Rückblick auf die ersten beiden Vorlesungswochen (§ 1)

- Gruppendefinition und Beispiele
  (abelsche Gruppen als Bestandteile algebraischer Strukturen, Permutationsgruppen, lineare Gruppen, Bewegungs- und Symmetriegruppen)
- Halbgruppen und Monoide
  (Die invertierbaren Elemente eines Monoid bilden mit der eingeschränkten Verknüpfung eine Gruppe.)
- wichtiges Ziel:
  Klassifikation der Gruppen einer bestimmten Ordnung (Elementezahl)
- Potenzen in Gruppen, Rechenregeln, multiplikative und additive Schreibweise

Rückblick auf die ersten beiden Vorlesungswochen (§ 2)

- Definition der Untergruppen, Beispiele
- Definition der von einer Teilmenge $S \subseteq G$ erzeugten Untergruppe $\langle S \rangle$
- zyklische und endlich erzeugte Gruppen
- Erzeugendensysteme der Permutationsgruppen
- Äquivalenzrelationen und Zerlegungen
- Satz von Langrange: Ist G eine endliche Gruppe und U eine Untergruppe, dann ist $|U|$ ein Teiler von $|G|$.
  (Grund: Die Menge G kann in endlich viele Teilmengen zerlegt werden, die alle genauso viele Elemente besitzen wie U, nämlich in die Linksnebenklassen gU, wobei g ein Repräsentantensystem von G/U durchläuft.)

Definition (3.1)

Sei G eine Gruppe.

- Die Anzahl $|G|$ der Elemente von G wird die Ordnung von G genannt.
- Ist $g \in G$ ein beliebiges Element, dann bezeichnen wir $\operatorname{ord}(g) = |\langle g \rangle|$ als die Ordnung von g.

Aus dem Satz von Lagrange folgt unmittelbar, dass für jedes $g \in G$ einer endlichen Gruppe G die Elementordnung $\operatorname{ord}(g)$ stets ein Teiler der Gruppenordnung $|G|$ ist.

Die Elemente einer zyklischen Gruppe

Lemma (3.2)

Sei G eine Gruppe, $g \in G$ und $m \in \mathbb{N}$ mit $g^m = e_G$. Dann ist die von g erzeugte Untergruppe gegeben durch

$$\langle g \rangle \quad = \quad \{g^r \mid 0 \leq r < m\}.$$

Charakterisierung der Elementordnung

Satz (3.3)

Sei G eine Gruppe und $g \in G$ ein beliebiges Element. Dann sind für jedes $n \in \mathbb{N}$ die folgenden Aussagen äquivalent.

(i) $n = \mathrm{ord}(g)$

(ii) Es gibt ein $m \in \mathbb{N}$ mit $g^m = e_G$, und darüber hinaus ist n die minimale natürliche Zahl mit dieser Eigenschaft.

(iii) Für alle $m \in \mathbb{Z}$ gilt $g^m = e_G$ genau dann, wenn m ein Vielfaches von n ist.

Beweis von Satz 3.3

geg: Gruppe G, $g \in G$, $n \in \mathbb{N}$

z.tg: Äquivalenz der drei Aussagen

(i) $n = \mathrm{ord}(g)$ (ii) $n \in \mathbb{N}$ ist minimal mit $g^n = e$

(iii) $\forall m \in \mathbb{Z}: g^m = e \iff n \mid m$

„(i) $\Rightarrow$ (ii)" Vor.: $|\langle g \rangle| = n$ Betrachte g^j für alle $j \in \mathbb{N}$

Wegen $|\{g^j \mid j \in \mathbb{Z}\}| = n$ gibt es $j, k \in \mathbb{N}$ mit

$j < k \leq n+1$ mit $g^j = g^k \Rightarrow g^k \cdot g^{-j} = e \Rightarrow$

$g^{k-j} = e$ Daher gilt $k - j \in \mathbb{N}$ und $k - j \leq n$.

Damit ist die Existenz eines $m \in \mathbb{N}$ mit $g^m = e$, $m \leq n$ bewiesen. zur Minimalität: Ang., es gibt ein $m \in \mathbb{N}$ mit $m < n$ und $g^m = e$. Lemma 3.2 $\rightarrow \langle g \rangle = \{ g^r \mid 0 \leq r < m \}$

$\Rightarrow |\langle g \rangle| \leq m \leq n-1$ ↯ zu $|\langle g \rangle| = n$.

„(ii) $\Rightarrow$ (iii)" Vor.: $n \in \mathbb{N}$ ist minimal mit $g^n = e$.

