Rückblick auf die bisher behandelte Gruppentheorie

§ 1. Definition der Gruppen, Beispiele

- Grundbegriffe:
  Halbgruppen, Monoide, Gruppen, Isomorphie von Gruppen
- Beispiele:
  Permutationsgruppen, lineare Gruppen, Symmetriegruppen

§ 2. Untergruppen und der Satz von Lagrange

- Jeder Teilmenge S einer Menge G kann eine Untergruppe $\langle S \rangle$ zugeordnet werden. wichtige Regel:
  $V \leq G$, $S \subseteq V \Rightarrow \langle S \rangle \subseteq V$
- Satz von Langrange:
  Ist G eine endliche Gruppe und $U \leq G$,
  dann ist $|U|$ ein Teiler von $|G|$.

§ 3. Elementordnungen und die Struktur zyklischer Gruppen

- Ist G eine Gruppe, $g \in G$ und $n \in \mathbb{N}$ mit $g^n = e$, dann ist $\operatorname{ord}(g)$ ein Teiler von n. Gilt zusätzlich $g^{n/p} \neq e$ für jeden Primteiler p von n, dann ist $\operatorname{ord}(g) = n$.
- Ist $\operatorname{ord}(g)$ bekannt, dann lässt sich $\operatorname{ord}(g^a)$ für jedes $a \in \mathbb{Z}$ berechnen.
- Ist G eine endliche zyklische Gruppe, dann gibt es für jeden Teiler d von $|G|$ genau eine Untergruppe $U \leq G$ mit $|U| = d$.
- Unter den endlichen Gruppen sind die zyklischen die einzigen mit dieser Eigenschaft. Die Gruppe A_4 der Ordnung 12 hat beispielsweise drei verschiedene Untergruppen der Ordnung 2 und vier verschiedene Untergruppen der Ordnung 3, aber keine Untergrupppe der Ordnung 6.

§ 4. Gruppenhomomorphismen

Definition (4.1)

Sind $(G, *)$ und $(H, \circ)$ Gruppen, so bezeichnet man eine Abbildung $\phi : G \to H$ als Gruppenhomomorphismus, wenn $\phi(g * g') = \phi(g) \circ \phi(g')$ für alle $g, g' \in G$ gilt.

Spezielle Arten von Homomorphismen

Definition (4.3)

Seien $(G, *)$ und $(H, \circ)$ Gruppen und $\phi : G \to H$ ein Homomorphismus von Gruppen. Man bezeichnet ϕ als

(i) Monomorphismus, wenn ϕ injektiv

(ii) Epimorphismus, wenn ϕ surjektiv

(iii) Isomorphismus, wenn ϕ bijektiv ist.

Zwei Gruppen G und H sind also genau dann zueinander isomorph, wenn ein Isomorphismus $\phi : G \to H$ existiert.

Ergänzungen zum Homomorphismus-Begriff

- Einen Gruppen-Homomorphismus $\phi : G \to G$ von $(G, \cdot)$ nach $(G, \cdot)$ bezeichnet man als Endomorphismus von G.
- Ist die Abbildung ϕ außerdem bijektiv, dann spricht man von einem Automorphismus der Gruppe G.
- Die Menge der Endomorphismen bezeichnen wir mit $\mathrm{End}(G)$, die der Automorphismen mit $\mathrm{Aut}(G)$.

Die Automorphismen als invertierbare Elemente

Sei $(G, \cdot)$ eine Gruppe.

- Sind $\phi_1, \phi_2 \in \mathrm{End}(G)$, dann auch $\phi_1 \circ \phi_2$.
- Die Verknüpfung $\circ$ auf $\mathrm{End}(G)$ erfüllt das Assoziativgesetz.
- Außerdem gilt $\phi_1 \circ \mathrm{id}_G = \mathrm{id}_G \circ \phi_1 = \phi_1$ für alle $\phi_1 \in \mathrm{End}(G)$. Also ist $(\mathrm{End}(G), \circ)$ ein Monoid.

Proposition (4.6)

Die invertierbaren Elemente in $\mathrm{End}(G)$ sind genau die Automorphismen der Gruppe G.

