

UNIVERSITÄT
LEIPZIG

# Algebra 1

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung

2. Mehr über $S_n$

3. Isomorphismen

4. Homomorphismen

- Sei $G$ eine Gruppe und $S \subseteq G$. Die Menge $S$ heißt *Erzeugendensystem* von $G$, falls jedes $g \in G$ als Produkt von Elementen aus $S$ und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{n_1} \cdots s_k^{n_k}$ mit $s_i \in S$ und $n_i \in \mathbb{Z}$.
  - Geschrieben: $G = \langle S \rangle$.
  - Übung $\mathrm{SL}(2, \mathbb{Z}) = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$.
- Eine Gruppe $G$ heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird.
  - Also $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.
- Beispiele: $(\mathbb{Z}, +)$, $\mathbb{Z}/n$, $\mathbb{Z}/a \times \mathbb{Z}/b$ wobei $\mathrm{ggT}(a, b) = 1$, $\{1, \zeta, \ldots, \zeta^{n-1}\}$ wobei $\zeta = e^{i2\pi/n}$, Rotationen eines $n$-ecks.

- Die *Ordnung* einer Gruppe $G$ ist ihre Kardinalität $|G|$.
- Sei $g \in G$. Die *Ordnung* von $g$, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches $n$ gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$
- Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

- Für Permutation verwenden wir meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein “Zyklus”.

- falls $\sigma$ and $\tau$ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

- Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Und zwar eindeutig bis auf die Reihenfolge der Zyklen.

- Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

1. Wiederholung

2. Mehr über $S_n$

3. Isomorphismen

4. Homomorphismen

Erinnerung aus der Linearen Algebra 2:

- Eine *Transposition* ist ein Zykel der Länge $2$. Z.B. $(1\,2)$.

- Jede Permutation ist ein Produkt von Transpositionen. z.B. $(1\,2\,3) = (1\,3)(1\,2)$.
  - Mit unserem neuen Wortschatz: Die Menge aller Transpositionen erzeugt $S_n$.

- Lässt sich eine Permutation als Produkt einer geraden Anzahl von Transpositionen darstellen, so hat jede solche Darstellung eine gerade Anzahl von Transpositionen.

- Damit ist die *Parität* einer Permutation wohldefiniert: Eine Permutation heißt *gerade*, falls sie ein Produkt einer geraden Anzahl von Transpositionen ist, sonst *ungerade*.

- Wir setzen $\operatorname{sgn}(\sigma) := 1$ für gerade $\sigma$ und $\operatorname{sgn}(\sigma) := -1$ für ungerade $\sigma$.
  - Es folgt $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$.
  - Mit Induktion folgt auch $\operatorname{sgn}(\sigma_1 \dots \sigma_k) = \operatorname{sgn}(\sigma_1) \cdot \ldots \cdot \operatorname{sgn}(\sigma_k)$.

- Die Menge der geraden Permutationen in $S_n$ heißt *alternierende Gruppe*: $A_n := \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$.
- Wegen $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$ ist $A_n$ eine Untergruppe von $S_n$.
- Übung: für $n \geqslant 2$ gilt $|A_n| = n!/2$.

**Lemma.** Sei $\sigma = \alpha_1 \dots \alpha_k$ ein Produkt disjunkter Zyklen der Längen $l_1, \dots, l_k$. Dann ist die Parität von $\sigma$ gleich mit der Parität der Zahl $(l_1 - 1) + \dots + (l_k - 1)$.

Andersgesagt:

$$\operatorname{sgn}(\sigma) = (-1)^{(l_1-1)+\dots+(l_k-1)}.$$

**Beweis.** Für einen Zykel $\alpha = (a_1 \ \dots \ a_l)$ gilt $\alpha = (a_1\, a_l) \cdots (a_1\, a_2)$. Also $\operatorname{sgn}(\alpha) = (-1)^{l-1}$.

Die Behauptung folgt nun aus $\operatorname{sgn}(\alpha_1 \cdots \alpha_k) = \operatorname{sgn}(\alpha_1) \cdots \operatorname{sgn}(\alpha_k)$. □

- Für $\sigma \in S_n$ heißt ein Paar $(i, j)$ mit $1 \leqslant i < j \leqslant n$ eine *Inversion*, falls $\sigma(i) > \sigma(j)$.
  - Mit $I(\sigma)$ bezeichnen wir die Anzahl der Inversionen von $\sigma$.

