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.

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

geg.: G Gruppe, $g \in G$, $m \in \mathbb{N}$ mit $g^m = e_G$

Beh.: $\langle g \rangle = \{ g^r \mid 0 \leq r < m \}$ $(\Rightarrow |\langle g \rangle| \leq m)$

„$\supseteq$" klar, da $\langle g \rangle = \{ g^a \mid a \in \mathbb{Z} \}$

„$\subseteq$" Sei $h \in \langle g \rangle$ $\Rightarrow \exists a \in \mathbb{Z}$ mit $h = g^a$

Division mit Rest $\Rightarrow \exists q, r \in \mathbb{Z}$ mit $a = qm + r$ und $0 \leq r < m$ Es gilt $h = g^a = g^{qm+r}$

$= (g^{qm}) \cdot g^r = (g^m)^q \cdot g^r = e_G^q \cdot g^r = g^r$ $\square$

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.

Beweis von Satz 3.3

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

Äquivalenz der Aussagen (i) $|\langle g \rangle| = n$

(ii) n ist die kleinste natürliche Zahl mit $g^n = e$

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

„(i) $\Rightarrow$ (ii)" Betrachte die Elemente $g^1 = g, g^2, g^3, g^4, \ldots$

Diese liegen alle in $\langle g \rangle$. Weil es in $\langle g \rangle$ nur n verschiedene Elemente gibt, existieren $i, j \in \mathbb{N}$ mit $i < j \leq n+1$ und $g^i = g^j \Rightarrow g^j g^{-i} = e \Rightarrow g^{j-i} = e$ Es gilt $j - i \in \mathbb{N}$ und $j - i \leq n$. Angenommen, für $m = j - i$

gilt $m < n$ $g^m = e$ $\xrightarrow{\text{Lemma 3.2}}$

$\langle g \rangle = \{ g^r \mid 0 \leq r < m \} \rightarrow |\langle g \rangle| \leq m < n$

