9. GRUNDBEGRIFFE DER GRUPPENTHEORIE

Eine Gruppe ist ein Modell der Gruppenaxiome GT, also eine $\mathscr{L}_{\mathsf{GT}}$-Struktur mit Bereich G, wobei $\mathscr{L}_{\mathsf{GT}} = \{\mathsf{e}, \circ\}$. Wie üblich identifizieren wir eine Gruppe $(G, e, \circ)$ mit ihrem Bereich G, oder wir schreiben $(G, \circ)$, um auch die binäre Operation $\circ$ hervorzuheben. Wenn wir keine Operation explizit definiert, betrachten wir die Gruppe als *multiplikative Gruppe*, wobei wir den Multiplikationspunkt "$\cdot$" meist weglassen. Bevor wir die Struktur von Gruppen untersuchen, beweisen wir ein paar unmittelbare Folgerungen aus den Axiomen.

EINFACHE FOLGERUNGEN AUS DEN GRUPPENAXIOMEN

PROPOSITION 9.1. *Sei G eine Gruppe mit Links-Neutralelement e. Dann gilt:*

(a) Links-Inverse Elemente sind auch rechtsinvers.

(b) e ist auch Rechts-Neutralelement.

(c) G hat genau ein Neutralelement (links und rechts).

(d) Jedes Element aus G hat genau ein Inverses (links und rechts).

Beweis. (a) Sei $a \in G$ beliebig und sei $\bar{\bar{a}}$ ein Links-Inverses von $\bar{a}$, wobei $\bar{a}$ ein Links-Inverses von a ist. Es gilt:

$$a\bar{a} \underset{\substack{\uparrow \\ e \text{ linksneutral}}}{=} e(a\bar{a}) = (\bar{\bar{a}}\bar{a})(a\bar{a}) \underset{\substack{\uparrow \\ \text{mit Assoziativität}}}{=} \bar{\bar{a}}(\bar{a}a)\bar{a} \underset{\substack{\uparrow \\ \bar{a}a = e}}{=} \bar{\bar{a}}(e\bar{a}) \underset{\substack{\uparrow \\ e\bar{a}=\bar{a}}}{=} \bar{\bar{a}}\bar{a} = e\,.$$

Somit ist $a\bar{a} = \bar{a}a = e$, was zeigt, dass das Links-Inverse $\bar{a}$ von a auch rechtsinvers ist. Weil jedes Element $a \in G$ mit GT_2 ein Links-Inverses hat, hat a auch ein Rechts-Inverses. Das Element $\bar{a}$ ist also ein *Inverses* von a.

(b) Es gilt

$$ae = a(\bar{a}a) \underset{\substack{\uparrow \\ \text{mit Assoziativität}}}{=} (a\bar{a})a \underset{\substack{\uparrow \\ \text{mit (a)}}}{=} ea \underset{\substack{\uparrow \\ e \text{ linksneutral}}}{=} a$$

Weil $a \in G$ beliebig war, ist e auch ein Rechts-Neutralelement. Das Element e ist also ein *Neutralelement* von G.

(c) Seien $e, \tilde{e} \in G$ Neutralelemente von G. Somit gilt für alle $x \in G$, $x\tilde{e} = ex = x$. Insbesondere gilt:

$$e \underset{\substack{\uparrow \\ \tilde{e} \text{ neutral}}}{=} e\tilde{e} \underset{\substack{\uparrow \\ e \text{ neutral}}}{=} \tilde{e}$$

Somit ist $e = \tilde{e}$ und es gibt genau ein Neutralelement in G.

(d) Sei $a \in G$ beliebig und seien $x, \tilde{x} \in G$ so, dass $xa = \tilde{x}a = e$, wobei $e \in G$ das Neutralelement von G ist. Mit (a) gilt $xa = ax = e$ und wir erhalten:

$$\tilde{x} \underset{\substack{\uparrow \\ e \text{ neutral}}}{=} \tilde{x}e = \tilde{x}(ax) \underset{\substack{\uparrow \\ \text{mit Assoziativität}}}{=} (\tilde{x}a)x = ex \underset{\substack{\uparrow \\ e \text{ neutral}}}{=} x$$

Somit ist $\tilde{x} = x$ und a hat genau ein Inverses in G. Weil a beliebig war, hat jedes Element aus G genau ein Inverses. ⊣

Ist die Operation $\circ$ einer Gruppe kommutativ, so heisst die Gruppe **abelsch**.