Sei $m \in \mathbb{Z}$ s.t.q. $g^m = e \iff n \mid m$

„$\Rightarrow$" Ang., es gilt $g^m = e$, aber $n \nmid m$. Division mit Rest $\Rightarrow \exists\, q, r \in \mathbb{Z}$ mit $m = qn + r$, wobei $0 \leq r < m$.

$n \nmid m \Rightarrow r > 0$ $\quad g^r = g^{m-qn} = g^m \cdot (g^n)^{-q} = e \cdot e^{-q} = e$

also: $r \in \mathbb{N}$, $g^r = e$, $r < n$ ↯ zur Minimalität von r

„⇐" Vor. $\Rightarrow n \mid m \Rightarrow \exists k \in \mathbb{N} : m = kn$

$\Rightarrow g^m = g^{kn} = (g^n)^k = e^k = e$

„(iii) $\Rightarrow$ (i)" Vor.: $\forall m \in \mathbb{Z} : g^m = e \Leftrightarrow n \mid m$

zzg. $|\langle g \rangle| = n$ $\quad n \mid n \overset{\text{Vor.}}{\Rightarrow} g^n = e$

Lemma 3.2 $\Rightarrow \langle g \rangle = \{e, g, \dots, g^{n-1}\}$

$\Rightarrow \langle g \rangle$ ist endl. Menge. $|\langle g \rangle| \leq n$

Angenommen, es gilt $|\langle g \rangle| < n$.

Dann müssen von den Potenzen $g^0, g^1, \dots, g^{n-1}$ bereits zwei dasselbe Element liefern.

$\Rightarrow \exists j, k \in \mathbb{N}_0, 0 \leq j < k \leq n-1$ mit

$g^i = g^k \Rightarrow g^{k-i} = e$, und dabei gilt

$0 < k-i < n$ (*) $g^{k-i} = e$, Vor. (iii) $\Rightarrow$

$n \mid (k-i)$ Dies ist aber wegen (*) unmöglich.

also: $|\langle g \rangle| = n$. □

Bsp Für eine Elementordnung

Betrachte $(\mathbb{Z}/6\mathbb{Z}, +)$.

$1 \cdot \bar{1} = \bar{1} + \bar{0}$, $2 \cdot \bar{1} = \bar{1} + \bar{1} = \bar{2} \neq \bar{0}$, ...,

$5 \cdot \bar{1} = \bar{5} \neq \bar{0}$, $6 \cdot \bar{1} = \bar{6} = \bar{0} \rightarrow \text{ord}(\bar{1}) = 6$

überprüfe ebenso: $\text{ord}(\bar{2}) = 3$, $\text{ord}(\bar{3}) = 2$,

$\text{ord}(\bar{4}) = \bar{3}$, $\text{ord}(\bar{5}) = 6$

Die Elemente einer zyklischen Gruppe

Folgerung (3.4)

Sei G eine Gruppe. Besitzt $g \in G$ die endliche Ordnung n, dann sind durch

$$e_G, g, g^2, ..., g^{n-1}$$

die n verschiedenen Elemente der zyklischen Gruppe $\langle g \rangle$ gegeben.

Elemente unendlicher Ordnung

Satz (3.5)

Ist G eine Gruppe und $g \in G$, dann sind die folgenden Aussagen äquivalent.

(i) $\operatorname{ord}(g) = \infty$

(ii) Es gibt kein $n \in \mathbb{N}$ mit $g^n = e_G$.

(iii) Die Abbildung $\phi : \mathbb{Z} \to G,\ k \mapsto g^k$ ist injektiv.

Beweis von Satz 3.5

Sei G eine Gruppe. $g \in G$.

z.Zg: Äquivalenz der Aussagen

(i) $|\langle g \rangle| = \infty$ (ii) $\neg(\exists n \in \mathbb{N} : g^n = e)$

(iii) $\phi : \mathbb{Z} \to G,\ k \mapsto g^k$ ist injektiv

„(i) $\Rightarrow$ (ii)" Ang. $|\langle g \rangle| = \infty$, und es gibt ein $n \in \mathbb{N}$ mit $g^n = e$. Lemma 3.2 $\Rightarrow \langle g \rangle = \{g^r \mid 0 \leq r \leq n-1\}$

$\Rightarrow |\langle g \rangle| \leq n$ ↯ zu $|\langle g \rangle| = \infty$

„(ii) $\Rightarrow$ (iii)" Ang. (ii) ist erfüllt, aber ϕ nicht injektiv.

