3 &= \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \end{aligned}$$

(b) $X = \mathbb{R}^2$, $G = \mathbf{SO}_2 = \left\{ \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \mid 0 \leqslant \varphi < 2\pi \right\}$. Dann ist

$$\mathbf{SO}_2 \times \mathbb{R}^2 \to \mathbb{R}^2, (A, x) \mapsto Ax$$

eine Operation mit $G_0 = G$, $G_x = e$ für $x \neq 0$.

Beispiel Konjugation

$\mathfrak{S}_3 = \{e, a, a^2, b, ab, a^2b\}$ mit $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ und $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $ba = a^2b$.

Konjugationsklassen:

$$\begin{array}{rcll} C_e & = & \{e\} & \\ C_a & = & \{a, a^2\} & \text{denn } bab = a^2\text{; das sind die Elemente der Ordnung 3} \\ C_b & = & \{b, ab, a^2b\} & \text{denn } a^{-1}ba = ab,\ a^{-2}ba^2 = ba = a^2n\text{, dies sind die Elemente der Ordnung 2} \end{array}$$

Zentralisatoren: Diese sind Untergruppen von $\mathfrak{S}_3$, haben also Ordnung $1, 2, 3$ oder 6.

$$\begin{array}{rcll} C_{\mathfrak{S}_3}(e) & = & \mathfrak{S}_3 & \\ C_{\mathfrak{S}_3}(a) & = & \{e, a, a^2\} & \text{nicht-triviale echte Untergruppe, denn } a \text{ vertauscht mit sich selbst, aber nicht mit } b \\ & = & C_{\mathfrak{S}_3}(a^2) & \\ C_{\mathfrak{S}_3}(b) & = & \{e, b\} & \text{nicht-triviale echte Untergruppe, denn } b \text{ vertauscht mit sich selbst, aber nicht mit } a \\ C_{\mathfrak{S}_3}(ab) & = & \{e, ab\} & \text{nicht-triviale echte Untergruppe, denn } ab \text{ vertauscht mit sich selbst, aber nicht mit } a \\ C_{\mathfrak{S}_3}(a^b) & = & \{e, a, a^2\} & \text{nicht-triviale echte Untergruppe, denn } a^2b \text{ vertauscht mit sich selbst, aber nicht mit } a \end{array}$$

Zentrum: $Z(G) = \{e\}$.

Beispiele für Normalteilter

(a) Ist G abelsch, dann sind alle Untergruppen von G Normalteiler.

(b) Die Normalteiler von $\mathfrak{S}_3$ sind $\{e\}$, S_3, $\left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle$.

(c) Ist $H \subset G$ Untergruppe vom Index 2, dann ist $H \lhd G$: Für $x \in G \backslash H$ gilt $G = H \cup xH = H \cup Hx$ disjunkt, also $xH = Hx$, für $x \in H$ gilt $xH = H = Hx$.

(d) Die einfachen abelschen Gruppen sind bis auf Isomorphie genau die $\mathbb{Z}/\mathbb{Z}p$, p prim.

Konstruktion äußerer semidirekter Produkte

Sei $m, n \in \mathbb{N}\backslash\{1\}$, $r \in \mathbb{Z}$ mit $r^m \equiv 1 \mod n$, dh. $\operatorname{ord}_n(r) \big| m$. Dann ist

$$\rho : \mathbb{Z}/\mathbb{Z}n \to \mathbb{Z}/\mathbb{Z}n, \overline{z} \mapsto \overline{rz}$$

Homomorphismus mit $\rho^m = \mathrm{id}_{\mathbb{Z}/\mathbb{Z}n}$. Also ist $\rho \in \operatorname{Aut}(\mathbb{Z}/\mathbb{Z}n)$ und $\operatorname{ord}(\rho)\big|m$. Die Abbildung

$$\tau : \mathbb{Z}/\mathbb{Z}m \to \operatorname{Aut}(\mathbb{Z}/\mathbb{Z}n), \overline{y} \mapsto \rho^y$$

ist Gruppenhomomorphismus, explizit

$$\tau(\overline{y})(\overline{x}) = \rho^y(\overline{x}) = \overline{r}^y\overline{x}$$

für $\overline{y} \in \mathbb{Z}/\mathbb{Z}m$, $\overline{x} \in \mathbb{Z}/\mathbb{Z}n$. Sei

$$G = \mathbb{Z}/\mathbb{Z}n \times_\tau \mathbb{Z}/\mathbb{Z}m.$$

In G gilt

$$(\overline{x}, \overline{y})(\overline{x}', \overline{y}') = (\overline{x} + \overline{r}^y\overline{x}', \overline{y} + \overline{y}'),$$

neutrales Element ist $(0, 0)$, Inverses ist $(\overline{x}, \overline{y})^{-1} = (-\overline{r}^{-y}\overline{x}, -\overline{y})$. Seien $a = (\overline{1}, \overline{0})$, $b = (\overline{0}, \overline{1})$, dann ist $\operatorname{ord}(a) = n$ und $\operatorname{ord}(b) = m$, ferner $bab^{-1} = a^r$ (äquivalent dazu: $ba = a^rb$). Es folgt $G = \{a^ib^j \mid 0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant m-1\}$. Außerdem $\langle a \rangle \lhd G$, $G = \langle a \rangle\langle b \rangle = \langle b \rangle\langle a \rangle$, $\langle a \rangle \cap \langle b \rangle = \{e\}$. G ist genau dann abelsch, wenn $r \equiv 1 \mod n$, dh. wenn τ trivial ist. Spezialfall: $1 \neq n \in \mathbb{N}$, $m = 2$ und $r = -1$. Dann ist

$$\mathbb{Z}/\mathbb{Z}n \times_\tau \mathbb{Z}/\mathbb{Z}2 = \{e, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\} \text{ mit } \operatorname{ord}(a) = n, \operatorname{ord}(b) = 2, ba = a^{n-1}b$$

die bereits bekannte Diedergruppe der Ordnung $2n$.

