Kurzskript Algebra

Immi Halupczok

29. April 2026

Inhaltsverzeichnis

Algebra

Mo 13.4.

1 Gruppen

1.1 Gruppen und Untergruppen

Konvention 1.1.1 *Wir fassen* 0 *als natürliche Zahl auf:* $\mathbb{N} = \{0, 1, 2, \dots\}$.

Definition 1.1.2 (a) *Eine* ***Gruppe*** *ist eine Menge* G *mit einer Verknüpfung* $\circ\colon G \times G \to G$ *und einem Element* $e \in G$*, die die folgenden* ***Gruppenaxiome*** *erfüllen:*

(i) $\forall a, b, c \in G\colon (a \circ b) \circ c = a \circ (b \circ c)$ *(****Assoziativität****)*

(ii) $\forall a \in G\colon a \circ e = e \circ a = a$ *(*e *ist ein* ***neutrales Element****.)*

(iii) $\forall a \in G\colon \exists b \in G\colon a \circ b = b \circ a = e$*. (Existenz von* ***Inversen****.)*

(b) *Eine Gruppe* G *heißt* ***kommutativ*** *oder* ***abelsch****, wenn außerdem gilt:* $\forall a, b \in G\colon a \circ b = b \circ a$

Bemerkung 1.1.3 *Das neutrale Element und die inversen Elemente sind eindeutig durch die Verknüpfung* $\circ$ *festgelegt, und es reicht, „eine Richtung zu prüfen“:*

(a) *Ist* $b \in G$ *so, dass für alle* $a \in G$ *gilt:* $a \circ b = b$*, dann ist* $b = e$*.*

(b) *Ist* $b \circ a = e$*, so ist* b *das Inverse von* a *(und umgekehrt).*

Notation 1.1.4 (a) *Die Verknüpfung wird oft auch als* $a \cdot b$ *oder ab geschrieben (****multiplikative Notation****), und das neutrale Element wird manchmal* 1 *genannt. Für* $n \in \mathbb{N}$ *setzen wir* $a^n := \underbrace{a \cdots a}_{n \text{ mal}}$ *und* $a^{-n} := (a^{-1})^n$*.*

(b) *Bei abelschen Gruppen verwendet man oft auch* ***additive Notation****: Verknüpfung:* $a + b$*; neutrales Element:* 0*; Inverses von* a*:* $-a$*. Wir definieren auch* $a - b := a + (-b)$*,* $0 \cdot a := 0$*,* $n \cdot a := \underbrace{a + \cdots + a}_{n \text{ mal}}$*,* $(-n) \cdot a := n \cdot (-a)$

Bemerkung 1.1.5 *Sei* G *eine Gruppe, und seien* $a, b \in G$*.*

(a) *Wenn ein* $c \in G$ *existiert mit* $ac = bc$ *(oder* $ca = cb$*), so gilt* $a = b$*.*

(b) *Es gilt* $(ab)^{-1} = b^{-1}a^{-1}$

(c) *Es gilt* $(a^{-1})^{-1} = a$*.*

(d) *Für beliebige* $m, n \in \mathbb{Z}$ *gilt:* $a^m \cdot a^n = a^{m+n}$*.*

Beispiel 1.1.6 (a) $(\mathbb{Z}, +)$ *ist eine abelsche Gruppe.*

(b) *Ist* K *ein Körper, so sind* $(K, +)$ *und* $(K^\times, \cdot)$ *abelsche Gruppen. Hierbei ist* $K^\times := K \setminus \{0\}$*.*

(c) *Ist außerdem* V *ein* K*-Vektorraum, so ist* $(V, +)$ *eine abelsche Gruppe.*

(d) *Die Menge*

$$\mathrm{GL}_n(K) := \{A \in K^{n\times n} \mid \det A \neq 0\}$$

der invertierbaren $n \times n$-Matrizen über K ist eine Gruppe mit Matrixmultiplikation als Verknüpfung. Ist $n \geq 2$, so ist $\mathrm{GL}_n(K)$ nicht abelsch.

Beispiel 1.1.7 *Ist M eine Menge, so definiert man die* ***symmetrische Gruppe*** *als*

$$\mathrm{Sym}(M) := \{f\colon M \to M \mid f \text{ ist bijektiv}\},$$

mit der Verkettung von Abbildungen als Verknüpfung. Das neutrale Element ist die Identitätsabbildung id_M; das inverse Element zu $f \in \mathrm{Sym}(M)$ ist die inverse Abbildung. Elemente von $\mathrm{Sym}(M)$ nennt man auch ***Permutationen*** *von M.*
Wir setzen auch: $S_n := \mathrm{Sym}(\{1, \ldots, n\})$.