$\Rightarrow \exists\, i, j \in \mathbb{Z}$ mit $i < j$ und $\phi(i) = \phi(j) \Rightarrow$

$g^i = g^j \Rightarrow g^{j-i} = e$ und $j-i \in \mathbb{N}$ $\lightning$ zu (ii)

„(iii) $\Rightarrow$ (i)" ϕ injektiv $\Rightarrow$ ϕ ist eine Bijektion zwischen $\mathbb{Z}$ und $\phi(\mathbb{Z})$, und $\phi(\mathbb{Z}) \subseteq \langle g \rangle$ Mit $\mathbb{Z}$ ist auch $\phi(\mathbb{Z})$ eine unendl. Menge $\Rightarrow$ $\langle g \rangle$ enthält eine unendl. Menge

$\Rightarrow |\langle g \rangle| = \infty$ □

□

Definition von ggT und kgV

Seien $a_1, ..., a_r \in \mathbb{Z}$.

- Eine Zahl $d \in \mathbb{N}$ heißt gemeinsamer Teiler dieser Zahlen, wenn $d \mid a_k$ für $1 \leq k \leq r$ gilt.
- Man nennt d den größten gemeinsamen Teiler dieser Zahlen und schreibt $d = \text{ggT}(a_1, ..., a_r)$, wenn $d' | d$ für jeden gemeinsamen Teiler d' von $a_1, ..., a_r$ gilt.
- Zwei Zahlen a und b werden als teilerfremd bezeichnet, wenn $\text{ggT}(a, b) = 1$ ist.
- Eine natürliche Zahl $d \in \mathbb{N}$ heißt gemeinsames Vielfaches von $a_1, ..., a_r$, wenn $a_k \mid d$ für $1 \leq k \leq r$ gilt, und kleinstes gemeinsames Vielfaches (Notation $d = \text{kgV}(a_1, ..., a_r)$), wenn $d \mid d'$ für jedes gemeinsame Vielfache d' dieser Zahlen erfüllt ist.

Die Ordnung der Permutationen

Satz (3.6)

Sei $n \in \mathbb{N}$ und $\sigma \in S_n$.

(i) Ist σ ein k-Zykel ($2 \leq k \leq n$), dann gilt $\text{ord}(\sigma) = k$.

(ii) Ist σ ein Element vom Zerlegungtyp $(k_1, ..., k_r)$, dann gilt $\text{ord}(\sigma) = \text{kgV}(k_1, ..., k_r)$.

Bsp. zu Satz 3.6 (i)

$\sigma = (1\,2\,3\,4) \in S_4 \qquad \sigma^2 = (1\,3)(2\,4) \neq id$,

$\sigma^3 = (1\,4\,3\,2) \neq id$, $\sigma^4 = id \rightarrow ord(\sigma) = 4$

Bsp zu 3.6 (ii): Elemente von S_6

Zerlegungstyp	()	(2)	(3)	(4)	(5)	(6)	(2,2)	(3,2)	(4,2)	(3,3)	(2,2,2)
Beispielelement	id	(12)	(123)	(1234)	(1...5)	(1...6)	(12)(34)	(123)(45)	(1234)∘(56)	(123)∘(456)	(12)(34)(56)
Ordnung	1	2	3	4	5	6	2	6	4	3	2

Beweis von Satz 3.6

zu (i) Sei $k \in \{2, \dots, n\}$ und $\sigma = (a_1 \dots a_k)$ ein k-Zykel in S_n.

Beh.: $\forall m \in \mathbb{N}_0 \; \forall i, j \in \{1, \dots, k\} : \sigma^m(a_i) = a_j \Rightarrow i + m \equiv j \bmod k$

Beweis durch vollst. Ind. über m

Ind.-Anf. $m = 0$. geg. $i, j \in \{1, \dots, k\}$ mit $\sigma^0(a_i) = a_j$

z.zg.: $i + 0 \equiv j \bmod k$ (*) $\sigma^0(a_i) = a_j \Rightarrow \mathrm{id}(a_i) = a_j$

$\Rightarrow a_i = a_j \Rightarrow i = j$ Also ist (*) erfüllt

Ind.-Schritt $m \mapsto m+1$: geg. $i, j \in \{1, \dots, k\}$ mit $\sigma^{m+1}(a_i) = a_j$

z.zg. $i + (m+1) \equiv j \bmod k$ (Dabei darf die Aussage für m verwendet werden.) Sei $r \in \{1, \dots, k\}$ die natürliche Zahl mit der Eig. $\sigma^m(a_i) = a_r$ Ind.-V. $\Rightarrow i + m \equiv r \bmod k$