↯ zu (i) $|\langle g \rangle| = n$ Also ist $j - i = n$,

es gilt $g^n = e$, und es gibt kein $m \in \mathbb{N}$

mit $g^m = e$ und $m < n$

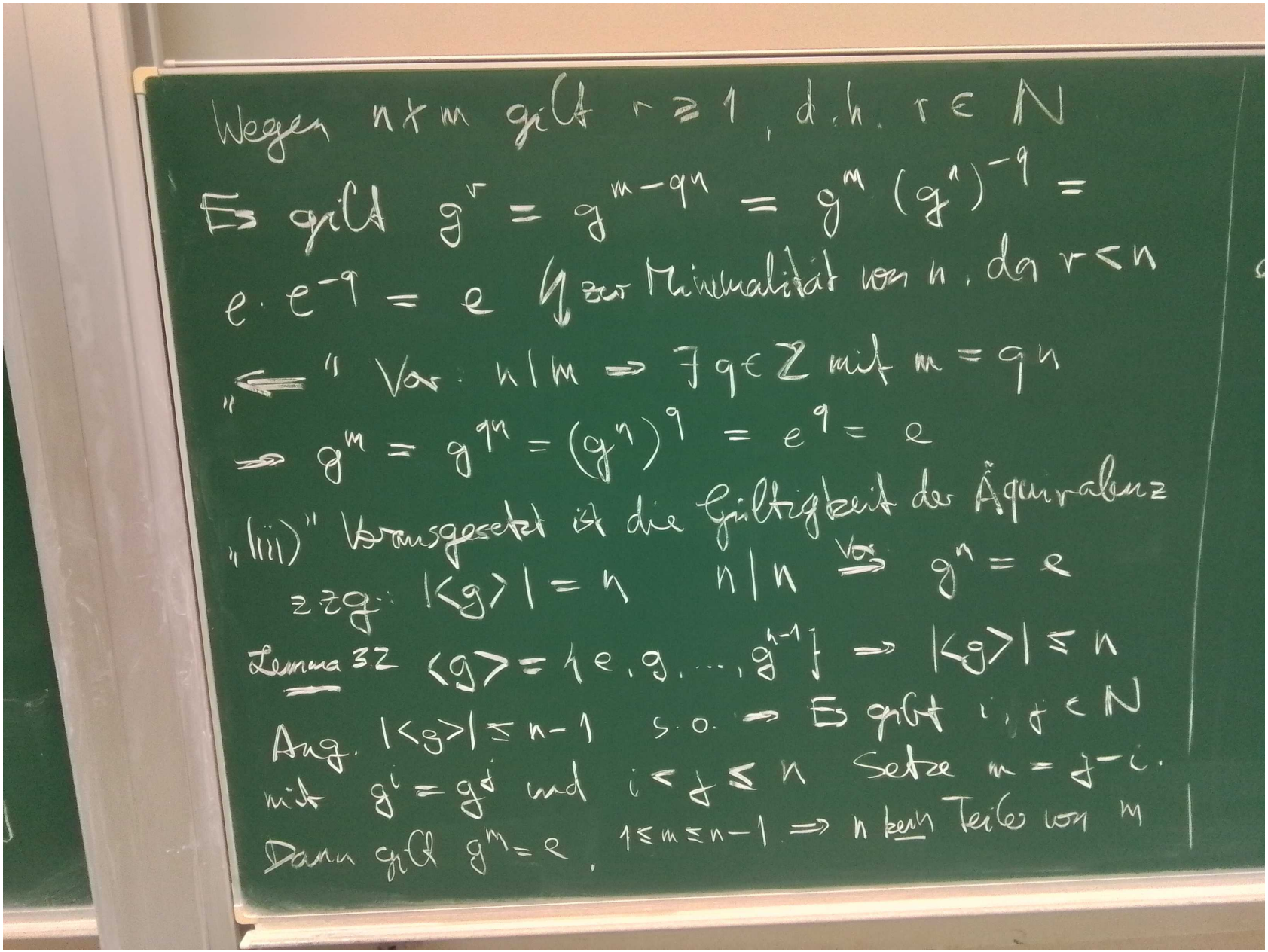
„(ii) $\Rightarrow$ (iii)" Voraussetzung: $n \in \mathbb{N}$ minimal

mit $g^n = e$. z.zg. ist die Äquivalenz

Sei $m \in \mathbb{Z}$. „$\Rightarrow$" Vor.: $g^m = e$,

ang. $n \nmid m$ Division mit Rest $\Rightarrow$

$\exists q, r \in \mathbb{Z}$ mit $m = qn + r$, $0 \leq r < n$



Korrektur: in der sechsten Zeile ersetze „(iii)“ durch „(iii) $\Rightarrow$ (i)“

Auf Grund des Kr. folgt aus $g^m = e$ aber, dass $n \mid m$. $\lightning$ also: Annahme war falsch, es gilt $|\langle g \rangle| = n$ $\square$

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.

