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 $\mathrm{ord}(g) = |\langle g \rangle|$ als die Ordnung von g.

Aus dem Satz von Lagrange folgt unmittelbar: Ist $n = |G|$ endlich, dann ist $\mathrm{ord}(g)$ für jedes $g \in G$ stets ein Teiler von n.

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

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

Beweis von Lemma 3.2

gegeben: Gruppe G, $g \in G$, $m \in \mathbb{N}$ mit $g^m = e$

Beh.: $\langle g \rangle = \{e, g, \dots, g^{m-1}\}$

bekannt: $\langle g \rangle = \{g^a \mid a \in \mathbb{Z}\}$, also z.zg.

$\{g^a \mid a \in \mathbb{Z}\} = \{g^a \mid 0 \le a \le m-1\}$

„$\supseteq$" offensichtlich „$\subseteq$" Sei $a \in \mathbb{Z}$ z.zg.: $\exists r \in \{0, 1, \dots, r-1\}$ mit $g^a = g^r$. Division mit Rest $\Rightarrow$ $\exists q, r \in \mathbb{Z}$ mit $\boxed{a = qm + r}$ und $0 \le r < m-1$.

$\Rightarrow g^a = g^{qm+r} = g^{qm} \cdot g^r = (g^m)^q \cdot g^r = e^q \cdot g^r = g^r$ $\square$

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.

Beispiele für Elementordnungen

ii) In $(\mathbb{Z}/n\mathbb{Z}, +)$ ist $\bar{1}$ ein Element der Ordnung n, denn: $1 \leq k \leq n-1$

$\Rightarrow k \cdot \bar{1} = \bar{k} \neq \bar{0}$ (Neutralelt. der Gruppe)

aber: $n \cdot \bar{1} = \bar{n} = \bar{0}$ also: n ist die kleinste nat. Zahl mit $n \cdot \bar{1} = \bar{0}$

Satz 3.3 (ii) $n = \mathrm{ord}(\bar{1})$

Ordnung von $\bar{2}$ in $(\mathbb{Z}/5\mathbb{Z}, +)$:

$1 \cdot \bar{2} = \bar{2} \neq \bar{0}$, $2 \cdot \bar{2} = \bar{4} \neq \bar{0}$, $3 \cdot \bar{2} = \bar{6} \neq \bar{0}$, $4 \cdot \bar{2} = \bar{8} = \bar{3} \neq \bar{0}$, $5 \cdot \bar{2} = \bar{10} = \bar{0}$

also: $\operatorname{ord}(\bar{2}) = 5$ in $(\mathbb{Z}/5\mathbb{Z}, +)$

$\operatorname{ord}(\bar{0}) = 1$ in $(\mathbb{Z}/5\mathbb{Z}, +)$

(allgem.: $\operatorname{ord}(e_G) = 1$ in jeder Gruppe G)

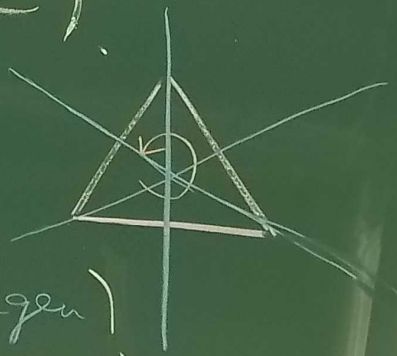
(ii) $D_\alpha = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$ Drehmatrix

Es gilt $\operatorname{ord}(D_{2\pi/n}) = n$ für jedes $n \in \mathbb{N}$ in der Gruppe $O(2)$.

(iii) Elemente von D_3

$|D_3| = 6$

1 Element der Ordn. 1 ($= E_2$)
3 Elemente der Ordnung 2 (Spiegelungen)
2 Elemente der Ordnung 3 (Drehungen)



Beweis von Satz 3.3

geg.: Gruppe G, $g \in G$, $n \in \mathbb{N}$, z.zg.: Äquivalenz der drei Aussagen i) $|\langle g \rangle| = n$

ii) n ist die kleinste nat. Zahl mit $g^n = e$

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

„i) $\Rightarrow$ ii)" Betrachte die Elemente $g^1, g^2, g^3, \ldots$ aus $\langle g \rangle$. Da $\langle g \rangle$ n.V. eine endliche Menge ist, muss es $i, j \in \mathbb{N}$ mit $i < j$ und $g^i = g^j$ geben. Annahme: i, j sind minimal mit dieser Eigenschaft. Wegen $|\langle g \rangle| = n$ muss $1 \leq i < j \leq n+1$ gelten. $g^i = g^j \Rightarrow g^{-i} \cdot g^i = g^{-i} \cdot g^j \Rightarrow e = g^{j-i}$, und $j - i \leq n$. Ang., es gilt