Die Automorphismengruppe einer Gruppe

Aus der Tatsache, dass die invertierbaren Elemente eines Monoids eine Gruppe bilden, folgt nun

Satz (4.7)

Die Automorphismen einer Gruppe G bilden mit der Verknüpfung $\circ$ selbst eine Gruppe. Man nennt sie die Automorphismengruppe $\mathrm{Aut}(G)$ der Gruppe G.

Ergänzung:

Ist $\phi : G \to H$ ein Isomorphismus von Gruppen, dann gilt dasselbe für die Umkehrabbildung $\phi^{-1} : H \to G$.

Erhaltung von Untergruppen unter Homomorphismen

Proposition (4.8)

Sei $\phi : G \to H$ ein Gruppenhomomorphismus, außerdem U eine Untergruppe von G und V eine Untergruppe von H. Dann gilt

(i) Die Bildmenge $\phi(U)$ ist eine Untergruppe von H.

(ii) Die Urbildmenge $\phi^{-1}(V)$ ist eine Untergruppe von G.

Beweis von Proposition 4.8

zu (i) zu überprüfen (0) $e_H \in \phi(U)$ (1) $\forall h, h' \in \phi(U)$: $hh' \in \phi(U)$, $h^{-1} \in \phi(U)$

zu (0) $U \leq G \Rightarrow e_G \in U$

$\Rightarrow e_H = \phi(e_G) \in \phi(U)$

zu (1) Seien $h, h' \in \phi(U)$. $\Rightarrow \exists u, u' \in U : h = \phi(u)$

und $h' = \phi(u')$ $U \leq G$, $u, u' \in U \longrightarrow uu', u^{-1} \in U$

$\Rightarrow hh' = \phi(u)\phi(u') = \phi(uu') \in \phi(U)$ und

$h^{-1} = \phi(u)^{-1} = \phi(u^{-1}) \in \phi(U)$

zu (ii) zu Erinnerung: $\phi^{-1}(V) = \{ g \in G \mid \phi(g) \in V \}$

zu überprüfen: (0) $e_G \in \phi^{-1}(V)$ (1) $\forall g, g' \in \phi^{-1}(V) : gg', g^{-1} \in \phi^{-1}(V)$

zu (0) $V \leq H \Rightarrow e_H \in V \Rightarrow \phi(e_G) = e_H \in V \Rightarrow e_G \in \phi^{-1}(V)$

zu (1) Seien $g, g' \in \phi^{-1}(V) \Rightarrow \phi(g), \phi(g') \in V \overset{V \leq H}{\Longrightarrow}$

$\phi(g)\phi(g') \in V$ und $\phi(g)^{-1} \in V \Rightarrow \phi(gg') \in V$ und $\phi(g^{-1}) \in V$

$\Rightarrow gg' \in \phi^{-1}(V)$ und $g^{-1} \in \phi^{-1}(V)$ $\square$

Kern und Bild eines Homomorphismus

Eine besonders wichtige Rolle spielen in der Gruppentheorie der Kern $\ker(\phi) = \phi^{-1}(\{e_H\})$ und das Bild $\mathrm{im}(\phi) = \phi(G)$ eines Gruppenhomomorphismus.

Proposition (4.9)

Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Die Abbildung ϕ ist genau dann injektiv, wenn $\ker(\phi) = \{e_G\}$ gilt.

Beweis von Proposition 4.9.

„⇐" Vor.: $\ker(\phi) = \{e_G\}$ zzg.: ϕ ist injektiv

Seien $g, g' \in G$ mit $\phi(g) = \phi(g')$ zzg.: $g = g'$

$\phi(g) = \phi(g') \Rightarrow \phi(g')\,\phi(g)^{-1} = e_G \Rightarrow \phi(g'g^{-1}) = e_G$

$\Rightarrow g'g^{-1} \in \ker(\phi) \overset{\text{Vor.}}{\Rightarrow} g'g^{-1} = e_G \Rightarrow g' = g$

„⇒" Vor.: ϕ ist injektiv zzg: $\ker(\phi) = \{e_G\}$

„⊇" ist erfüllt, da $\ker(\phi) \leq G$

„⊆" Sei $g \in \ker(\phi) \Rightarrow \phi(g) = e_H = \phi(e_G) \overset{\text{Vor.}}{\Rightarrow} g = e_G$

$\Rightarrow g \in \{e_G\}$.