Beweis von Satz 3.5

geeg.: G Gruppe, $g \in G$

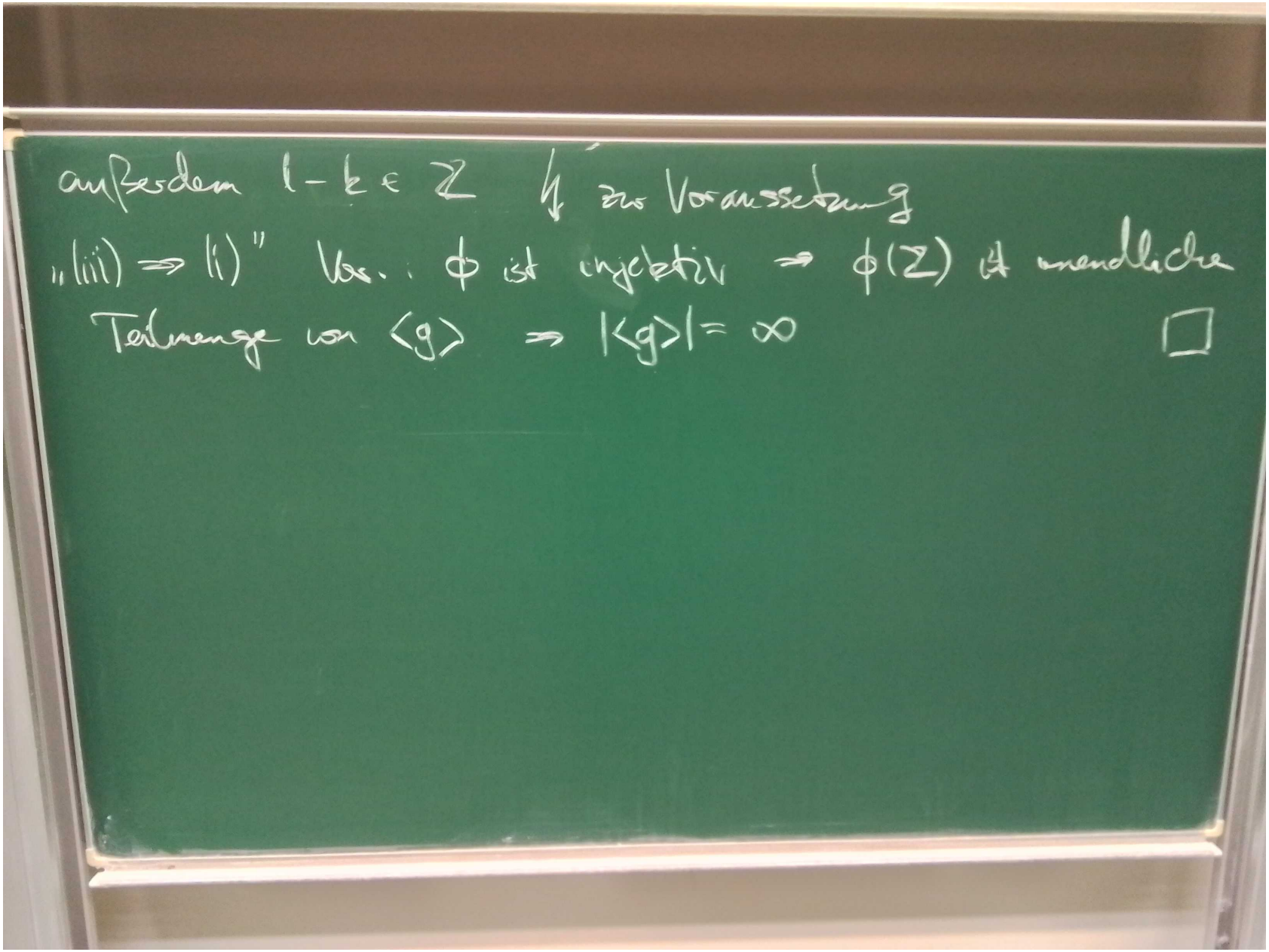
z.zg.: Äquivalenz der Aussagen

(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)" Vor. $|\langle g \rangle| = \infty$, ang. $\exists n \in \mathbb{N}$ mit $g^n = e \overset{\text{Lemma 3.2}}{\Longrightarrow} |\langle g \rangle| \leq n$, widerspr. $\langle g \rangle$ endl. $\lightning$

„(ii) $\Rightarrow$ (iii)" Vor.: $g^n \neq e\ \forall n \in \mathbb{N}$ Ang. ϕ ist nicht inj. $\Rightarrow \exists k, l \in \mathbb{Z}, k < l$ mit $\phi(k) = \phi(l) \Rightarrow g^k = g^l \Rightarrow g^{l-k} = e$



Korrektur: in der ersten Zeile ersetze $\ell - k \in \mathbb{Z}$ durch $\ell - k \in \mathbb{N}$

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

$\rightarrow$ $\exists\, a_1, \dots, a_k \in M_n$, alle verschieden, mit $\sigma = (a_1\ a_2 \dots a_k)$

z.zg: $\operatorname{ord}(\sigma) = k$

Beh: Für alle $i, j \in \{1, \dots, k\}$ und $m \in \mathbb{N}_0$ mit

$\sigma^m(a_i) = a_j$ gilt $i + m \equiv j \mod k$ (*)

Zeige (*) durch vollst. Ind. über m.