$j - i < n$. Dann folgt aus Lemma 3.2 und g^{j-i}, dass $\langle g \rangle$ höchstens $j-i$ verschiedene Elemente besitzt. $\lightning$ zu $|\langle g \rangle| = n$

also: $g^n = e$, und n ist minimal mit dieser Eigenschaft

„(ii) $\Rightarrow$ (iii)" Setze (ii) voraus. Sei $m \in \mathbb{Z}$.

„$\Leftarrow$": $n \mid m \Rightarrow \exists k \in \mathbb{Z}$ mit $m = kn$

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

„$\Rightarrow$" Ang.: $g^m = e$, aber n ist kein Teiler von m. Division mit Rest $\rightarrow \exists q, r \in \mathbb{Z}$

mit $m = qn + r$ und $1 \leq r \leq n-1$

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

↯ zur Minimalität von n also: $n \mid m$

„(iii) $\Rightarrow$ (i)" Setze (iii) voraus. z.Zg.: $|\langle g \rangle| = n$

$n \mid n \Rightarrow g^n = e \overset{\text{Lemma 3.2}}{\Rightarrow}$ $\langle g \rangle$ enthält höchstens n verschiedene Elemente, d.h. $|\langle g \rangle| \leq n$

Ang. $|\langle g \rangle| < n$ Wie im ersten Schritt sieht man, dass es dann $1 \leq i < j \leq n$ mit $g^i = g^j$ geben muss $\overset{\text{s.o.}}{\Rightarrow} g^{j-i} = e$, $1 \leq j-i < n$

$\Rightarrow n$ kein Teiler von $j-i$ ↯ zu (iii) für $m = j-i$ □

Die Elemente einer zyklischen Gruppe

Folgerung (3.4)

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

$$e_G, g, g^2, \ldots, g^{n-1}$$

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.

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 $d = \mathrm{ggT}(a_1, ..., a_r)$, wenn $d' | d$ für jeden gemeinsamen Teiler d' von $a_1, ..., a_r$ gilt.
- Zwei Zahlen a und b werden als teilerfremd bezeichnet, wenn $\mathrm{ggT}(a, b) = 1$ 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 $d = \mathrm{kgV}(a_1, ..., a_r)$), 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 $\mathrm{ord}(\sigma) = k$.

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

Beweis von Satz 3.6:

zu i) geg. $n \in \mathbb{N}$, $k \in \{2, 3, \dots, n\}$, $\sigma \in S_n$ k-Zykel
d.h. $\sigma = (a_1\, a_2 \dots a_k)$ mit $a_1, \dots, a_k \in M_n$ verschieden
z.zg.: $\operatorname{ord}(\sigma) = k$ in S_n

zeige durch vollst. Ind. über $m \in \mathbb{N}_0$:
Sind $r, j \in \{1, \dots, k\}$ mit $\sigma^m(a_r) = a_j$,
dann gilt $r + m \equiv j \mod k$.

Ind_Anf.: geg. $r, j \in \{1, \dots, k\}$ mit $\sigma^0(a_r) = a_j$
$\Rightarrow a_r = a_j \Rightarrow r = j \Rightarrow r + 0 \equiv j \mod k$

Ind.-Schritt $m \mapsto m+1$: Sei $r \in \{1, \dots, k\}$, und $j \in \{1, \dots, k\}$ gegeben durch $\sigma^m(a_r) = a_j$. Ind.-V. $\Rightarrow$ $r + m \equiv j \bmod k$.