FAKTUM 9.2. *Sei G eine Gruppe mit Neutralelement e. Ist $aa = e$ für alle Elemente $a \in G$, so ist G abelsch.*

Beweis. Seien $a, b \in G$ beliebig. Aus

$$(ba)(ab) = beb = bb = e$$

folgt $(ba) = (ab)^{-1}$, wobei $(ab)^{-1}$ das Inverse von ab ist.

Andererseit gilt nach Voraussetzung $(ab)(ab) = e$. Somit ist $(ab) = (ab)^{-1}$ und aus der Eindeutigkeit des Inversen folgt $ba = ab$. Weil a, b beliebig waren ist G abelsch. ⊣

UNTERGRUPPEN

Sei G eine Gruppe. Eine nicht-leere Menge $H \subseteq G$ ist eine **Untergruppe** von G, falls für alle $x, y \in H$ gilt $x\,y^{-1} \in H$.

Ist H eine Untergruppe von G, dann schreiben wir $H \leqslant G$.

PROPOSITION 9.3. *Ist $H \leqslant G$, dann ist H eine Gruppe.*

Beweis. Wir müssen zeigen, dass H die Axiome GT erfüllt.

- GT_1: Sei $x \in H$. Dann ist, nach Definition, $xx^{-1} = e \in H$, und somit ist das Neutralelement e von G in H.
- GT_2: Sei $x \in H$. Dann ist, nach Definition, $ex^{-1} = x^{-1} \in H$.
- GT_0: Seien $x, y \in H$. Dann ist auch $y^{-1} \in H$, und nach Definition ist $x(y^{-1})^{-1} = xy \in H$. Damit ist H abgeschlossen unter der assoziativen Operation auf G. ⊣

Ist G eine Gruppe, so sind $\{e\}$ und G die sogenannten **trivialen Untergruppen** von G.

PROPOSITION 9.4. *Der Durchschnitt beliebig vieler Untergruppen einer Gruppe G ist wieder eine Untergruppe von G.*

Beweis. Sei Λ irgend eine Menge und für jedes $\lambda \in \Lambda$ sei $H_\lambda \leqslant G$. Sei

$$H_0 = \bigcap_{\lambda \in \Lambda} H_\lambda$$

und seien $x, y \in H_0$ beliebig. Dann sind x, y in allen H_λ, und mit $H_\lambda \leqslant G$ gilt für jedes $\lambda \in \Lambda$, $x\,y^{-1} \in H_\lambda$. Somit sind $x\,y^{-1} \in H_0$. Weil $x, y \in H_0$ beliebig waren ist $H_0 \leqslant G$. ⊣

Sei G eine Gruppe. Die Kardinalität $|G|$ der Menge G ist die **Ordnung** der Gruppe G. Sei e das Neutralelement von G und sei $x \in G$. Die kleinste positive Zahl $n \in \mathbb{N}$, sodass $x^n = e$ (sofern sie existiert), ist die **Ordnung von x**, bezeichnet mit $\mathrm{ord}(x)$ – wobei wir die Notation

$$x^n := \underbrace{x \cdot \ldots \cdot x}_{n\text{-mal}}$$

benutzen. Falls es keine solche Zahl gibt, sei $\mathrm{ord}(x) := \infty$, denn für alle $n \in \mathbb{N}$ gilt $x^n \neq e$.

Die Ordnung eines Elements $x \in G$ einer endlichen Gruppe G ist immer endlich: Weil die Menge $\{x^1, x^2, x^3, \ldots\} \subseteq G$ endlich ist, existieren $0 < n < m$ mit $x^n = x^m = x^n\,x^{m-n}$ und es folgt $e = x^{m-n}$ mit $m - n > 0$.