**Lemma.** Für jede Permutation $\sigma \in S_n$ gilt $\operatorname{sgn}(\sigma) = (-1)^{I(\sigma)}$.

**Beweis.** • Induktion über $I(\sigma)$. Falls $I(\sigma) = 0$, ist $\sigma$ streng monoton, also $\sigma = e$.

- Sonst gibt es ein $i$ mit $\sigma(i) > \sigma(i+1)$. Sei $\tau = (i\, i+1)$. Dann gilt $I(\sigma\tau) = I(\sigma) - 1$.
  - Für jedes $j \notin \{i, i+1\}$ bleibt die Gesamtzahl der Inversionen zwischen $j$ und $i, i+1$ unverändert.
  - Nur das Paar $(i, i+1)$ ist danach keine Inversion mehr.
- Nach Induktion gilt $\operatorname{sgn}(\sigma\tau) = (-1)^{I(\sigma\tau)} = (-1)^{I(\sigma)-1}$.
- Multiplizierung durch $\tau$ ändert gleichzeitig die Parität von $\operatorname{sgn}$ und von $I$. Die Behauptung folgt also aus $\sigma = \sigma\tau\tau$. □

1. Wiederholung

2. Mehr über $S_n$

3. Isomorphismen

4. Homomorphismen

- Wir haben mehrere zyklische Gruppen der Ordnung $n$ kennengelernt:
  - $(\mathbb{Z}/n, +)$;
  - die $n$-ten Einheitswurzeln $\{1, \zeta, \ldots, \zeta^{n-1}\}$ mit Multiplikation;
  - die Drehungen eines regelmäßigen $n$-Ecks.
- Algebraisch sehen diese Gruppen gleich aus: In multiplikativer Schreibweise haben sie alle die Form $\{e, g, \ldots, g^{n-1}\}$, wobei $g$ ein Erzeuger ist.
  - Wir wollen dieses „Gleichsein“ präzise beschreiben.
- Weiteres Beispiel: $S_3$ und die Gruppe aller Isometrien eines gleichseitigen Dreiecks.
  - Jede Isometrie permutiert die drei Ecken. Umgekehrt entspricht jeder Permutation der Ecken eine Isometrie.

- Eine Bijektion $f\colon G \to H$ zwischen zwei Gruppen heißt *Isomorphismus*, falls $f(xy) = f(x)f(y)$ für alle $x, y \in G$.
  - Existiert ein Isomorphismus, so heißen $G$ und $H$ *isomorph*.

**Lemma.** Für einen Isomorphismus $f\colon G \to H$ gilt:

- $f(e_G) = e_H$.
- $f(x^{-1}) = f(x)^{-1}$ für alle $x \in G$.

**Beweis.** • Für alle $x \in G$ gilt $f(e_G)f(x) = f(e_G x) = f(x)$. Wegen der Surjektivität von $f$ folgt $f(e_G) = e_H$.

• $f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_H$, also $f(x^{-1}) = f(x)^{-1}$. □

• Übung: $f^{-1}\colon H \to G$ ist auch ein Isomorphismus.

- Beispiel: $\log\colon \mathbb{R}_+ \to \mathbb{R}$ ist ein Isomorphismus zwisschen $(\mathbb{R}_+, \cdot)$ und $(\mathbb{R}, +)$. Der Inverse Isomorphismus ist $x \mapsto 2^x$.

**Lemma.** Zwei zyklische Gruppen derselben Ordnung sind isomorph.

**Beweis.** • Seien $G = \langle g \rangle$ und $H = \langle h \rangle$ zyklische Gruppen derselben Ordnung.

- Wir definieren $f\colon G \to H$ durch $f(g^k) := h^k$ für $k \in \mathbb{Z}$.
  - wohldefiniert: $g^k = g^l$ gdw $\operatorname{ord}(g) \mid l - k$ gdw $h^k = h^l$.
  - Bijektion: Z.B. sei $d := ord(g) < \infty$, dann $G = \{1, g, \ldots, g^{d-1}\}$, $H = \{1, h, \ldots, h^{d-1}\}$.
- $f(g^k g^l) = f(g^{k+l}) = h^{k+l} = h^k h^l = f(g^k) f(g^l)$. □

**Lemma.** Die Isometriegruppe $G$ gleichseitigen Dreiecks ist isomorph zu $S_3$.

**Beweis.** • Wir nummerieren die drei Ecken mit $1, 2, 3$. Jede Symmetrie $\alpha \in G$ permutiert die Ecken und liefert somit eine Abbildung $f\colon G \to S_3$.

• $f$ ist surjektiv: Die drei Drehungen liefern $e, (1\,2\,3), (1\,3\,2)$, die drei Spiegelungen liefern $(1\,2), (1\,3), (2\,3)$.