□

Eindeutigkeit von Homomorphismen

Satz (4.10)

Seien G, H Gruppen und $S \subseteq G$ ein Erzeugendensystem von G. Sind $\phi, \phi' : G \to H$ Gruppenhomomorphismen mit

$$\phi(s) = \phi'(s) \quad \text{für alle } s \in S \quad ,$$

dann folgt $\phi = \phi'$.

Beweis von Satz 4.10:

geg: Gruppen G, H, $S \subseteq G$ mit $G = \langle S \rangle$

$\phi, \phi' : G \to H$ Gruppenhom. mit $\phi|_S = \phi'|_S$

(d.h. $\phi(s) = \phi'(s)$ $\forall s \in S$) (*)

Beh.: $\phi = \phi'$

Betrachte in G die Teilmenge

$$U = \{ g \in G \mid \phi(g) = \phi'(g) \}.$$

zeige: (1) $U \leq G$ (2) $U \supseteq S$

(Dann folgt $U \supseteq \langle S \rangle = G$, also $U = G$

und somit $\phi(g) = \phi'(g)$ $\forall g \in G$, d.h. $\phi = \phi'$.

zu (1) überprüfe (i) $e_G \in U$ (ii) $\forall u, u' \in U: uu', u^{-1} \in U$

zu (i) $\phi(e_G) = e_H = \phi'(e_G) \Rightarrow e_G \in U$

zu (ii) Seien $u, u' \in U$. $\Rightarrow \phi(u) = \phi'(u)$ und $\phi(u') = \phi'(u')$. $\Rightarrow \phi(uu') = \phi(u)\phi(u') = \phi'(u)\phi'(u') = \phi'(uu') \Rightarrow uu' \in U$

$\phi(u^{-1}) = \phi(u)^{-1} = \phi'(u)^{-1} = \phi'(u^{-1})$

$\Rightarrow u^{-1} \in U$.

zu (2) folgt nach Def. von U direkt aus (*).

□

Verhalten der Elementordnung unter Homomorphismen

Proposition (4.11)

Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Ist $g \in G$ ein Element von endlicher Ordnung n, dann ist auch $\text{ord}(\phi(g))$ endlich, und ein Teiler von n.

Beweis von Proposition 4.11:

geg: Gruppenhom. $\phi: G \to H$, $n \in \mathbb{N}$, $g \in G$
mit $n = \operatorname{ord}(g)$

z.z.g. $\operatorname{ord}(\phi(g)) \mid n$ (insb.: $\operatorname{ord}(\phi(g))$ ist endlich)

$n = \operatorname{ord}(g) \Rightarrow g^n = e_G \Rightarrow \phi(g)^n = \phi(g^n) = \phi(e_G)$
$= e_H \overset{\text{Satz 3.3}}{\Longrightarrow} \operatorname{ord}(\phi(g))$ ist endlich, und $\operatorname{ord}(\phi(g)) \mid n$.

□

Existenz von Homomorphismen auf zyklischen Gruppen

Proposition (4.12)

Sei G eine zyklische Gruppe, $g \in G$ ein erzeugendes Element, H eine weitere Gruppe und $h \in H$. Ist

- $\operatorname{ord}(g) = \infty$ oder
- $\operatorname{ord}(g)$ endlich und ein Vielfaches von $\operatorname{ord}(h)$,

dann existiert ein (eindeutig bestimmter) Gruppenhomomorphismus $\phi : G \to H$ mit $\phi(g) = h$.

Folgerung (4.13)

Je zwei unendliche zyklische Gruppen sind isomorph. Ebenso sind zwei endliche zyklische Gruppen derselben Ordnung isomorph.

Zusammen mit Satz 2.22 (i) folgt daraus: Für jede Primzahl p ist $(\mathbb{Z}/p\mathbb{Z}, +)$ bis auf Isomorphie die einzige Gruppe der Ordnung p.

$k = \mathrm{ord}(g) \Rightarrow g^k = e_G \Rightarrow \phi(g) = \phi(g^k) = \phi(e_G)$

$= e_H \overset{\text{Satz 3.3}}{\Longrightarrow}$ $\mathrm{ord}(\phi(g))$ ist endlich, und $\mathrm{ord}(\phi(g)) \mid n$.