Definition 1.1.8 *Seien G und H Gruppen. Das* ***(direkte) Produkt*** *von G und H ist die Gruppe $G \times H$ mit der komponentenweiser Verknüpfung:*

$$(a, b) \cdot (a', b') := (aa', bb')$$

für $a, a' \in G$, $b, b' \in H$.

Definition 1.1.9 *Sei $(G, \circ, e)$ eine Gruppe. Ist $H \subseteq G$ eine Teilmenge, so dass $(H, \circ|_{H\times H}, e)$ auch eine Gruppe ist, so nennt man H eine* ***Untergruppe*** *von G. Die Notation $H \leq G$ bedeutet, dass H eine Untergruppe von G ist.*

Bemerkung 1.1.10 *Eine Teilmenge H einer Gruppe G ist eine Untergruppe genau dann, wenn H nicht leer ist, und wenn für alle $a, b \in H$ gilt: $a \circ b^{-1} \in H$.*

Beispiel 1.1.11 *Ist G eine beliebige Gruppe, so sind G selbst und $\{e\}$ Untergruppen von G. ($\{e\}$ nennt man die* ***triviale Untergruppe****.)*

Beispiel 1.1.12 *Ist G eine Gruppe und $a \in G$, so ist $\{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.*

Bemerkung 1.1.13 *Ist G eine Gruppe und sind $H_i \leq G$ Untergruppen, für $i \in I$, so ist auch der Schnitt $\bigcap_{i\in I} H_i$ eine Untergruppe von G.*

Beispiel 1.1.14 *Die Untergruppen von $\mathbb{Z}$ sind genau die Teilmengen der Form $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, für ein $n \in \mathbb{N}$. (Im Fall $n = 0$ ist $n\mathbb{Z} = \{0\}$.)*

Mi 15.4.

Lemma 1.1.15 *Ist G eine Gruppe und $A \subseteq G$ eine beliebige Teilmenge, so existiert unter allen Untergruppen von G, die A enthalten, eine kleinste.*

Zur Erinnerung: Ist $\mathcal{M}$ eine Menge von Mengen, so nennt man $A \in \mathcal{M}$ die **kleinste Menge** von $\mathcal{M}$, wenn jede Menge $B \in \mathcal{M}$ eine Obermenge von A ist. (Eine kleinste Menge muss nicht immer existieren, aber wenn sie existiert, ist sie eindeutig.)

Definition 1.1.16 *Sei G eine Gruppe.*

(a) *Ist $A \subseteq G$ eine beliebige Teilmenge, so nennt man die kleinste Untergruppe von G, die A enthält, die von A **erzeugte Untergruppe**. Notation für diese Untergruppe: $\langle A \rangle$. Statt $\langle \{a_1, \ldots, a_n\} \rangle$ (für $a_1, \ldots, a_n \in G$) schreibt man auch $\langle a_1, \ldots, a_n \rangle$.*

(b) *Gilt $\langle A \rangle = G$, so sagt man, die Elemente von A sind **Erzeuger** von G; und: G wird von (den Elementen von) A **erzeugt**.*

(c) *Wird G von einem eizelnen Element erzeugt (d. h. $G = \langle a \rangle$ für ein $a \in G$), so nennt man G **zyklisch**.*

Beispiel 1.1.17 *Ist G eine Gruppe und $a \in G$, so ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.*

Beispiel 1.1.18 *Ist G abelsch und sind $a_1, \ldots, a_n \in G$, so ist*

$$\langle a_1, \ldots, a_n \rangle = \{a_1^{r_1} \cdots a_n^{r_n} \mid r_1, \ldots, r_n \in \mathbb{Z}\}.$$

1.2 Gruppenhomomorphismen und Normalteiler

Definition 1.2.1 *Seien G und H Gruppen.*

(a) *Ein **(Gruppen-)Homomorphismus** ist eine Abbildung $f\colon G \to H$, für die gilt:*

$$\forall a, b \in G\colon\ f(ab) = f(a)f(b).$$

Die Menge der Gruppenhomomorphismen von G nach H wird mit $\mathrm{Hom}(G, H)$ bezeichnet.

