

Gruppen

Sei G eine nichtleere Menge, sei $\cdot$ eine binäre Operation, i eine unäre Operation auf G , und sei $1 \in G$. Die algebraische Struktur $(G, \cdot, i, 1)$ ist eine *Gruppe* wenn für alle $x, y, z \in G$ gilt:

- (a) (Assoziativität) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;
- (b) (neutrales Element) $1 \cdot x = x$;
- (c) (Invertierbarkeit) $i(x) \cdot x = 1$.

Auf jeder Menge Ω bildet die Menge aller bijektiven Funktionen,

$$\text{Sym}(\Omega) := \{f : \Omega \rightarrow \Omega \mid f \text{ ist bijektiv}\},$$

eine Gruppe bezüglich der Komposition von Funktionen. $(\text{Sym}(\Omega), \circ, {}^{-1}, \text{id}_\Omega)$ heißt die *symmetrische Gruppe* auf Ω .

In jeder Gruppe existiert ein linksneutrales Element und zu jedem Element ein linksinverses. Aus den Gruppenaxiomen kann man auch die Existenz eines rechtsneutralen und rechtsinversen Elements folgern.

Lemma 1. *Sei $(G, \cdot, i, 1)$ eine Gruppe. Für alle $x, y \in G$ gilt:*

- (a) $x \cdot 1 = x$;
- (b) $i(1) = 1$;
- (c) $i(i(x)) = x$;
- (d) $x \cdot i(x) = 1$;
- (e) $i(x \cdot y) = i(y) \cdot i(x)$.

Falls $(G, \cdot, i, 1)$ eine Gruppe ist, dann sind die Operationen i und 1 durch die Multiplikation $\cdot$ bereits eindeutig bestimmt.

Eine Teilmenge H von G heißt *Untergruppe* der Gruppe $(G, \cdot, i, 1)$, geschrieben $H \leq G$, falls H unter $\cdot$ und i abgeschlossen ist und falls $1 \in H$.

Sei H eine Untergruppe von $(G, \cdot)$. Für $x \in G$ sei $xH := \{xh \mid h \in H\}$. Die Zahl der *Linksnebenklassen* $\{xH \mid x \in G\}$ von H in G heißt der *Index* von H in G , geschrieben $|G : H|$.

Satz 2 (Lagrange). *Sei G eine endliche Gruppe, sei $H \leq G$. Dann gilt $|G| = |H| \cdot |G : H|$. Insbesondere sind Ordnung und Index einer Untergruppe Teiler der Gruppenordnung.*

Die *Ordnung* eines Gruppenelementes g , $\text{ord}(g)$, ist die Ordnung der von g erzeugten zyklischen Untergruppe $\langle g \rangle$.

Satz 3 (Fermat). *Sei G eine endliche Gruppe, sei $g \in G$. Dann ist $\text{ord}(g)$ ein Teiler von $|G|$ und $g^{|G|} = 1_G$.*

Seien $(G, \cdot_G, i_G, 1_G)$ und $(H, \cdot_H, i_H, 1_H)$ Gruppen. Eine Abbildung $\varphi : G \rightarrow H$ heißt *Homomorphismus* wenn für alle $x, y \in G$ gilt:

- (a) $\varphi(x \cdot_G y) = \varphi(x) \cdot_H \varphi(y)$;
- (b) $\varphi(i_G(x)) = i_H(\varphi(x))$;
- (c) $\varphi(1_G) = 1_H$.

Erfüllt eine Funktion die Bedingung (a) (Multiplikativität) dann auch (b) und (c). Die Menge aller Homomorphismen von G nach H bezeichnen wir mit $\text{Hom}(G, H)$. Den *Kern* von $\varphi \in \text{Hom}(G, H)$ definieren wir als $\text{Ker}(\varphi) := \{g \in G \mid \varphi(g) = 1_H\}$ und das *Image* von φ als $\text{Im}(\varphi) := \{\varphi(g) \mid g \in G\}$. Es gilt $\text{Ker}(\varphi) \leq G$ und $\text{Im}(\varphi) \leq H$.

Homomorphiesatz. $G/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$.

Gruppenoperationen

Sei $(G, \cdot)$ eine Gruppe, Ω eine Menge, und sei $*$: $G \times \Omega \rightarrow \Omega$ eine Verknüpfung, sodass für alle $g, h \in G, \omega \in \Omega$ die folgenden Eigenschaften erfüllt sind:

- (a) $1 * \omega = \omega$,
- (b) $(g \cdot h) * \omega = g * (h * \omega)$.

Dann heißt $*$ *Gruppenoperation* von G auf Ω ; wir sagen G *operiert* auf Ω .

Sei $*$ eine Gruppenoperation von G auf Ω , sei $\omega \in \Omega$. Dann heißt $G * \omega := \{g * \omega \mid g \in G\}$ *Orbit* von $\omega \in \Omega$ unter G . Es gilt $\Omega = \bigcup \{G * \omega \mid \omega \in \Omega\}$. Wir nennen $G_\omega := \{g \in G \mid g * \omega = \omega\}$ den *Stabilisator* von ω in G . Man sieht leicht, dass G_ω eine Untergruppe von G ist.

Wir betrachten einige Beispiele für Operationen von Gruppen auf Mengen:

- (a) Permutationsgruppen: Sei Ω eine Menge, und sei G eine Untergruppe der symmetrischen Gruppe $\text{Sym}(\Omega) := \{f : \Omega \rightarrow \Omega \mid f \text{ ist bijektiv}\}$.