1. Fall: $r < k$ Dann gilt $a_j = \sigma^{m+1}(a_i) = \sigma(\sigma^m(a_i))$

$= \sigma(a_r) = a_{r+1}. \Rightarrow j = r+1 \Rightarrow i+m+1 \equiv r+1$

$\equiv j \mod k$

2. Fall: $r = k$ Dann gilt $a_j = \sigma^{m+1}(a_i) = \sigma(\sigma^m(a_i))$

$= \sigma(a_r) = \sigma(a_k) = a_1. \Rightarrow j = 1 \Rightarrow$

$i+(m+1) = (i+m)+1 = r+1 = k+1 \equiv 1 \equiv j \mod k$

($\Rightarrow$ Beh.)

Um z.zg., dass $\operatorname{ord}(\sigma) = k$ gilt, überprüfen wir $\sigma^l \neq \mathrm{id}$ für $l \in \mathbb{N}$ mit $l < k$ und $\sigma^k = \mathrm{id}$.

Sei $l \in \mathbb{N}$ mit $l < k$. $\sigma^l(a_1) = a_{1+l} \neq a_1$ (und $1+l \leq k$)

$\Rightarrow \sigma^l \neq \mathrm{id}$. aber: $\sigma^k(a_j) = a_j$ für $1 \leq j \leq k$ auf Grund der Beh., weil j die einzige Zahl in $\{1, \ldots, k\}$ ist.

die kongruent zu j modulo k ist. Außerdem $\sigma^l(u) = u$ für alle $u \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$. Insgesamt gilt also $\sigma^k = id$.

zu (ii) Sei $\sigma \in S_n$ ein Element vom Zerlegungstyp $(k_1, \dots, k_r)$. Sei $m = ord(\sigma)$. Überprüfe, dass m die Eigenschaften des kgV von $k_1, \dots, k_r$ hat. Schreibe dazu $\sigma = \sigma_1 \circ \dots \circ \sigma_r$, wobei σ_j jeweils ein Zykel der Länge k_j ist, mit $supp(\sigma_i) \cap supp(\sigma_j) = \emptyset$ für $i \neq j$. Wichtig: $\boxed{\sigma^l = \sigma_1^l \circ \dots \circ \sigma_r^l}$

$\forall l \in \mathbb{Z}$, da $\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i \quad \forall i, j \in \{1, \dots, r\}$

Überprüfe nun:

(1) $k_j \mid m$ für $1 \leq j \leq r$

(2) $m' \in \mathbb{N}$, $k_j \mid m'$ für $1 \leq j \leq r$

$\longrightarrow m \mid m'$

zu (1) $\operatorname{ord}(\sigma) = m \Rightarrow \sigma^m = \mathrm{id} \Rightarrow$

$(\sigma_1 \circ \dots \circ \sigma_r)^m = \mathrm{id} \Rightarrow \sigma_1^m \circ \dots \circ \sigma_r^m = \mathrm{id}$

Da die Träger der σ_i^m paarweise disj. sind, folgt damit $\sigma_i^m = \mathrm{id}$ für $1 \leq i \leq r$

Teil (i) $\Rightarrow \operatorname{ord}(\sigma_i) = k_i$ (jeweils für $1 \leq j \leq m$)

Satz 3.3 (iii) $\Rightarrow$ $\sigma_m = \mathrm{id}$ $k_j \mid m$

zu (2) Sei m' wie angeg $\quad k_j \mid m' \Rightarrow \exists\, l_j \in \mathbb{N}$

mit $m' = k_j \cdot l_j$ $\quad \sigma^{m'} = (\sigma_1 \circ \dots \circ \sigma_r)^{m'} =$

$\sigma_1^{m'} \circ \dots \circ \sigma_r^{m'} = \sigma_1^{k_1 l_1} \circ \dots \circ \sigma_r^{k_r l_r}$

$= (\sigma_1^{k_1})^{l_1} \circ \dots \circ (\sigma_r^{k_r})^{l_r} = id^{l_1} \circ \dots \circ id^{l_r} = id$

$\uparrow \sum \operatorname{ord}(\sigma_j) = k_j$

$\Rightarrow \sigma_j^{k_j} = id$

Satz 3.3.

$\Rightarrow \operatorname{ord}(\sigma) \mid m' \Rightarrow m \mid m'$. $\square$