(b) *Das **Bild** von f ist $\operatorname{im} f := \{f(a) \mid a \in G\}$; der **Kern** von f ist $\ker f := \{a \in G \mid f(a) = e\}$.*

(c) *Ein **Isomorphismus von Gruppen** ist ein bijektiver Gruppenhomomorphismus. Zwei Gruppen G und H heißen **isomorph** (zueinander), wenn ein Isomorphismus $G \to H$ existiert. Notation dafür: $G \cong H$*

(d) *Ein **Automorphismus** einer Gruppe G ist ein Isomorphismus von G nach G. Die Menge der Automorphismen von G wird mit $\mathrm{Aut}(G)$ bezeichnet.*

Bemerkung 1.2.2 *Ist $f\colon G \to H$ ein Gruppenhomomorphismus, so gilt $f(e) = e$, und für $a \in G$ gilt $f(a^{-1}) = f(a)^{-1}$.*

Bemerkung 1.2.3 *Die Verknüpfung von zwei Gruppenhomomorphismen ist wieder ein Gruppenhomomorphismus, und das Inverse eines Gruppenisomorphismusses ist ein Gruppenisomorphismus. Insbesondere ist $\mathrm{Aut}(G)$ eine Untergruppe von $\mathrm{Sym}(G)$.*

Beispiel 1.2.4 *Ist G eine Gruppe und $a \in G$, so ist $\mathbb{Z} \to G, n \mapsto a^n$ ein Gruppenhomomorphismus. Das Bild davon ist $\langle a \rangle$.*

Beispiel 1.2.5 *Ist G eine Gruppe und $a \in G$ ein fest gewähltes Element, so ist $G \to G, x \mapsto axa^{-1}$ ein Automorphismus von G. Diese Abbildung nennt man die* ***Konjugation*** *mit a.*

Lemma 1.2.6 *Ist $f\colon G \to H$ ein Gruppenhomomorphismus (insbesondere seien G, H Gruppen) so ist $\operatorname{im} f$ eine Untergruppe von H. Allgemeiner gilt: Ist $G' \leq G$ eine Untergruppe, so ist $f(G')$ eine Untergruppe von H. Außerdem: Wird G' von $A \subseteq G$ erzeugt, so wird $f(G')$ von $f(A)$ erzeugt.*

Definition 1.2.7 *Ein* ***Normalteiler*** *(auch:* ***normale Untergruppe****) von G ist eine Untergruppe $N \leq G$, für die gilt: Für alle $a \in N$ und alle $b \in G$ gilt $bab^{-1} \in N$. Die Notation $N \lhd G$ bedeutet, dass N ein Normalteiler von G ist.*

Bemerkung 1.2.8 (a) *Für beliebige Gruppen G sind sowohl G als auch $\{e\}$ Normalteiler von G.*
(b) *Ist G abelsch, so ist jede Untergruppe von G bereits ein Normalteiler von G.*

Mo 20.4.

Lemma 1.2.9 *Sind G und H Gruppen und ist $f\colon G \to H$ ein Gruppenhomomorphismus, so ist $\ker f$ ein Normalteiler von G. Allgemeiner gilt: Ist $H' \leq H$ eine Untergruppe bzw. ein Normalteiler von H, so ist $f^{-1}(H')$ eine Untergruppe bzw. ein Normalteiler von G.*

1.3 Nebenklassen und Quotienten

Definition 1.3.1 *Sei G eine Gruppe und $H \leq G$ eine Untergruppe.*

(a) *Eine* ***Linksnebenklasse*** *von H ist eine Menge der Form $aH := \{ah \mid h \in H\}$ für $a \in G$. Die Menge aller Linksnebenklassen von H wird mit G/H bezeichnet.*
(b) *Eine* ***Rechtsnebenklasse*** *von H ist eine Menge der Form $Ha := \{ha \mid h \in H\}$ für $a \in G$. Die Menge aller Rechtsnebenklassen von H wird mit $H\backslash G$ bezeichnet.*

Bemerkung: Wenn wir additive Notation verwenden, schreiben wir Nebenklassen als $a + H = \{a + h \mid h \in H\}$.

Lemma 1.3.2 *Ist G eine Gruppe und $N \lhd G$ ein Normalteiler und $a \in G$, so gilt $aN = Na$. Insbesondere sind Linksnebenklassen das gleiche wie Rechtsnebenklassen, und man spricht einfach von* ***Nebenklassen****.*

Lemma 1.3.3 *Sei G eine Gruppe und $H \leq G$ eine Untergruppe.*

(a) *Die Menge der Linksnebenklassen von H bildet eine Partition von G, d. h. jedes Element $a \in G$ liegt in genau einer Linksnebenklasse, nämlich $a \in aH$.*
(b) *Zwei Elemente $a, b \in G$ liegen in der gleichen Linksnebenklasse von H genau dann, wenn $a^{-1}b \in H$ gilt.*
(c) *Jede Linksnebenklasse von H hat die gleiche Kardinalität wie H (d. h. für beliebige $a \in G$ gilt: $\#(aH) = \#H$).*

Analoge Aussagen gelten für Rechtsnebenklassen.