Ist $\mathrm{ord}(x) = n$, so ist $|\{x^1, \ldots, x^n\}| = n$, denn sonst finden wir $1 \leq k < l \leq n$ mit $x^k = x^l$, also $x^{l-k} = e$ mit $l - k < n$.

Sei $x \in G$ mit $\mathrm{ord}(x) = n$. Setzen wir $x^0 := e$, so ist $\{x^k : k \in n\}$ eine Untergruppe von G, denn für $l_1, l_2 \in n$ ist $x^{l_1} \cdot x^{l_2} = x^{l_1+l_2} = x^k$ für ein $k \in n$ und $x^l \cdot x^{n-l} = e$. Zudem ist $\{x^k : k \in n\}$ die kleinste Untergruppe $H \leqslant G$, die x enthält. Denn mit $x \in H$ ist auch jede Potenz von x in H. Somit enthält jede Untergruppe $H \leqslant G$ die x enthält immer auch die Gruppe $\{x^k : k \in n\}$.

Für eine Gruppe G und eine Menge $X \subseteq G$ sei die von X **erzeugte Untergruppe** definiert als

$$\langle X \rangle := \bigcap_{\substack{H \leqslant G \\ X \subseteq H}} H \,.$$

Aus Proposition 9.4 folgt, dass $\langle X \rangle$ eine Untergruppe von G ist. Diese Untergruppe ist die kleinste Gruppe, welche durch X **erzeugt** (oder **generiert**) wird. Ist $X = \{x\}$, dann schreiben wir $\langle x \rangle$ anstelle von $\langle \{x\} \rangle$ und nennen x einen **Generator** der Gruppe $\langle x \rangle$.

Für $x \in G$ ist $\langle x \rangle$ die kleinste Untergruppe von G die x enthält. Ist also $x \in G$ mit $\operatorname{ord}(x) = n$, so gilt $\langle x \rangle = \{x^k : k \in n\}$.

Zyklische Gruppen

Eine endliche Gruppe G mit $|G| = n$ ist **zyklisch**, wenn ein Element $g \in G$ existiert, sodass $G = \{g^k : k \in n\}$, insbesondere gilt $G = \langle g \rangle$ und g ist ein **Generator** der Gruppe G. Das folgende Faktum ist eine Umformulierung der Definition.

Faktum 9.5. *Eine endliche Gruppe G ist genau dann zyklisch, wenn in G ein Element g existiert mit* $\operatorname{ord}(g) = |G|$.

Beachte, dass aus $x^n \cdot x^m = x^{n+m} = x^m \cdot x^n$ (für alle $n, m \in \mathbb{N}$) folgt, dass zyklische Gruppen immer abelsch sind.

Faktum 9.6. *Ist G eine Gruppe und $x \in G$ mit $\operatorname{ord}(x) = n$, dann ist $\langle x \rangle$ eine zyklische Gruppe der Ordnung n, d. h. $|\langle x \rangle| = n$.*

Beweis. Die Gruppe $\langle x \rangle$ besteht aus den Elementen $x^1, x^2, \ldots, x^n$, wobei $x^n = e$. Andererseits ist $\{x^1, x^2, \ldots, x^n\}$ eine zyklische Gruppe der Ordnung n. ⊣

Als unmittelbare Folgerung erhalten wir:

Korollar 9.7. *Sei G eine Gruppe. Ist $x \in G$ ein Element von endlicher Ordnung, dann ist $\langle x \rangle \leqslant G$ und* $\operatorname{ord}(x) = |\langle x \rangle|$.

Produkte von Gruppen

Proposition 9.8. *Seien $(G, \circ, e_G)$ und $(H, \bullet, e_H)$ zwei beliebige Gruppen. Dann ist*

$$\big(G \times H, *, \langle e_G, e_H \rangle\big)$$

mit

$$\langle g_1, h_1 \rangle * \langle g_2, h_2 \rangle := \langle g_1 \circ g_2, h_1 \bullet h_2 \rangle$$

eine Gruppe.