Dann operiert G auf Ω durch $g * \omega := g(\omega)$ für $g \in G, \omega \in \Omega$.

- (b) Lineare Gruppen: Sei G eine Untergruppe von $\text{GL}(n, K)$ für $n \in \mathbb{N}$ und einen Körper K . Dann operiert G auf dem Vektorraum K^n durch Multiplikation $g * v := gv$ für $g \in G, v \in K^n$.

- (c) Eine Gruppe $(G, \cdot)$ operiert auf der Menge G durch Konjugation: $g * x := gxg^{-1}$ für $g, x \in G$.

Traditionellerweise schreibt man für $g^{-1}xg$ kurz x^g . Damit gilt $gxg^{-1} = x^{(g^{-1})}$. Die Abbildung $*' : G \times G \rightarrow G, (g, x) \mapsto x^g$, ist aber nach unserer Definition keine Gruppenoperation.

- (d) Sei H eine Untergruppe von $(G, \cdot)$. Dann operiert G auf der Menge der Linksnebenklassen $\{xH \mid x \in G\}$ von H in G durch $g * xH := gxH$ für $g, x \in G$.

Satz 4. Sei $*$ eine Gruppenoperation von G auf Ω .

- (a) Für $g \in G$ sei $g_\Omega : \Omega \rightarrow \Omega, \omega \mapsto g * \omega$. Dann ist $h : G \rightarrow \text{Sym}(\Omega), g \mapsto g_\Omega$, ein Homomorphismus.
- (b) Sei G endlich. Dann gilt $|G * \omega| \cdot |G_\omega| = |G|$ für alle $\omega \in \Omega$.

Der nächste Satz wird oft fälschlicherweise Burnside zugeschrieben.

Satz 5. Sei $*$ eine Gruppenoperation einer endlichen Gruppe G auf einer endliche Menge Ω . Sei n die Anzahl der Orbits von G auf Ω . Dann gilt

$$n = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|,$$

wobei $\text{Fix}(g) = \{\omega \in \Omega \mid g * \omega = \omega\}$.

Einen Homomorphismus von G in eine Permutationsgruppe nennt man *Permutationsdarstellung* von G . Nach dem nächsten Satz ist jede Gruppe zu einer Permutationsgruppe isomorph.

Satz 6 (Cayley). *Jede Gruppe G ist in $\text{Sym}(G)$ einbettbar.*

Die Beweise folgender Sätze lassen sich ebenfalls mittels geeigneter Gruppenoperationen führen.

Satz 7. *Sei G eine endliche Gruppe mit $|G| = n$, und sei K ein Körper. Dann ist G in $\text{GL}(n, K)$ einbettbar.*

Wir lassen im Folgenden die Gruppe $(G, \cdot)$ auf sich selbst durch Konjugation operieren, das heißt, $g * x := gxg^{-1}$ für $g \in G, x \in G$. Das Orbit $\{x^g \mid g \in G\}$ von x unter dieser Operation heißt *Konjugiertheitsklasse* von x in G . Der Stabilisator von x in G ist durch $C_G(x) := \{g \in G \mid x^g = x\}$ gegeben und heißt *Zentralisator* von x in G . Zwei Elemente $x, y \in G$ heißen *konjugiert* in G , wenn $g \in G$ existiert, sodass $x^g = y$.

Lemma 8. *Sei G eine endliche Gruppe, sei $x \in G$. Die Anzahl der Elemente der Konjugiertheitsklasse von x in G ist $|G : C_G(x)|$.*

Sei G endlich, und sei k die Anzahl der Konjugiertheitsklassen von G , genannt *Klassenzahl*. Seien $n_1, \dots, n_k$ die Anzahlen der Elemente in den Konjugiertheitsklassen. Es gilt die *Klassengleichung*

$$|G| = n_1 + \dots + n_k.$$

Wir nennen $Z(G) := \{x \in G \mid x^g = x \text{ für alle } g \in G\}$ das *Zentrum* von G . Dann ist $Z(G)$ die Vereinigung aller einelementigen Konjugiertheitsklassen von G .

Eine endliche Gruppe, deren Ordnung eine Potenz einer Primzahl p ist, heißt *p-Gruppe*. Mithilfe der Klassengleichung erhält man folgenden wichtigen Satz.

Satz 9. *Sei G eine endliche p-Gruppe mit $G \neq 1$. Dann ist $Z(G) \neq 1$.*

Sei G eine endliche Gruppe, sei p eine Primzahl, und sei $a \in \mathbb{N}_0$ maximal, sodass p^a die Ordnung von G teilt. Eine Untergruppe von G mit Ordnung p^a heißt *Sylow p-Untergruppe*.

Satz 10 (Sylow). *Sei G eine endliche Gruppe, und sei p eine Primzahl. Dann gilt:*

- (a) *Jede p-Untergruppe von G ist in einer Sylow p-Untergruppe von G enthalten. (Insbesondere: Sylow p-Untergruppen existieren.)*
- (b) *Für die Anzahl n_p der Sylow p-Untergruppen von G gilt $n_p \equiv 1 \pmod{p}$.*
- (c) *Alle Sylow p-Untergruppen von G sind konjugiert in G .*