Definition 1.3.4 *Sei G eine Gruppe.*

(a) *Statt „Kardinalität von G“ sagt man auch **Ordnung** von G. (Als Notation verwendet man trotzdem $\#G$.)*
(b) *Der **Index** einer Untergruppe $H \leq G$ ist definiert durch $(G : H) := \#(G/H) \in \mathbb{N} \cup \{\infty\}$. (Manche Leute schreiben auch $[G : H]$ für den Index von H in G.)*

Notation 1.3.5 *Sind $a, b \in \mathbb{Z}$, so schreiben wir $a \mid b$, wenn a ein Teiler von b ist, d. h. wenn ein $c \in \mathbb{Z}$ existiert, so dass $ac = b$ ist. Man sagt auch „a **teilt** b“.*

Satz 1.3.6 (Satz von Lagrange) *Ist G eine Gruppe und $H \leq G$ eine Untergruppe, so gilt $\#G = \#H \cdot (G : H)$. Insbesondere gilt $\#H \mid \#G$.*

Bemerkung 1.3.7 *Ist $f \colon G \to H$ ein Gruppenhomomorphismus mit Kern $N \triangleleft G$ und sind $a, b \in G$, so gilt $f(a) = f(b)$ genau dann wenn $aN = bN$. Insbesondere ist f injektiv genau dann, wenn $\ker f = \{e\}$ ist.*

Satz 1.3.8 *Sei G eine Gruppe und $N \triangleleft G$ ein Normalteiler.*

(a) *Für $a, b \in G$ gilt: $\{a'b' \mid a' \in aN, b' \in bN\} = (ab)N$.*
(b) *Die Menge G/N wird mit der Verknüpfung $(aN) \cdot (bN) := (ab)N$ eine Gruppe.*
(c) *Die Abbildung $G \to G/N, a \mapsto aN$ ist ein surjektiver Gruppenhomomorphismus mit Kern N.*

Definition 1.3.9 *Die Gruppe G/N („G **modulo** N“) aus dem vorigen Satz wird **Quotientengruppe** (oder manchmal auch **Faktorgruppe**) genannt.*

Mi 22.4.

Notation 1.3.10 *Ist G eine Gruppe, $N \triangleleft G$ und $a \in G$, so schreiben wir für die Nebenklasse $aN \in G/N$ manchmal auch $\bar{a}$. Diese Abbildung $G \to G/N$ nennt man auch die **kanonische Abbildung**.*

Beispiel 1.3.11 *Für $n \geq 1$ ist $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.*

Definition 1.3.12 *Eine Gruppe G heißt **einfach**, wenn G und $\{e\}$ ihre einzigen Normalteiler sind.*

Beispiel 1.3.13 *Ist p eine Primzahl, so ist jede Gruppe der Ordnung p einfach. Insbesondere ist $\mathbb{Z}/p\mathbb{Z}$ einfach.*

1.4 Der Homomorphiesatz und Anwendungen

Satz 1.4.1 (Homomorphiesatz) *Seien G und H Gruppen und $f\colon G \to H$ ein Homomorphismus. Dann erhalten wir einen Isomorphismus*

$$\tilde{f}\colon G/\ker f \to \operatorname{im} f, \bar{a} \mapsto f(a).$$

Satz 1.4.2 *Ist G eine Gruppe und $a \in G$, so existiert ein $n \in \mathbb{N}$, so dass man einen Isomorphismus*

$$\mathbb{Z}/n\mathbb{Z} \to \langle a \rangle, \bar{m} \mapsto a^m$$

erhält. Insbesondere ist jede zyklische Gruppe isomorph zu $\mathbb{Z}/n\mathbb{Z}$, für ein $n \in \mathbb{N}$.

Definition 1.4.3 *Sei G eine Gruppe. Die **Ordnung** $\operatorname{ord}(a)$ eines Elements a von G ist die definiert als die Ordnung der von a erzeugten Gruppe $\langle a \rangle$. Ist $\langle a \rangle$ unendlich, so setzt man $\operatorname{ord}(a) := \infty$.*

Die Ordnung eines Elements a ist 1 genau dann, wenn a das neutrale Element ist.