Beweis. Da die Verknüpfung $*$ komponentenweise definiert ist, ist $*$ eine Operation auf $G \times H$ Da die Operationen $\circ$ und $\bullet$ assoziativ sind, ist auch die Operation $*$ assoziativ. Weiter ist $\langle e_G, e_H \rangle$ das Neutralelement und $\langle g^{-1}, h^{-1} \rangle$ ist das Inverse von $\langle g, h \rangle$. ⊣

Zwei Gruppen $(G_0, \circ)$ und $(G_1, \bullet)$ sind **isomorph**, bezeichnet mit $G_0 \cong G_1$, falls eine Bijektion $\alpha : G \to H$ existiert, sodass für alle $x, y \in G$ gilt: $\alpha(x \circ y) = \alpha(x) \bullet \alpha(y)$. Beachte, dass bei einem Isomorphismus $\alpha : G_0 \to G_1$, das Neutralelemt von G_0 auf das Neutralelement von G_1 abgebildet wird, und das Inverse von x auf das Inverse von $\alpha(x)$ abgebildet wird, d. h. $\alpha(x^{-1}) = \alpha(x)^{-1}$.

FAKTUM 9.9. *$G \times \{e_H\} \leqslant G \times H$ und $G \cong G \times \{e_H\}$.*

Beweis. Da $\{e\}$ eine Untergruppe von H ist, ist $G \times \{e_H\}$ eine Untergruppe von $G \times H$. Die Einbettung $\alpha\colon G \to G \times \{e_H\}$ mit $x \mapsto \alpha(x) := \langle x, e_H\rangle$ ist ein Isomorphismus. ⊣

NEBENKLASSEN

Für $H \leqslant G$ und $x \in G$ seien

$$xH := \{xh : h \in H\} \quad \text{und} \quad Hx := \{hx : h \in H\}\,.$$

Die Mengen $xH, Hx \subseteq G$ heissen **Linksnebenklassen** bzw. **Rechtsnebenklassen** von H in G.

Das folgende Lemma ist eine Zusammenfassung der wichtigsten Eigenschaften von Nebenklassen:

LEMMA 9.10 (links-Version). *Sei G eine Gruppe, $H \leqslant G$ und seien $x, y \in G$ beliebig.*

(a) $|xH| = |H|$, *d. h. es existiert eine Bijektion zwischen H und xH.*
(b) $x \in xH$.
(c) $xH = H$ *genau dann, wenn* $x \in H$.
(d) $xH = yH$ *genau dann, wenn* $x^{-1}y \in H$.
(e) $xH = \{g \in G : gH = xH\}$.

Beweis. (a) Definiere die Abbildung $\varphi_x : H \to xH$ durch $\varphi_x(h) := xh$. Wir müssen zeigen, dass φ_x eine Bijektion ist: Ist $\varphi_x(h_1) = \varphi_x(h_2)$ für $h_1, h_2 \in H$, d. h. $xh_1 = xh_2$, dann ist $xh_1{h_2}^{-1} = xh_2{h_2}^{-1} = xe = x$, woraus $h_1{h_2}^{-1} = e$ folgt, also $h_1 = h_2$. Somit ist die Abbildung φ_x injektiv.

Andererseits ist jedes Element in xH von der Form xh (für ein $h \in H$), und weil gilt $xh = \varphi_x(h)$, ist die Abbildung φ_x auch surjektiv. Somit ist φ_x eine Bijektion zwischen H und xH.

(b) Weil $e \in H$, ist $xe = x \in xH$.

(c) Ist $xH = H$, dann gilt, weil $e \in H$, $xe = x \in H$. Für die andere Richtung nehmen wir an $x \in H$ (also auch $x^{-1} \in H$): Weil H eine Gruppe ist, haben wir $xH \subseteq H$.

Sei nun $h \in H$ irgend ein Element aus H. Weil $x^{-1} \in H$, ist $x^{-1}h \in H$ und somit gilt $xH \ni x(x^{-1}h) = h$. Weil $h \in H$ beliebig war, erhalten wir $xH \supseteq H$. Damit gilt $xH \subseteq H \subseteq xH$, woraus die Gleichheit $xH = H$ folgt.

