

Überblick §4: Homomorphismen und Faktorgruppen

- Definition der **Gruppenhomomorphismen**
- Struktur der Automorphismengruppe $\text{Aut}(G)$ für eine zyklische Gruppe G
- Definition der **Normalteiler** ($N \trianglelefteq G$)
- Komplexprodukte von Untergruppen
($NU = \{nu \mid n \in N, u \in U\}$), innere direkte Produkte
- Definition der **Faktorgruppe** G/N ($N \trianglelefteq G$)
- Homomorphiesatz $G/N \cong H$, falls $\phi : G \rightarrow H$ Epimorphismus und $N = \ker(\phi)$, Isomorphiesätze als Folgerung
- Korrespondenzsatz (Untergruppenstruktur von G/N vs. Untergruppenstruktur von G)

Definition der Gruppenhomomorphismen

Definition (4.1)

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

Lemma (4.2)

Sei ϕ ein Homomorphismus zwischen den Gruppen $(G, *)$ und $(H, \circ)$. Dann gilt

$$\phi(e_G) = e_H \quad \text{und} \quad \phi(g^{-1}) = \phi(g)^{-1} \quad \text{für alle } g \in G.$$

Spezielle Arten von Homomorphismen

Definition (4.3)

Seien $(G, *)$ und $(H, \circ)$ Gruppen und $\phi : G \rightarrow H$ 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 $\phi : G \rightarrow H$ existiert.

- Einen Gruppen-Homomorphismus $\phi : G \rightarrow G$ 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 $\text{End}(G)$, die der Automorphismen mit $\text{Aut}(G)$.

Die Automorphismen als invertierbare Elemente

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

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

Proposition (4.6)

Die invertierbaren Elemente in $\text{End}(G)$ 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** $\text{Aut}(G)$ der Gruppe G .

Ergänzung:

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

Proposition (4.8)

Sei $\phi : G \rightarrow H$ 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.

geg. Gruppenhom. $\phi: G \rightarrow H$, $U \leq G$, $V \leq H$

zu (1) z.zg. $\phi(U) \leq H$ zu überprüfen:

$$(1) e_H \in \phi(U) \quad (2) \forall h, h' \in \phi(U): hh' \in \phi(U), h^{-1} \in \phi(U)$$

zu (1) $U \leq G \Rightarrow e_G \in U \Rightarrow e_H = \phi(e_G) \in \phi(U)$

zu (2) Seien $h, h' \in \phi(U) \rightarrow \exists u, u' \in U$ mit $\phi(u) = h, \phi(u') = h'$

$$u, u' \in U, U \leq G \Rightarrow uu' \in U, u^{-1} \in U$$

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

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

$$\text{und } u = \phi(u) = \phi(u^{-1}) \in \phi(u)$$

zu (ii) Nach Def gilt $\phi^{-1}(V) = \{g \in G \mid \phi(g) \in V\}$

zu überprüfen (1) $e_G \in \phi^{-1}(V)$ (2) $\forall g, g' \in \phi^{-1}(V) : gg', g^{-1} \in \phi^{-1}(V)$

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

zu (2) Seien $g, g' \in \phi^{-1}(V)$. Dann gilt $\phi(g), \phi(g') \in V$

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

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

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

□

Kern und Bild eines Homomorphismus

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

Proposition (4.9)

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

Beweis von Proposition 4.9

geg. Gruppenhom. $\phi: G \rightarrow H$

Beh.: ϕ ist injektiv $\iff \ker(\phi) = \{e_G\}$

" $\implies$ " Von ϕ injektiv " $\Leftarrow$ " ist offensichtlich,
da $\ker(\phi)$ eine Untergruppe von G ist

" $\Leftarrow$ " Sei $g \in \ker(\phi)$, z.z.zg: $g = e_G$

Es gilt $\phi(g) = e_H = \phi(e_G) \xRightarrow{\phi \text{ inj.}} g = e_G$
 $\uparrow$ da $g \in \ker(\phi)$

" $\Leftarrow$ " Seien $g, g' \in G$ mit $\phi(g) = \phi(g') \implies$
 $\phi(g')\phi(g)^{-1} = e_H \implies \phi(g'g^{-1}) = e_H \implies g'g^{-1} \in \ker(\phi)$
 $\ker(\phi) = \{e_G\} \implies g'g^{-1} = e_G \implies g = g'$ $\square$

Satz (4.10)

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

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

dann folgt $\phi = \phi'$.

Beweis von Satz 4.10

geg. Gruppenhom. $\phi, \phi' : G \rightarrow H$

$S \subseteq G$ mit $G = \langle S \rangle$

Es gelte $\phi|_S \stackrel{(*)}{=} \phi'|_S$, d.h. $\phi(s) = \phi'(s) \quad \forall s \in S$

z.zg. $\phi = \phi'$

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

Dann gilt $U \supseteq S$ wegen (*), z.zg. ist $U = G$.