Bemerkung 1.4.4 *Sei G eine Gruppe und $a \in G$. Ist $\operatorname{ord}(a) \in \mathbb{N}$, so gilt $a^m = 1$ genau dann, wenn m ein Vielfaches von $\operatorname{ord}(a)$ ist. Insbesondere ist $\operatorname{ord}(a)$ die kleinste positive natürliche Zahl n, so dass $a^n = e$ gilt. Ist $\operatorname{ord}(a) = \infty$, so ist $a^m \neq e$ für alle $m \neq 0$.*

Satz 1.4.5 *Ist G eine endliche Gruppe und $a \in G$, so ist $a^{\#G} = e$.*

Satz 1.4.6 (Kleiner Satz von Fermat) *Ist p eine Primzahl und $a \in \mathbb{Z}$ nicht durch p teilbar, so ist $a^{p-1} - 1$ durch p teilbar.*

Mo 27.4.

Bemerkung 1.4.7 *Für jede Primzahl p existiert bis auf Isomorphie genau eine Gruppe der Ordnung p, nämlich $\mathbb{Z}/p\mathbb{Z}$.*

1.5 Die symmetrischen und alternierenden Gruppen

Notation 1.5.1 *Sind $x_1, \ldots, x_n$ paarweise verschiedene Elemente von $\{1, \ldots, n\}$, so ist*

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ x_1 & x_2 & \cdots & x_n \end{pmatrix}$$

eine Notation für das Element $\sigma \in S_n$, das i auf x_i abbildet, für $i = 1, \ldots, n$.

Definition 1.5.2 (a) *Sei $k \geq 2$. Ein Element $\sigma \in S_n$ heißt **Zyklus** (der Länge k), wenn es paarweise verschiedene $x_1, \ldots, x_k \in \{1, \ldots, n\}$ gibt, so dass gilt: $\sigma(x_i) = x_{i+1}$ für $1 \leq i < k$; $\sigma(x_k) = x_1$; $\sigma(y) = y$ falls $y \notin \{x_1, \ldots, x_k\}$. Die Menge $\{x_1, \ldots, x_k\}$ nennt man den **Träger** von σ. Meine Notation für einen solchen Zyklus: $\overbrace{x_1, x_2, \ldots, x_k}$. Andere (üblichere) Notationen: $(x_1, x_2, \ldots, x_k)$, $(x_1\ x_2\ \cdots\ x_k)$.*

(b) *Zykel der Länge 2 nennt man auch **Transpositionen**. Transpositionen der Form $\overbrace{x, x+1}$ nennt man **Nachbartranspositionen**.*

Lemma 1.5.3 *Sind $\sigma, \sigma' \in S_n$ Zykel mit disjunkten Trägern, so gilt $\sigma\sigma' = \sigma'\sigma$.*

Satz 1.5.4 *Jedes Element $\sigma \in S_n$ lässt sich als Produkt $\sigma_1 \cdots \sigma_m$ von Zykeln σ_j schreiben, die paarweise disjunkte Träger haben. Diese Schreibweise ist eindeutig bis auf Reihenfolge. (Man nennt dies die **Zykelzerlegung** von σ.)*

Satz 1.5.5 *S_n wird von den Nachbartransposition erzeugt (d. h. jedes Element von S_n lässt sich als Produkt von Nachbartransposition schreiben).*

Lemma 1.5.6 *Ist $\sigma = \overbrace{x_1, \ldots, x_k}$ ein Zyklus und $\tau \in S_n$ beliebig, so ist $\tau\sigma\tau^{-1} = \overbrace{\tau(x_1), \ldots, \tau(x_k)}$.*

Insbesondere: Ist $N \triangleleft S_n$ ein Normalteiler, der einen Zyklus der Länge k enthält, so enthält N alle Zyklen der Länge k.

Definition 1.5.7 *Sei $\sigma \in S_n$.*

(a) *Die zugehörige **Permutationsmatrix** ist diejenige Matrix $A_\sigma \in \mathbb{Z}^{n \times n}$, die $e_i \in \mathbb{Z}^n$ abbildet auf $e_{\sigma(i)}$ für $i = 1, \ldots n$.*

(b) *Das **Signum** von σ ist definiert als* $\operatorname{sgn}(\sigma) := \det(A_\sigma)$.

Ist $A_\sigma = (a_{ij})_{ij}$, so ist also $a_{\sigma(i),i} = 1$ für alle i, und alle restlichen Einträge sind 0.