Beweis von Prop 4.12

geg: Gruppen G, H, $g \in G$ mit $G = \langle g \rangle$, $h \in H$ ein Element, das die angeg. Bedingung erfüllt

Die Eindeutigkeit eines Hom. $\phi: G \to H$ mit $\phi(g) = h$ folgt direkt aus Satz 4.10. zu Existenz:

1. Fall: $\mathrm{ord}(g) = \infty$

Dann hat jedes Element in G eine eindeutige Darstellung in der Form g^a mit $a \in \mathbb{Z}$. Wir können somit eine Abb. $\phi: G \to H$ definieren durch $\phi(g^a) = h^a \quad \forall a \in \mathbb{Z}$. Offenbar gilt $\phi(g) = \phi(g^1) = h^1 = h$.

noch zzg: ϕ ist ein Gruppenhom. Seien $g', g'' \in G$. z.z. $\phi(g'g'') = \phi(g')\phi(g'')$. $G = \langle g \rangle \Rightarrow \exists a, b \in \mathbb{Z}$ mit $g' = g^a$, $g'' = g^b$.

$\Rightarrow \phi(g' g'') = \phi(g^a \cdot g^b) = \phi(g^{a+b}) =$

$h^{a+b} = h^a \cdot h^b = \phi(g^a) \cdot \phi(g^b)$

2. Fall: $n = \operatorname{ord}(g)$ mit $n \in \mathbb{N}$

Dann sind g^k mit $0 \leq k < n$ die n verschiedenen Elemente von $G = \langle g \rangle$. Definiere $\phi: G \to H$ durch $\phi(g^k) = h^k$ für $0 \leq k < n$.

Beh.: $\phi(g^a) = h^a \quad \forall a \in \mathbb{Z}$

Sei $a \in \mathbb{Z}$. Dividiere a durch n mit Rest.

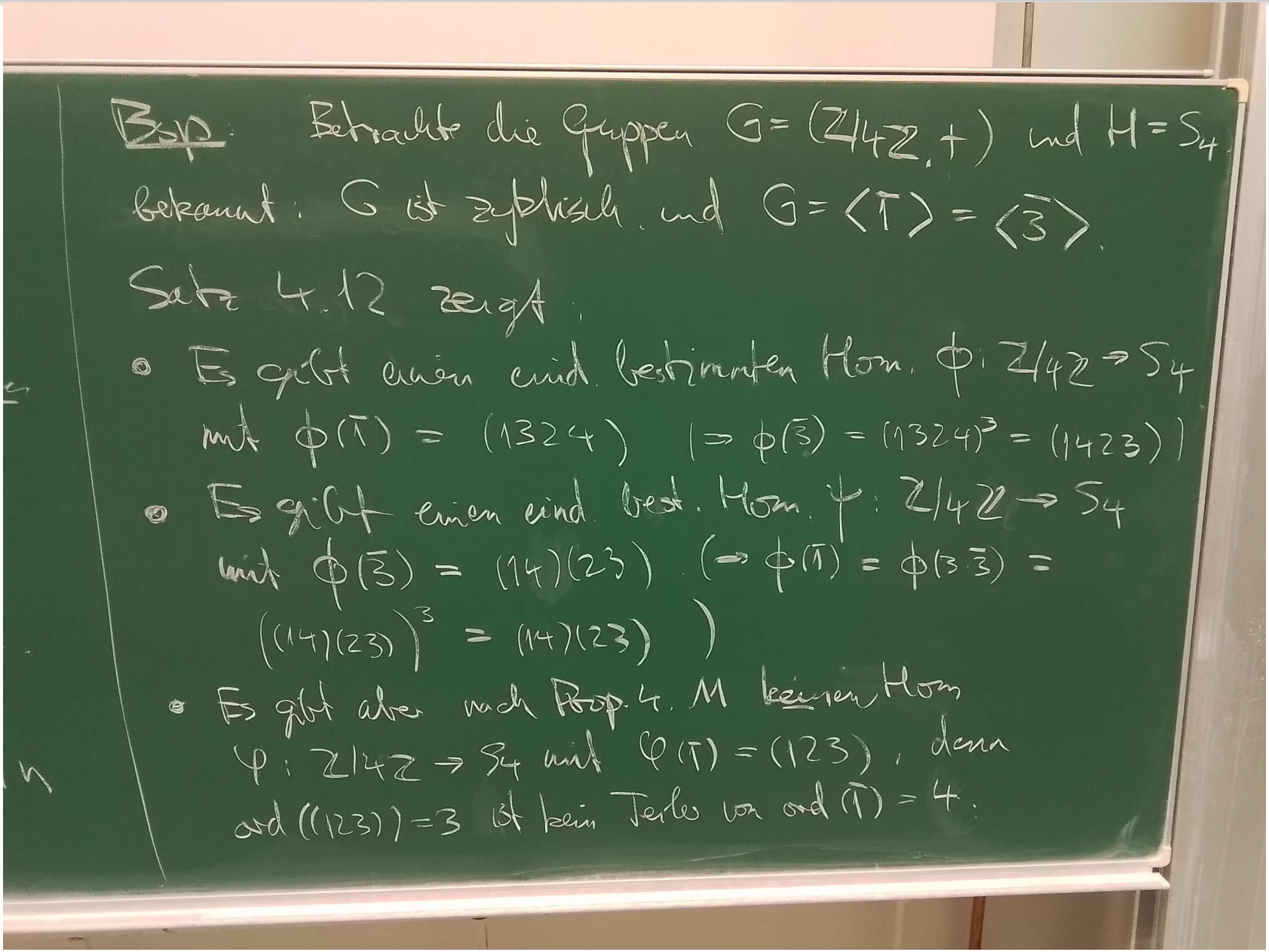
$\Rightarrow \exists q \in \mathbb{Z}, r \in \{0, \ldots, n-1\}$ mit $a = qn + r$.