$m = 0$ z.zg: $\sigma^0(a_i) = a_j \Rightarrow i \equiv j \mod k$ $\forall i, j \in \{1, \dots, k\}$

$\sigma^0(a_i) = a_j \Rightarrow a_i = a_j \Rightarrow i = j \Rightarrow i \equiv j \mod k$

$m = 0$ zzg.: $\sigma^0(a_i) = a_j \Rightarrow i \equiv j \bmod k$ $\forall i,j \in \mathbb{N}$

$\sigma^0(a_i) = a_j \Rightarrow a_i = a_j \Rightarrow i = j \Rightarrow i \equiv j \bmod k$

$m \mapsto m+1$ Setze die Aussage für m voraus

Voraussetzung außerdem: $\sigma^{m+1}(a_i) = a_j$

zzg: $i + m + 1 \equiv j \bmod k$

Sei $j_0 \in \{1, \dots, k\}$ gegeben durch $\sigma^m(a_i) = a_{j_0}$

Ind.-V. $\Rightarrow i + m \equiv j_0 \bmod k$

1 Fall: $j_0 < k \Rightarrow a_j = \sigma^{m+1}(a_i) = \sigma(\sigma^m(a_i)) = \sigma(a_{j_0})$

$= a_{j_0+1} \Rightarrow j = j_0 + 1 \Rightarrow j \equiv j_0 + 1 \equiv i + m + 1 \bmod k$

2. Fall: $j_0 = k \Rightarrow a_j = \sigma^{m+1}(a_i) = \sigma(\sigma^m(a_i)) = \sigma(a_{j_0})$

$= \sigma(a_k) = a_1 \Rightarrow j = 1 \Rightarrow i + m + 1 \overset{\text{s.o.}}{\equiv} j_0 + 1 \equiv$

$k + 1 \equiv 1 \equiv j \bmod k$ ($\Rightarrow$ Beh)

Zeige nun, $\operatorname{ord}(\sigma) = k$, gleichbedeutend nach Satz 3.3: k ist die kleinste natürliche Zahl mit $\sigma^k = id$

Sei $r \in \mathbb{N}$ mit $r < k \Rightarrow \sigma^r(a_1) = a_{r+1} \neq a_1 \Rightarrow \sigma^r \neq id$ andererseits:

Für $1 \leq i \leq r$ gilt $\sigma^k(a_i) = a_j$, wobei $j \in \{1, \dots, k\}$ eind. best. durch $i + k \equiv j \bmod k$

also $i \equiv j \bmod k$ (siehe Beh.)

$i, j \in \{1, \dots, k\}$, $i \equiv j \bmod k \Rightarrow i = j$

$\rightarrow \sigma^k(a_i) = a_i$ für $1 \leq i \leq k \Rightarrow \sigma^k = id$

zu (ii) Sei $\sigma \in S_n$ vom Zerlegungstyp $(m_1, \dots, m_r)$

Sei $d = \operatorname{ord}(\sigma)$. Zeige: d erfüllt die definierenden Eigenschaften von $\operatorname{kgV}(m_1, \dots, m_r)$

dafür zu überprüfen: (1) $m_k \mid d$ für $1 \le k \le r$

(2) Ist $d' \in \mathbb{N}$ mit $m_k \mid d'$ für $1 \le k \le r$, dann folgt $d \mid d'$

Sei $\sigma = \sigma_1 \circ \dots \circ \sigma_r$, wobei σ_i m_i-Zykel für $1 \le i \le r$, σ_i, σ_j disjunkt für $j \neq i$.