Lemma 1.5.8 *Die Signum-Abbildung ist ein Gruppenhomomorphismus von S_n nach $\{\pm 1\}$. Lässt sich $\sigma \in S_n$ als Produkt von k Transpositionen schreiben, so ist* $\operatorname{sgn}(\sigma) = (-1)^k$.

Mi 29.4.

Bemerkung 1.5.9 *Das Signum eines Elements $\sigma \in S_n$ lässt sich auch wie folgt berechnen: Ein **Fehlstand** von σ ist ein Paar $a, b \in \{1, \ldots, n\}$ mit $a < b$ und $\sigma(a) > \sigma(b)$. Es gilt:* $\operatorname{sgn}(\sigma) = -1^{\#\{(a,b) | (a,b)\ ist\ Fehlstand\}}$.

Definition 1.5.10 *Die **alternierende Gruppe** $A_n \leq S_n$ ist der Kern von* $\operatorname{sgn}\colon S_n \to \{\pm 1\}$.

Bemerkung 1.5.11 *S_n hat Ordnung $n!$. Ist $n \geq 2$, so hat A_n Ordnung $\frac{n!}{2}$.*

Beispiel 1.5.12 *Die Gruppen A_1 und A_2 sind trivial. $A_3 \cong \mathbb{Z}/3\mathbb{Z}$.*

Satz 1.5.13 *Für $n \geq 5$ ist A_n einfach.*

Bemerkung 1.5.14 *Die Menge*

$$V = \{\mathrm{id}, \overline{1,2} \circ \overline{3,4}, \overline{1,3} \circ \overline{2,4}, \overline{1,4} \circ \overline{2,3}\}$$

*ist ein Normalteiler von A_4, die **kleinsche Vierergruppe**. (Dies werden wir später überprüfen.) Also ist A_4 nicht einfach.*

1.6 Operationen von Gruppen auf Mengen

Definition 1.6.1 *Sei G eine Gruppe und X eine Menge. Eine **Gruppenwirkung** (auch: **Gruppenoperation**) von G auf X ist ein Gruppenhomomorphismus λ von G nach $\mathrm{Sym}(X)$. Ist $a \in G$ und $x \in X$, so schreiben wir meistens $\lambda_a(x)$ statt $(\lambda(a))(x)$.*

Bemerkung 1.6.2 *Eine Gruppenwirkung $\lambda\colon G \to \mathrm{Sym}(X)$ kann man auch auffassen als eine Abbildung $G \times X \to X, (a, x) \mapsto \lambda_a(x)$, also eine Verknüpfung von Elementen von G mit Elementen von X, die Elemente von X liefert. Manchmal verwendet man auch eine entsprechende Notation, d. h. man schreibt ax statt $\lambda_a(x)$.*

Beispiel 1.6.3 *Einige Gruppen kommen mit einer **natürlichen Gruppenwirkung**: S_n wirkt auf $\{1, \ldots, n\}$, $\mathrm{GL}_n(K)$ wirkt auf K^n (für Körper K), $\mathrm{Aut}(G)$ wirkt auf G (für Gruppen G).*

Bemerkung 1.6.4 *Sei G eine Gruppe, die auf einer Menge X wirkt. Dann gilt für alle $a, b \in G$ und alle $x, y \in X$:*

(a) $ex = x$.
(b) $(ab)x = a(bx)$.
(c) *Ist $ax = y$, so ist $a^{-1}y = x$.*

Bemerkung 1.6.5 *Wirkt eine Gruppe G auf einer Menge X, so wirkt auch jede Untergruppe $H \leq G$ auf X.*

Beispiel 1.6.6 *Jede Gruppe G operiert auf mehrere Weisen auf sich selbst:*

(a) *durch **links-Multiplikation**: $G \to \mathrm{Sym}(G), a \mapsto (b \mapsto ab)$.*
(b) *durch **rechts-Multiplikation**: $G \to \mathrm{Sym}(G), a \mapsto (b \mapsto ba^{-1})$.*

(c) *durch* ***Konjugation*** *(vgl. Beispiel 1.2.5):* $G \to \mathrm{Sym}(G), a \mapsto (b \mapsto aba^{-1})$.

Mo 4.5.