Beh. U ist eine Untergruppe von G

Aus $S \subseteq U$ und der Beh. folgt $\langle S \rangle \subseteq U$,
wegen $G = \langle S \rangle$ also auch $U = G$.

Für den Beweis der Beh. müssen wir überprüfen

□

$$(1) e_G \in U \quad (2) \forall g, h \in U: gh, g^{-1} \in U$$

zu (1) $\phi(e_G) = e_H = \phi'(e_G) \Rightarrow e_G \in U$

zu (2) Seien $g, h \in U \Rightarrow \phi(g) = \phi'(g), \phi(h) = \phi'(h)$

$$\Rightarrow \phi(gh) = \phi(g)\phi(h) = \phi'(g)\phi'(h) = \phi'(gh)$$

$$\Rightarrow gh \in U, \text{ ebenso: } \phi(g^{-1}) = \phi(g)^{-1} = \phi'(g)^{-1} =$$

$$\phi'(g^{-1}) \Rightarrow g^{-1} \in U$$



Proposition (4.11)

Sei $\phi : G \rightarrow H$ 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 Prop. 4.11:

geg.: Gruppenhom. $\phi: G \rightarrow H$, $g \in G$ ein
Element der endlichen Ordnung n

z.zg.: $\text{ord}(\phi(g))$ ist endlich und ein Teiler von n

$$\text{ord}(g) = n \Rightarrow g^n = e_G \Rightarrow \phi(g)^n = \phi(g^n) =$$

$$\phi(e_G) = e_H \quad \underline{\text{Satz 3.3}} \quad \text{ord}(\phi(g)) \text{ ist endlich,}$$

und es gilt $\text{ord}(\phi(g)) \mid n$.



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

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

dann existiert ein (eindeutig bestimmter) Gruppenhomomorphismus $\phi : G \rightarrow H$ 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 **einzigste** Gruppe der Ordnung p .

Beweis von Proposition 4.12

geg. Gruppen G, H , $g \in G$, $h \in H$, wobei $G = \langle g \rangle$

1. Fall: $\text{ord}(g) = \infty$ z.zg. Es gibt einen Hom. $\phi: G \rightarrow H$ mit $\phi(g) = h$. (Die Eindeichtigkeit folgt aus Satz 4.10.)
Wegen $\text{ord}(g) = \infty$ gibt es (siehe Satz 3.5) für jedes $g_1 \in G$ ein eindeutig bestimmtes $a_1 \in \mathbb{Z}$ mit $g_1 = g^{a_1}$. Definiere dann $\phi(g_1) = h^{a_1}$. Dann gilt offenbar $\phi(g) = \phi(g^1) = h^1 = h$. Außerdem ist ϕ ein Gruppenhom., denn: Seien $g_1, g_2 \in \langle g \rangle$ und $a_1, a_2 \in \mathbb{Z}$ mit $g_1 = g^{a_1}$, $g_2 = g^{a_2}$, dann

$g_1, g_2 \in \langle g \rangle$ und $a_1, a_2 \in \mathbb{Z}$ mit $g_1 = g^{a_1}$, $g_2 = g^{a_2}$, dann

$$\text{folgt } \phi(g_1 g_2) = \phi(g^{a_1 + a_2}) = h^{a_1 + a_2} = h^{a_1} h^{a_2} = \phi(g_1) \phi(g_2)$$

2. Fall: $\text{ord}(g) = n$ für ein $n \in \mathbb{N}$

In diesem Fall gibt es für jedes $g_i \in \langle g \rangle$ ein eindeutig bestimmtes $a_i \in \{0, 1, \dots, n-1\}$ mit $g_i = g^{a_i}$. Sei nun $h \in H$ wie im Satz angegeben, also mit $\text{ord}(h) \mid n$. Bilde dann g^{a_i} für $0 \leq a_i \leq n-1$ jeweils auf

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

Wegen $\text{ord}(g) = n$, $\text{ord}(h) \mid n$ gilt $g^n = e_G$, $h^n = e_H$.

Sei nun $a \in \mathbb{Z}$. Division mit Rest $\Rightarrow \exists q, r \in \mathbb{Z}$ mit $a = qn + r$ und $r \in \{0, 1, \dots, n-1\}$. Aus der Def. von ϕ folgt $\phi(g^r) = h^r$.

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

Mit derselben Rechnung wie im 1. Fall folgt nun,
dass ϕ ein Gruppenhom. ist. $\square$

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 $\text{ggT}(a, n) = 1$ ist.

