

UNIVERSITÄT
LEIPZIG

Algebra 1

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung

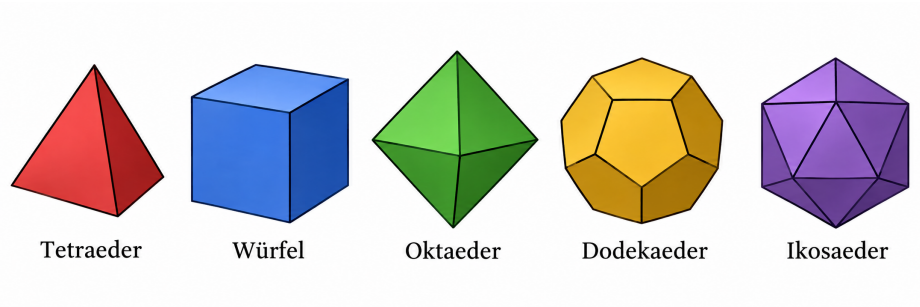
2. Erzeugendensysteme, Ordnung, zyklische Gruppen

3. Mehr über S_n

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$ für alle $a, b \in G$.
- Untergruppe, triviale Untergruppe, richtige Untegruppe

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.
- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.



- die Gruppe aller Isometrien, die einen Körper auf sich selbst abbilden.

- $\mathrm{Bij}(X)$.
- Insbesondere für $X = \{1, \ldots, n\}$: $S_n := \mathrm{Bij}(X)$.
  - Die Elemente heißen *Permutationen*.

1. Wiederholung

2. Erzeugendensysteme, Ordnung, zyklische Gruppen

3. Mehr über S_n

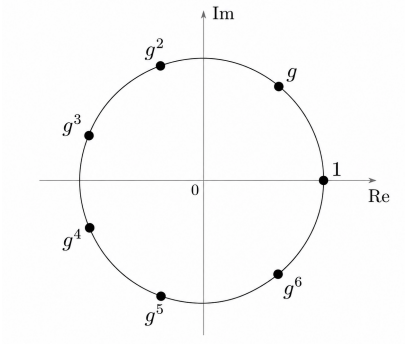
- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.
- Eine Gruppe heißt *endlich erzeugt*, falls sie ein endliches Erzeugendensystem besitzt.

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

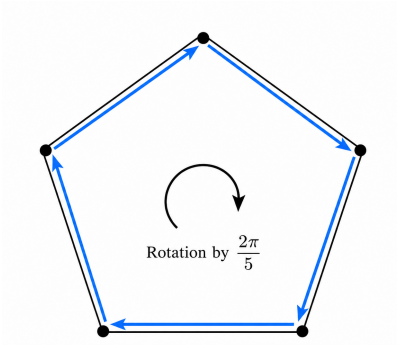
Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition modulo n ist $\mathbb{Z}/n$ eine zyklische Gruppe, erzeugt von $[1]$.

- Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden eine zyklische Gruppe mit Multiplikation.
  - Ein Erzeuger ist $e^{2\pi i/n}$.



- Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.
  - Also: Rotationen des n-Ecks.



  - G ist eine zyklische Gruppe, erzeugt von der Drehung um den Winkel $2\pi/n$.

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$ und $b \mid k - l$, also auch $ab \mid k - l$. Das bedeutet aber $k = l$.

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- 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 $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn $g^{m-n} = e$, weil wir die Gleichheit durch g^{-n} multiplizieren können.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld} g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

  ▶ Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots, g^d\}$. □

• Häufig schreibt man $\langle g \rangle = \{e, g, \ldots, g^{d-1}\}$.

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ erzeugen $\mathrm{SL}(2,\mathbb{Z})$.

1. Wiederholung

2. Erzeugendensysteme, Ordnung, zyklische Gruppen

3. Mehr über S_n

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir verwenden 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".
  - Im obigen Beispiel: $\sigma = (1\,2\,3)(4\,5)$, $\tau = (1\,2)$ und $\sigma\tau = (1\,3)(4\,5)$.

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder ...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt uns eine Darstellung von σ als Produkt paarweise disjunkter Zyklen.

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen. So erhalten wir ein Gegenbeispiel mit $k - 1$ Zyklen, Widerspruch. □

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

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

Beweis.
- Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.
- Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.
- Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.
- Die kleinste solche Zahl m ist $\mathrm{kgV}(l_1, \ldots, l_k)$. □