• Jede Isometrie ist durch ihre Wirkung auf die drei Ecken eindeutig bestimmt.

  ▶ Also ist $f$ injektiv.

  ▶ Außerdem wirkt $\alpha\beta$ auf die drei Ecken genau wie die Permutation $f(\alpha)f(\beta)$. Somit gilt $f(\alpha\beta) = f(\alpha)f(\beta)$. □

• Übung: Zeigen Sie, dass die Isometriegruppe des Standardsimplex $\Delta_n := \operatorname{conv}(e_1, \ldots, e_{n+1}) \subseteq \mathbb{R}^{n+1}$ isomorph zu $S_{n+1}$ ist.

- Ein *Automorphismus* einer Gruppe $G$ ist ein Isomorphismus $G \to G$.
  - Übung: Die Automorphismen bilden eine Gruppe $\mathrm{Aut}(G)$ mit Komposition.
- Für $g \in G$ ist die Abbildung $\varphi_g \colon G \to G$, $x \mapsto gxg^{-1}$, ein *innerer Automorphismus*.
  - Bijektiv: Die Umkehrabbildung ist $\varphi_{g^{-1}}$.
  - Homomorphismus: $\varphi_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi_g(x)\varphi_g(y)$.
- Verschiedene Elemente können denselben inneren Automorphismus liefern.
  - Ist $G$ abelsch, so ist $\varphi_g = \mathrm{id}_G$ für alle $g \in G$.
- Nicht jeder Automorphismus ist inner.
  - Beispiel: Für $(\mathbb{Z}, +)$ ist $n \mapsto -n$ ein Automorphismus, aber alle inneren Automorphismen sind die Identität.
- Übung: Zeigen Sie, dass $\mathrm{Aut}(\mathbb{Z}^2) \cong \mathrm{GL}(2, \mathbb{Z})$.

**Satz.** (Cayley) Jede Gruppe $G$ ist isomorph zu einer Untergruppe von $\mathrm{Bij}(G)$. Insbesondere ist jede endliche Gruppe der Ordnung $n$ isomorph zu einer Untergruppe von $S_n$.

**Beweis.** • Wir betrachten die Menge $H := \{\lambda_g \mid g \in G\}$, wobei $\lambda_g \colon G \to G$, mit $\lambda_g(x) := gx$.

- Es gilt $\lambda_g \circ \lambda_h = \lambda_{gh}$, denn $g(hx) = (gh)x$. Außerdem ist $\lambda_e = \mathrm{id}_G$ und $\lambda_g^{-1} = \lambda_{g^{-1}}$.
  - Somit ist $H$ eine Untergruppe von $\mathrm{Bij}(G)$.
- Wir zeigen, dass $f \colon G \to H$, $f(g) := \lambda_g$, ein Isomorphismus ist.
  - $f$ ist surjektiv nach Definition.
  - $f$ ist injektiv: Aus $\lambda_g = \lambda_h$ folgt $g = \lambda_g(e) = \lambda_h(e) = h$.
  - Schließlich gilt $f(gh) = \lambda_{gh} = \lambda_g \circ \lambda_h = f(g) \circ f(h)$.
- Für $|G| = n$ gilt $\mathrm{Bij}(G) \cong S_n$. □

1. Wiederholung

2. Mehr über $S_n$

3. Isomorphismen

4. Homomorphismen

- Eine Abbildung $f\colon G \to H$ zwischen Gruppen heißt *Homomorphismus*, falls $f(xy) = f(x)f(y)$ für alle $x, y \in G$.
- Übung: $f(e_G) = e_H$, $f(x^{-1}) = f(x)^{-1}$.
- Beispiele:
  - Die Signatur $\operatorname{sgn}\colon S_n \to \{1, -1\}$ ist ein Homomorphismus.
  - Die inneren Automorphismen bilden eine Untergruppe $\operatorname{Inn}(G) := \{\varphi_g \mid g \in G\} \leqslant \operatorname{Aut}(G)$. Die Abbildung $G \to \operatorname{Inn}(G)$, $g \mapsto \varphi_g$, ist ein Homomorphismus, denn für alle $g, h, x \in G$ gilt $\varphi_{gh}(x) = ghx(gh)^{-1} = g(hxh^{-1})g^{-1} = \varphi_g(\varphi_h(x))$.
  - Die Abbildung $\mathbb{Z} \to \mathbb{Z}/n$, $k \mapsto [k]$, ist ein surjektiver Homomorphismus, denn $[k + l] = [k] + [l]$.