Satz 1.6.7 (Satz von Cayley) *Jede endliche Gruppe ist isomorph zu einer Untergruppe von* S_n*, für ein geeignetes* $n \in \mathbb{N}$*.*

Definition 1.6.8 *Sei* G *eine Gruppe, die auf einer Menge* X *wirkt, und sei* $x \in X$*.*

(a) *Die* ***Bahn*** *von* x *ist die Menge* $Gx := \{ax \mid a \in G\} \subseteq X$*.*
(b) *Gilt* $Gx = \{x\}$*, so nennt man* x *einen* ***Fixpunkt*** *dieser Gruppenwirkung.*
(c) *Gilt* $Gx = X$ *(für ein beliebiges* $x \in X$*), so sagt man, „*G *wirkt* ***transitiv*** *auf* X*“.*

Bemerkung 1.6.9 *Die Menge* $\{Gx \mid x \in X\}$ *aller Bahnen ist eine Partition von* X*. Zwei Elemente* $x, y \in X$ *liegen in der gleichen Bahn genau dann, wenn ein* $a \in G$ *existiert mit* $ax = y$*.*

Beispiel 1.6.10 *Sei* G *eine Gruppe und* X *die Menge aller Untergruppen von* G*. Dann wirkt* G *durch Konjugation auf* X*:* $a \mapsto (H \mapsto aHa^{-1})$*. Eine Untergruppe* $H \in X$ *ist ein Normalteiler von* G *genau dann, wenn* H *ein Fixpunkt der Wirkung ist.*

Definition 1.6.11 *Sei* G *eine Gruppe, die auf einer Menge* X *wirkt, und seien* $a \in G$ *und* $x \in X$*.*

(a) *Man sagt,* a ***stabilisiert*** x *oder* a ***hält*** x ***fest****, wenn* $ax = x$ *gilt.*
(b) *Der* ***Stabilisator*** *von* x *ist* $\mathrm{Stab}_G(x) := \{a \in G \mid ax = x\}$*.*

Bemerkung 1.6.12 $\mathrm{Stab}_G(x)$ *ist eine Untergruppe von* G*. Es gilt* $\mathrm{Stab}_G(x) = G$ *genau dann, wenn* x *ein Fixpunkt der Wirkung ist.*

Satz 1.6.13 (Bahnenformel) *Sei* G *eine endliche Gruppe, die auf einer endlichen Menge* X *wirkt, und seien* $Gx_1, \ldots, Gx_k$ *die Bahnen dieser Wirkung (mit* $Gx_i \neq Gx_j$ *für* $i \neq j$*). Dann gilt*

$$\#(Gx_i) = (G : \mathrm{Stab}_G\, x_i) = \frac{\#G}{\#(\mathrm{Stab}_G\, x_i)}$$

und insbesondere

$$\#X = \sum_{i=1}^{k} \frac{\#G}{\#(\mathrm{Stab}_G\, x_i)}.$$

1.7 Auflösbarkeit und p-Gruppen

Definition 1.7.1 *Eine Gruppe heißt* ***auflösbar****, wenn eine Folge von Untergruppen $\{e\} = G_r \leq G_{r-1} \leq \cdots \leq G_0 = G$ existiert, so dass G_{i+1} ein Normalteiler von G_i ist und der Quotient G_{i-1}/G_i abelsch ist für $i = 1, \ldots, r$. Die Gruppen $G_r \leq \cdots \leq G_0$ nennt man eine* ***Auflösung*** *von G.*

Bemerkung 1.7.2 *Ist $\{e\} = G_r \leq G_{r-1} \leq \cdots \leq G_0 = G$ eine Auflösung einer endlichen Gruppe G, so gilt $\#G = \prod_{i=1}^{r} \#(G_{i-1}/G_i)$.*

Beispiel 1.7.3 *Für $n \leq 4$ ist S_n auflösbar.*

Bemerkung 1.7.4 *Sind G_1, G_2 Gruppen, $N_1 \triangleleft G_1, N_2 \triangleleft G_2$ Normalteiler und ist $f\colon G_1 \to G_2$ ein Gruppenhomomorphismus mit $f(N_1) \subseteq N_2$, so erhalten wir einen wohldefinierten Gruppenhomomorphismus $G_1/N_1 \to G_2/N_2$, der aN_1 auf $f(a)N_2$ abbildet.*

Lemma 1.7.5 *Sei G eine auflösbare Gruppe. Dann ist auch jede Untergruppe von G auflösbar, und ist $N \triangleleft G$ ein Normalteiler, so ist auch G/N auflösbar.*

Beispiel 1.7.6 *Für $n \geq 5$ ist S_n nicht auflösbar.*

Lemma 1.7.7 *Ist G endlich und auflösbar, so existiert eine Auflösung $\{e\} = G_r \leq \cdots \leq G_0 = G$ von G, so dass die Quotienten G_{i-1}/G_i isomorph zu $\mathbb{Z}/p_i\mathbb{Z}$ sind, für Primzahlen p_i.*