1. Fall: $j < k \Rightarrow \sigma^{m+1}(a_r) = \sigma(\sigma^m(a_r)) = \sigma(a_j)$
$= a_{j+1}$, und es gilt $r + (m+1) \equiv j+1 \bmod k$

2. Fall: $j = k \Rightarrow \sigma^{m+1}(a_r) = \sigma(\sigma^m(a_r)) = \sigma(a_j)$
$= \sigma(a_k) = a_1$, und $r + (m+1) \equiv j+1 \equiv k+1$
$\equiv 1 \bmod k$ ($\Rightarrow$ Ind.-Beweis fertig)

Zeige nun, dass k die kleinste nat. Zahl mit $\sigma^k = id$ ist. Ist $m < k$ und $j \in \{1, \dots, k\}$ mit $\sigma(a_1) = a_j$.

dann gilt $1+m \equiv j \bmod k$ und $1+m \not\equiv 1 \bmod k$

wegen $k \geq 2$) $\Rightarrow j \neq 1 \Rightarrow a_1 \neq a_j \Rightarrow$

$\sigma \neq id$

Dagegen gilt für $1 \leq r \leq k$. Ist $\sigma^k(a_r) = a_j$,

dann gilt $r+k \equiv j \bmod k \Rightarrow j \equiv r \bmod k$

$\Rightarrow j = r \Rightarrow \sigma^k(a_r) = a_r$

$j, r \in \{1, \ldots, k\}$

Also werden $a_1, \ldots, a_k$ durch σ^k auf sich abgebildet, die Elemente aus $\{a_1, \ldots, a_k\}$ natürlich auch $\Rightarrow \sigma^k = id$

insgesamt: $ord(\sigma) = k$

zu i)

zu ii)

zu (iv) Sei $\sigma \in M_n$ ein Element vom Zerlegungstyp $(k_1, \dots, k_r) \Rightarrow \exists \sigma_1, \dots, \sigma_r \in S_n$ mit $\sigma = \sigma_1 \circ \dots \circ \sigma_r$, σ_j ist k_j-Zykel für $1 \le j \le r$, σ_i, σ_j disjunkt für $j \neq i$

Daraus folgt, dass für diese i, j jeweils $\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i$ gilt, d.h. die Elemente sind vertauschbar. Daraus wiederum folgt

$$\boxed{\sigma^m = \sigma_1^m \circ \dots \circ \sigma_r^m \quad \forall m \in \mathbb{Z}.}$$

Da $\sigma_1, \dots, \sigma_r$ paarweise disjunkt sind, gilt auch:

$\sigma^m = id \iff \sigma_j^m = id$ für $1 \le j \le r$

mod k

⇒

$= a_j$,

mod k

ch als -

$\ldots a_k$?

Zeige man, dass $n = \operatorname{ord}(\sigma)$ die definierenden Eigenschaften der Zahl $\operatorname{kgV}(k_1, \ldots, k_r)$ besitzt.

überprüfe: i) $k_j \mid n$ für $1 \leq j \leq r$

ii) Ist m ein gemeinsames Vielfaches von $k_1, \ldots, k_r$, dann folgt $n \mid m$.

zu i) $n = \operatorname{ord}(\sigma) \overset{(3.3)}{\Longrightarrow} \sigma^n = \mathrm{id} \overset{5.0}{\Longrightarrow}$

$\sigma_j^n = \mathrm{id}$ für $1 \leq j \leq r \overset{(3.3)}{\Longrightarrow} \operatorname{ord}(\sigma_j) \mid n$

für $1 \leq j \leq r \overset{\text{ii)}}{\Longrightarrow} k_j \mid n$ für $1 \leq j \leq n$

zu ii) $k_j \mid m$ für $1 \leq j \leq r \overset{\text{i)}}{\Longrightarrow}$

für $1 \leq j \leq r$ $\Rightarrow$ $k_j \mid n$ für $1 \leq j \leq n$

$\operatorname{ord}(\alpha_j) \mid m$ für $1 \leq j \leq n$ $\overset{(3.3)}{\Rightarrow}$

$\alpha_j^m = \mathrm{id}$ für $1 \leq j \leq n$ $\Rightarrow$

$\alpha^m = \alpha_1^m \circ \dots \circ \alpha_r^m = \mathrm{id}$ $\overset{3.3}{\Rightarrow}$

$\operatorname{ord}(\alpha) \mid m \Rightarrow k \mid m$