Beispiele: Symmetrische Gruppe

(a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 1 & 6 \end{pmatrix} = (13425) \in \mathfrak{S}_6$

(b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 1 & 4 & 7 & 9 & 3 & 8 & 6 & 5 & 10 \end{pmatrix} = (12)(34786)(59)$

(c) Sei p prim, $\sigma = (a_1 \dots a_p)$ ein p-Zykel. Dann sind auch $\sigma^2, \dots, \sigma^{p-1}$ p-Zyklen, denn diese Elemente haben alle Ordnung p. Dagegen: für $\sigma = (1234)$ ist $\sigma^2 = (13)(24)$.

(d) Es gilt $|\mathfrak{S}_3| = 6$, $|A_3| = 3$. Man macht sich leicht klar, daß

$$\begin{aligned} \mathfrak{S}_3 &= \{\mathrm{id}, (123), (132), (12), (13), (23)\} \\ A_3 &= \{\mathrm{id}, (123), (132)\} \lhd \mathfrak{S}_3 \end{aligned}$$

Als nächstes betrechten wir die Gruppe $\mathfrak{S}_4$. Analog zu oben gilt $|\mathfrak{S}_4| = 24$, $|A_4| = 12$. Es ist nun bereits weit aufwendiger, die Gruppen auszurechenen:

$$\begin{aligned} \mathfrak{S}_4 &= \{\mathrm{id}, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), \\ &\quad (143), (234), (243), (1234), (1243), (1324), (1342), (1423), (1432)\} \\ A_4 &= \{\mathrm{id}, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\} \lhd \mathfrak{S}_4 \\ V &= \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd \mathfrak{S}_4 \quad \text{die Klein'sche Vierergruppe} \end{aligned}$$

Also ist A_4 semidirektes Produkt aus V und den Untergruppen der Ordnung 3.

Beispiele: Sylow-Sätze

(a) $G = \mathfrak{S}_3$. 2-Sylowuntergruppen: $\langle(12)\rangle$, $\langle(13)\rangle$, $\langle(23)\rangle$. 3-Sylowuntergruppe: $\langle(123)\rangle$.

(b) Die Sylowuntergruppen einer endlichen abelschen Gruppe sind genau die p-Komponenten.

(c) Eine Gruppe der Ordnung 6 ist isomorph zu $\mathbb{Z}/6\mathbb{Z}$ oder zu $D_3 \cong \mathfrak{S}_3$.

(d) Die Sylowuntergruppen von $\mathfrak{S}_4$:
   (i) $p = 2$: $\mathfrak{S}_4$ enthält eine Diedergruppe der Ordnung 8, diese ist 2-Sylowuntergruppe. Also sind die 2-Sylowuntergruppen von $\mathfrak{S}_4$ genau die Diedergruppen der Ordnung 8, die in $\mathfrak{S}_4$ enthalten sind. Für deren Anzahl s_2 gilt, $s_2 \big| 3$ und $s_2 \equiv 1 \mod 2$. Also $s_2 \in \{1, 3\}$. Da $\mathfrak{S}_4$ mehr als 8 Elemente enthält, deren Ordnung 2-Potenz ist, folgt $s_2 = 3$.
   V ist in jeder 2-Sylowuntergruppe enthalten, offenbar ist dann $V = O_s(\mathfrak{S}_4)$.

   (ii) $p = 3$: Die 3-Sylowuntergruppen von $\mathfrak{S}_4$ sind genau die Untergruppen der Ordnung 3. Für deren Anzahl gilt $s_3 = 4$.

(e) Die Sylowuntergruppen von A_4:
   (i) $p = 2$: V.
   (ii) $p = 3$: Wie in $\mathfrak{S}_4$.

Beispiele: nilpotente und auflösbare Gruppen

(a) Endliche abelsche Gruppen sind nilpotent.

(b) $\mathfrak{S}_3$ ist nicht nilpotent.

(c) Allgemein gilt: D_n ist genau dann nilpotent, wenn n Potenz von 2 ist.

(d) Abelsche Gruppen, endliche p-Gruppen und endliche nilpotente Gruppen sind auflösbar.

(e) $\mathfrak{S}_3$ und $\mathfrak{S}_4$ sind auflösbar mit den Normalreihen mit abelschen Faktoren

$$\mathfrak{S}_3 \supset A_3 \supset \{e\} \quad \text{und} \quad \mathfrak{S}_4 \supset A_4 \supset V \supset \{e\}$$

aber nicht nilpotent.

(f) D_n, $n \geqslant 2$, ist auflösbar, denn jede solche Gruppe hat einen zyklischen Normalteiler vom Index 2.

(g) Endliche, einfache nicht-abelsche Gruppen sind nicht auflösbar. Insbesondere sind die Gruppen A_n für $n \geqslant 5$ nicht auflösbar. Damit sind auch die $\mathfrak{S}_n$ für $n \geqslant 5$ nicht auflösbar.

(h) Sind $p \neq q$ Primzahlen, $a, b \in \mathbb{N}$. Dann ist jede Gruppe der Ordnung $p^a q^b$ auflösbar (Burnside).

(i) Jede Gruppe ungerader Ordnung ist auflösbar (Feit, Thompson).