Korollar 1.7.8 *Ist G eine endliche auflösbare Gruppe und ist p eine Primzahl, die $\#G$ teilt, so existiert ein $a \in G$ der Ordnung p.*

Definition 1.7.9 *Sei p eine Primzahl. Eine p-Gruppe ist eine endliche Gruppe G, deren Ordnung eine Potenz von p ist.*

Satz 1.7.10 *Jede p-Gruppe ist auflösbar.*

Definition 1.7.11 *Das* ***Zentrum*** *einer Gruppe G ist die Menge $Z(G) := \{a \in G \mid \forall b \in G\colon ab = ba\}$ der Elemente, die mit allen Elementen von G kommutieren.*

Bemerkung 1.7.12 *Das Zentrum einer Gruppe ist immer abelsch.*

Lemma 1.7.13 *Jede Untergruppe $H \leq Z(G)$ ist ein Normalteiler von G.*

Lemma 1.7.14 *Ist G eine nicht-triviale p-Gruppe, so ist $Z(G)$ nicht-trivial.*

Korollar 1.7.15 *Ist G eine Gruppe der Ordnung p^2, für eine Primzahl p, so ist G abelsch.*

1.8 Die Sylow-Sätze

Definition 1.8.1 *Sei p eine Primzahl und G eine endliche Gruppe. Wir schreiben die Ordnung von G als $\#G = m \cdot p^\ell$ für $\ell, m \in \mathbb{N}$ mit $p \nmid m$.*

(a) *Eine **p-Untergruppe** von G ist eine Untergruppe, die eine p-Gruppe ist (also der Ordnung p^k für ein $k \leq \ell$).*
(b) *Eine **Sylow-p-Untergruppe** von G ist eine Untergruppe der Ordnung genau p^ℓ.*

Notation 1.8.2 *Sind $a, b \in \mathbb{Z}$ und ist $n \in \mathbb{N}, n \geq 1$, so bedeutet $a \equiv b \mod n$ (Aussprache: „a ist **kongruent** zu b **modulo** n“), dass $a - b$ durch n teilbar ist.*

Satz 1.8.3 (Sylow-Sätze) *Sei G endlich und sei p eine Primzahl. Wir schreiben $\#G = m \cdot p^\ell$ für $\ell, m \in \mathbb{N}$ mit $p \nmid m$. Dann gilt:*

(a) *Jede p-Untergruppe von G ist in einer Sylow-p-Untergruppe enthalten.*
(b) *Alle Sylow-p-Untergruppen von G sind konjugiert, d. h. sind $P, P' \leq G$ Sylow-p-Untergruppen, so gibt es ein $a \in G$ mit $aPa^{-1} = P'$.*
(c) *Ist s_p die Anzahl der Sylow-p-Untergruppen von G, so gilt $s_p \equiv 1 \mod p$ und $s_p \mid m$.*

Bemerkung 1.8.4 *Insbesondere folgt, dass G mindestens eine Sylow-p-Untergruppe besitzt.*

Bemerkung 1.8.5 *Außerdem folgt: Eine Sylow-p-Untergruppe $P \leq G$ ist ein Normalteiler von G genau dann, wenn P die einzige Sylow-p-Untergruppe von G ist.*

Beispiel 1.8.6 (a) *A_4 hat vier Sylow-3-Untergruppen.*
(b) *Die kleinsche Vierergruppe V aus Bemerkung 1.5.14 ist die einzige Sylow-2-Untergruppe von A_4 und damit ein Normalteiler.*

Lemma 1.8.7 *Ist G eine endliche Gruppe und p eine Primzahl mit $p \mid \#G$, so existiert eine Sylow-p-Untergruppe von G.*

Lemma 1.8.8 *Sei G eine endliche Gruppe, $P \leq G$ eine Sylow-p-Untergruppe und $H \leq G$ eine p-Gruppe. Wir nehmen an, dass für alle $h \in H$ gilt: $hPh^{-1} = P$. Dann ist $H \leq P$.*

Korollar 1.8.9 (Satz von Cauchy) *Ist G eine endliche Gruppe und p eine Primzahl mit $p \mid G$, so existiert in G ein Element der Ordnung p.*

Korollar 1.8.10 *Gruppen der Ordnung pq, für Primzahlen q, p, sind auflösbar.*

Korollar 1.8.11 *Seien p und q Primzahlen mit $q > p$ und $p \nmid (q - 1)$. Dann gibt es bis auf Isomorphie nur eine Gruppe der Ordnung pq, nämlich $\mathbb{Z}/pq\mathbb{Z}$.*