(d) Ist $xH = yH$, dann gilt

$$H = eH = (x^{-1}x)H = x^{-1}(xH) = x^{-1}(yH) = (x^{-1}y)H \overset{\text{mit (c)}}{\Longrightarrow} x^{-1}y \in H\,.$$

Ist $x^{-1}y \in H$, dann folgt aus (c), dass gilt $(x^{-1}y)H = H$, und somit ist

$$xH = x(x^{-1}y)H = (xx^{-1})yH = yH.$$

(e) Ist $g \in xH$, dann ist $g = xh$ für ein $h \in H$. Somit ist $gH = xhH = xH$, woraus folgt, dass gilt $xH \subseteq \{g \in G : gH = xH\}$.

Gilt umgekehrt $xH = gH$ für ein $g \in G$, dann folgt aus (b), $g \in xH$. Somit haben wir $\{g \in G : gH = xH\} \subseteq xH$, womit auch (e) bewiesen ist. ⊣

Es gibt natürlich auch eine rechts-Version von Lemma 9.10, welche analog bewisen wird. Als Folgerung aus Lemma 9.10.(b), sowie dessen rechts-Version, erhalten wir:

KOROLLAR 9.11. *Sei $H \leqslant G$, dann gilt*

$$\bigcup_{x \in G} xH = G = \bigcup_{x \in G} Hx\,.$$

Das folgende Lemma ist eine Folgerung aus Lemma 9.10 (e):

LEMMA 9.12 (links-Version). *Sei $H \leqslant G$. Dann gilt für alle $x, y \in G$ entweder $xH = yH$ oder $xH \cap yH = \emptyset$.*

Beweis. Entweder ist $xH \cap yH = \emptyset$ (und wir sind fertig), oder es gibt ein $z \in xH \cap yH$. Es gilt nun:

$$\left.\begin{array}{l} z \in xH \overset{\text{mit (e)}}{\Rightarrow} zH = xH \\ z \in yH \overset{\text{mit (e)}}{\Rightarrow} zH = yH \end{array}\right\} \Rightarrow xH = yH$$

⊣

Auch für dieses Lemma gibt es analog wieder eine Version für Rechtsnebenklassen.

Sei G eine Gruppe und $H \leqslant G$ eine Untergruppe. Dann definieren wir

$$G/H := \{xH : x \in G\} \quad \text{und} \quad H\backslash G := \{Hx : x \in G\}\,.$$

Eine **Partition** einer Menge S ist eine Menge von paarweise disjunkten nicht-leeren Teilmengen von S, sodass die Vereinigung dieser Mengen S ist.

Als eine unmittelbare Folgerung von Lemma 9.10.(a), Korollar 9.11 und Lemma 9.12 (links- und rechts-Versions) erhalten wir:

KOROLLAR 9.13. *Sei $H \leqslant G$, dann ist sowohl G/H wie auch $H\backslash G$ eine Partition von G, wobei jeder Teil dieser Partitionen dieselbe Kardinalität hat wie H.*

Sei $H \leqslant G$. Dann ist $|G/H| = |H\backslash G|$ der **Index** von H in G, bezeichnet mit $[G : H]$.

Als Folgerung aus Korollar 9.13 erhalten wir:

KOROLLAR 9.14. *Sei G eine Gruppe und sei $H \leqslant G$ eine Untergruppe von G. Ist $[G : H] = 2$, dann gilt für alle $x \in G$, $xH = Hx$.*

Beweis. Ist $x \in H$, dann gilt, weil H eine Gruppe ist, $xH = Hx = H$. Sei nun $x \in G$ mit $x \notin H$. Mit Korollar 9.13 haben wir $G = H \cup xH$ und $G = H \cup Hx$, wobei $H \cap xH = \emptyset = H \cap Hx$, woraus die Gleichheit $xH = Hx$ folgt. ⊣