Beweis von Proposition 4.14:

geg. $n \in \mathbb{N}$, $a \in \mathbb{Z}$

Beh. $a+n\mathbb{Z}$ ist invertierbar im
Monoid $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ $\Leftrightarrow \text{ggT}(a, n) = 1$
(kurz: $a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$)

" $\Leftarrow$ " $\text{ggT}(a, n) = 1 \xRightarrow{\text{Bezout}} \exists k, l \in \mathbb{Z} \text{ mit } ka + ln = 1$

$$\rightarrow (k+n\mathbb{Z})(a+n\mathbb{Z}) + (l+n\mathbb{Z})(\underbrace{n+n\mathbb{Z}}_{=0+n\mathbb{Z}}) = 1+n\mathbb{Z}$$

$$\Rightarrow (k+l\mathbb{Z})(a+n\mathbb{Z}) = 1+n\mathbb{Z}$$

$$\Rightarrow a+n\mathbb{Z} \text{ ist invertierbar, } (a+n\mathbb{Z})^{-1} = k+n\mathbb{Z}$$

" $\Rightarrow$ " $a+n\mathbb{Z}$ ist invertierbar in $(\mathbb{Z}/n\mathbb{Z}, \cdot)$

$$\Rightarrow \exists k \in \mathbb{Z} \text{ mit } (k+n\mathbb{Z})(a+n\mathbb{Z}) = 1+n\mathbb{Z}$$

$$\Rightarrow ka+n\mathbb{Z} = 1+n\mathbb{Z} \Rightarrow ka \equiv 1 \pmod{n}$$

$$\Rightarrow n \mid (1-ka) \Rightarrow \exists l \in \mathbb{Z} : nl = 1-ka$$

$$\Rightarrow ka+ln = 1 \quad \text{Sei } d \in \mathbb{N} \text{ ein gemeinsamer Teiler}$$

$$\text{von } a \text{ und } n. \Rightarrow d \mid (ka+ln) \Rightarrow d \mid 1 \Rightarrow d = 1$$

Also sind a und n teilerfremd. $\square$

Anwendungsbeispiele:

$$(1) (\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$$

$$(2) (\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$$

Struktur der Automorphismengruppen zyklischer Gruppen

Sei nun G eine zyklische Gruppe der endlichen Ordnung n und $g \in G$ mit $G = \langle g \rangle$. Für jedes $a \in \mathbb{Z}$ existiert ein eindeutig bestimmter Endomorphismus

$$\tau_a : G \rightarrow G \quad \text{mit} \quad \tau_a(g) = g^a.$$

Satz (4.15)

Die Abbildung $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(G)$, $a + n\mathbb{Z} \mapsto \tau_a$ ist ein Isomorphismus von Gruppen.

Im Fall, dass $G = \langle g \rangle$ **unendlich** ist, gilt $\text{Aut}(G) \cong (\mathbb{Z}/2\mathbb{Z}, +)$.

Beweis von Satz 4.15:

Zeige zunächst, dass eine Abb. $\phi: (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(G)$,
 $a+n\mathbb{Z} \mapsto \tau_a$ existiert, mit $\tau_a(g) = g^a$.

Definiere $\phi: (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{End}(G)$ durch $\phi(a+n\mathbb{Z}) = \tau_a$
für alle $a \in \mathbb{Z}$ mit $0 \leq a < n$ und $\text{ggT}(a, n) = 1$.

$\text{ggT}(a, n) = 1 \xRightarrow{\text{siehe §3}} \text{ord}(\tau_a(g)) = \text{ord}(g^a) = n$

$\Rightarrow \langle \tau_a(g) \rangle = G \Rightarrow \tau_a$ ist surjektiv $\xRightarrow{G \text{ ist unendliche Menge}} \tau_a$ ist injektiv

$\Rightarrow \tau_a$ ist bijektiv, also $\tau_a \in \text{Aut}(G)$

noch zu überprüfen: (1) Es gilt $\phi(a+n\mathbb{Z}) = \tau_a$ für
alle $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$.

$$\text{ggT}(a, n) = 1 \xLeftrightarrow{\text{Steuer}} \text{ord}(\tau_a(g)) = \text{ord}(g) = n$$

$$\Rightarrow \langle \tau_a(g) \rangle = G \Rightarrow \tau_a \text{ ist surjektiv} \xLeftrightarrow{G \text{ ist}} \tau_a \text{ ist injektiv}$$

(2) ϕ ist ein Gruppenhomomorphismus $(\mathbb{Z}/n\mathbb{Z})^* \rightarrow \text{Aut}(G)$

(3) ϕ ist injektiv (4) ϕ ist surjektiv

zu (1) Sei $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$. Division mit Rest $\Rightarrow \exists q, r \in \mathbb{Z}$

$$\text{mit } a = qn + r, 0 \leq r < n \quad \text{ggT}(a, n) = 1 \Rightarrow \text{ggT}(r, n) = 1$$

$$\text{s.o.} \Rightarrow \phi(r + n\mathbb{Z}) = \tau_r \quad \text{Es genügt somit, } \tau_a = \tau_r \text{ zu}$$

$$\text{überprüfen, denn } \phi(a + n\mathbb{Z}) = \phi(r + n\mathbb{Z}) \quad \tau_a(g) = g^a =$$

$$g^{qn+r} = (g^n)^q \cdot g^r = g^r = \tau_r(g) \quad \xLeftrightarrow{G = \langle g \rangle} \tau_a = \tau_r$$

Eindeutigkeit
Satz 4.10