$d = \operatorname{ord}(\sigma) \Rightarrow \sigma^d = \mathrm{id} \Rightarrow (\sigma_1 \circ \dots \circ \sigma_r)^d = \mathrm{id}$

$= \sigma_1^d \circ \dots \circ \sigma_r^d = \mathrm{id}$ Weil $\sigma_1^d, \dots, \sigma_r^d$

$\Sigma \sigma_i, \sigma_j$ vertauschbar für $i \neq j$

paarweise disj. Träger haben, folgt $\sigma_i^d = id$

für $1 \le i \le r$ $\quad \sigma_i^d = id$, $\operatorname{ord}(\sigma_i) = m_i \overset{\text{Satz 3.3}}{\Longrightarrow} m_i \mid d$

(für $1 \le i \le r$)

zu (2) Sei $d' \in \mathbb{N}$ mit $m_i \mid d'$ für $1 \le i \le r$

$m_i \mid d'$, $\operatorname{ord}(\sigma_i) = m_i \overset{\text{Satz 3.3}}{\Longrightarrow} \sigma_i^{d'} = id$

$\Rightarrow \sigma^{d'} \overset{\text{s.o.}}{=} \sigma_1^{d'} \circ \sigma_2^{d'} \circ \dots \circ \sigma_r^{d'} = id \circ id \circ \dots \circ id = id$

$\sigma^{d'} = id$, $d = \operatorname{ord}(\sigma) \overset{\text{Satz 3.3}}{\Longrightarrow} d \mid d'$ $\square$

Die Untergruppen einer zyklischen Gruppe, Teil I

Satz (3.7)

Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer gilt: Sei G eine zyklische Gruppe, g ein Element mit $G = \langle g \rangle$ und U eine Untergruppe $\neq \{e_G\}$. Dann gibt es ein $m \in \mathbb{N}$ mit

$$U \quad = \quad \langle g^m \rangle.$$

Ist $\mathrm{ord}(g) = n$ endlich, dann kann die Zahl m so gewählt werden, dass sie ein Teiler von n ist.

Beweis von Satz 3.7:

geg.: zyklische Gruppe G, $g \in G$ mit $G = \langle g \rangle$

$U \leq G$ mit $U \neq e_G$

Beh.: $\exists\, m \in \mathbb{N}$ mit $g^m \in U$

$G = \{g^a \mid a \in \mathbb{Z}\}$ $\quad U \neq \{e_G\} \rightarrow \exists\, a \in \mathbb{Z} \setminus \{0\}$

mit $g^a \in U$ 1. Fall: $a > 0 \Rightarrow$ setze $m = a$

2. Fall: $a < 0$ $\quad g^a \in U$, $U \leq G \rightarrow (g^a)^{-1} \in U$

$\rightarrow g^{-a} \in U$, $-a > 0 \Rightarrow$ setze $m = -a$

Dann ist $g^m \in U$ und $m \in \mathbb{N}$ in jedem Fall erfüllt.

Sei nun $m \in \mathbb{N}$ minimal mit $g^m \in U$.

Beh.: $U = \langle g^m \rangle$ „$\supseteq$" klar, aus $g^m \in U$ folgt $\langle g^m \rangle \subseteq U$

„$\subseteq$" Sei $h \in U \Rightarrow h \in \langle g \rangle \Rightarrow \exists a \in \mathbb{Z}$ mit $h = g^a$

Division mit Rest $\Rightarrow \exists q, r \in \mathbb{Z}$ mit $a = qm + r$ und

$0 \leq r < m$. 1. Fall: $r = 0 \Rightarrow a = qm \Rightarrow h = g^a = g^{qm}$

$= (g^m)^q \in \langle g^m \rangle$ 2. Fall: $1 \leq r < m$ $g^r = g^{a - qm} =$

$g^a \cdot (g^m)^{-q} \in U$ ↯ zur Minimalität von m.

$\in U$ $\in U$

(Fall ord (g) endlich: nächste Stunde)