Ist $H \leqslant G$ und gilt $xH = H = Hx$ für alle $x \in G$, so ist $H = xHx^{-1}$ für alle $x \in G$. Untergruppen $H \leqslant G$, für die gilt $H = xHx^{-1}$ für alle $x \in G$, heissen **Normalteiler** von G, bezeichnet mit $H \trianglelefteq G$. Jede Gruppe G besitzt die trivialen Normalteiler $\{e\}$ und G. Mit Korollar 9.14 ist aber auch jede Untergruppe $H \leqslant G$ mit Index 2 ein Normalteiler von G, und ist G eine abelsche Gruppe, so ist jede Untergruppe $H \leqslant G$ ein Normalteiler von G, denn für alle $x \in G$ gilt $xH = Hx$.

DER SATZ VON LAGRANGE

Der folgende Satz spielt eine wichtige Rolle, um die Struktur von endlichen Gruppen zu untersuchen.

SATZ VON LAGRANGE. *Sei G eine (endliche oder unendliche) Gruppe und sei $H \leqslant G$ eine Untergruppe von G. Dann gilt*

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

Insbesondere gilt für endliche Gruppen G, dass die Ordnung von H die Ordnung von G teilt.

Beweis. Betrachte die Partition G/H von G. Diese Partition hat $[G : H]$ Teile und jeder Teil hat $|H|$ Elemente (mit Lemma 9.10.(a)). Somit gilt $|G| = [G : H] \cdot |H|$. Ist nun G eine endliche Gruppe, d. h. $|G| = n$ für ein positives $n \in \mathbb{N}$, so ist $|H| \cdot [G : H] = n$, woraus folgt, dass $|H|$ ein Teiler von n ist. ⊣

Als Folgerung aus dem Satz von Lagrange erhalten wir:

KOROLLAR 9.15. *Ist G eine endliche Gruppe, dann gilt für alle $x \in G$,*

$$x^{|G|} = e.$$

Beweis. Für jedes $x \in G$ ist $\langle x \rangle$ eine endliche Untergruppe von G. Mit dem Satz von Lagrange gilt nun, dass $|\langle x \rangle|$ die Gruppenordnung $|G|$ teilt. Weil nun $|\langle x \rangle| = \operatorname{ord}(x)$, existiert ein $k \in \mathbb{N}$ mit $\operatorname{ord}(x) \cdot k = |G|$. Somit ist, weil $x^{\operatorname{ord}(x)} = e$,

$$x^{|G|} = x^{\operatorname{ord}(x) \cdot k} = \left(x^{\operatorname{ord}(x)}\right)^k = e^k = e.$$

⊣

BEMERKUNGEN ZU NORMALTEILERN*

Sei $N \trianglelefteq G$ ein Normalteiler der Gruppe G, d. h. N ist eine Untergruppe von G und für alle $x \in G$ gilt $xN = Nx$ bzw. $xNx^{-1} = N$. Dann können wir auf der Menge G/N der Linksnebenklassen von N eine Gruppenstruktur wie folgt definieren: Für $x, y \in G/N$ ist

$$(xN)(yN) = x(\underbrace{yNy^{-1}}_{=N})(yN) = (xy)N(yy^{-1})N = (xy)N(\underbrace{eN}_{=N}) = (xy)(\underbrace{NN}_{=N}) = (xy)N$$

und wir definieren die Gruppenoperation auf G/N durch

$$(xN)(yN) := (xy)N.$$

Wir müssen nun natürlich zeigen, dass diese Operation wohldefiniert ist und dass G/N mit dieser Operation tatsächlich eine Gruppe ist, nämlich die sogenannte **Faktorgruppe** von G nach N.

Beachte, dass aus $K \trianglelefteq N \trianglelefteq G$ im Allgemeinen nicht folgt, dass K ein Normalteiler von G ist. Andererseits folgt aber zum Beispiel aus $K \leqslant H \leqslant G$ und $K \trianglelefteq G$, dass K ein Normalteiler von H ist.

*gehört nicht zum Vorlesungsstoff