$\operatorname{ord}(g) = n \Rightarrow g^n = e_G$ Vor. $\Rightarrow \operatorname{ord}(h) \mid n$

$\Rightarrow h^n = e_H$, erhalte nun

$$\phi(g^q) = \phi(g^{qn+r}) = \phi((g^n)^q \cdot g^r) =$$
$$\phi(e_G^q \cdot g^r) = \phi(g^r) = h^r = e_H^q \cdot h^r =$$
$$(h^n)^q \cdot h^r = h^{qn+r} = h^a$$

Wie im 1. Fall kann man nun nachrechnen, dass ϕ ein Gruppenhomomorphismus ist. $\square$



Korrektur: Im mittleren Punkt • muss es natürlich $\psi(\bar{3}) = (1\ 4)(2\ 3)$ und $\psi(\bar{1}) = (1\ 4)(2\ 3)$ heißen.

Die primen Restklassengruppen

Nach § 1 bildet die Teilmenge $(\mathbb{Z}/n\mathbb{Z})^\times$ der invertierbaren Elemente im Monoid $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ eine Gruppe. Man bezeichnet sie als prime Restklassengruppe.

Proposition (4.14)

Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Das Element $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann in $(\mathbb{Z}/n\mathbb{Z})^\times$ enthalten, wenn $\mathrm{ggT}(a, n) = 1$ ist.

Beweis von Proposition 4.14:

„⇒" geg: $a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, mit $a \in \mathbb{Z}$ z.zg: $ggT(a,n)=1$

$a+n\mathbb{Z}$ invertierbar $\Rightarrow \exists b \in \mathbb{Z}$ mit $(a+n\mathbb{Z})\cdot(b+n\mathbb{Z}) = 1+n\mathbb{Z}$

$\Rightarrow ab+n\mathbb{Z} = 1+n\mathbb{Z} \Rightarrow ab \equiv_n 1 \Rightarrow n \mid (ab-1)$

$\Rightarrow \exists k \in \mathbb{Z}: nk = ab-1 \Rightarrow 1 = ab+(-k)n$

Sei nun $d \in \mathbb{N}$ ein gem. Teiler von a und n. $\Rightarrow d \mid (ab+(-k)n)$

$\Rightarrow d \mid 1 \Rightarrow d = 1$ also: $ggT(a,n)=1$

„⇐" $ggT(a,n)=1$ Lemma von Bézout $\Rightarrow \exists k,l \in \mathbb{Z}$ mit

$ak+ln=1 \Rightarrow ak \equiv_n 1 \Rightarrow ak+n\mathbb{Z} = 1+n\mathbb{Z} \Rightarrow$

$(a+n\mathbb{Z})(k+n\mathbb{Z}) = 1+n\mathbb{Z} \Rightarrow a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times \quad (a+n\mathbb{Z})^{-1} = k+n\mathbb{Z}$ □

Anwendungsbeispiele zu Prop 4.14:

- $(\mathbb{Z}/5\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$
- $(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$
- $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.