

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)

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 $\text{Aut}(G) \cong (\mathbb{Z}/2\mathbb{Z}, +)$. Die beiden Automorphismen sind gegeben durch $g \mapsto g$ und $g \mapsto g^{-1}$.

Beweis von Satz 4.15 (Abschluss)

bereits bekannt: • $\forall a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$: $\tau_a \in \text{Aut}(G)$
(wobei τ_a geg. durch $\tau_a(g) = g^a$)

• Es gibt eine Abb. $\phi: (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \text{Aut}(G)$ mit
 $\phi(a+n\mathbb{Z}) = \tau_a$ für alle $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$.

noch zu überprüfen: (2) ϕ ist Gruppenhom.

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

zu (2) z.zg. $\phi((a+n\mathbb{Z})(b+n\mathbb{Z})) = \phi(a+n\mathbb{Z}) \circ \phi(b+n\mathbb{Z})$

gleichbedeutend: $\phi(ab+n\mathbb{Z}) = \phi(a+n\mathbb{Z}) \circ \phi(b+n\mathbb{Z})$

bzw. $\tau_{ab} = \tau_a \circ \tau_b$, jeweils für alle $a, b \in \mathbb{Z}$ mit
 $\text{ggT}(a, n) = \text{ggT}(b, n) = 1$.

Seien also $a, b \in \mathbb{Z}$ vorgeg., beide teilerfremd zu n .

Wegen $G = \langle g \rangle$, genügt es z.zg., dass $\tau_{ab}(g) = (\tau_a \circ \tau_b)(g) \in \langle g \rangle$.

$$\text{Tatsächlich ist } (\tau_a \circ \tau_b)(g) = \tau_a(g^b) = \tau_a(g)^b = (g^a)^b \\ = g^{ab} = \tau_{ab}(g).$$

zu (3) genügt z.zg.: $\ker(\phi) \subseteq \{1+n\mathbb{Z}\}$. Sei $a+n\mathbb{Z} \in \ker(\phi)$.

$$\text{mit } a \in \mathbb{Z}, g \cdot \tau(a, n) = 1 \Rightarrow \phi(a+n\mathbb{Z}) = \text{id}_G \Rightarrow \tau_a = \text{id}_G$$

$$\Rightarrow \tau_a(g) = \text{id}_G(g) \Rightarrow g^a = g \Rightarrow g^a g^{-1} = e_G \Rightarrow g^{a-1} = e_G$$

$$\text{Satz 3.3} \Rightarrow n \mid (a-1) \Rightarrow a \equiv 1 \pmod{n} \Rightarrow a+n\mathbb{Z} = 1+n\mathbb{Z}$$

$$\Rightarrow a+n\mathbb{Z} \in \{1+n\mathbb{Z}\}$$

zu (4) Sei $\tau \in \text{Aut}(G)$ z.zg.: $\exists a \in \mathbb{Z}, g \cdot \tau(a, n) = 1$ mit $\phi(a+n\mathbb{Z}) = \tau$

$$\tau(g) \in \langle g \rangle \Rightarrow \tau(g) = g^a \text{ für ein } a \in \mathbb{Z} \Rightarrow \forall k \in \mathbb{Z}: \tau(g^k) =$$

$$\tau(g)^k = (g^a)^k \Rightarrow \tau(G) \subseteq \langle g^a \rangle \xRightarrow{\tau \text{ bijektiv}} \tau(G) = G, G = \langle g^a \rangle$$

$$\Rightarrow \text{ord}(g^a) = |\langle g^a \rangle| = |G| = n \xrightarrow{\S 3} \frac{n}{\text{ggT}(a, n)} = n$$

$$\Rightarrow \text{ggT}(a, n) = 1 \Rightarrow \phi(a + n\mathbb{Z}) = \tau_a = \tau,$$

und $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

zu

Erz

bi(a

z.zg

1. Fall

2. Fall

und a

∃ disj.

Definition (4.16)

Sei G eine Gruppe. Eine Untergruppe U von G wird **Normalteiler** von G genannt, wenn $gU = Ug$ für alle $g \in G$ gilt.

Notation: Sei G eine Gruppe.

- $U \leq G$ bedeutet: U ist Untergruppe von G
- $N \trianglelefteq G$ bedeutet: N ist Normalteiler von G

Proposition (4.17)

Sei G eine Gruppe und U eine Untergruppe. Dann sind die folgenden Bedingungen äquivalent:

- (i) U ist Normalteiler von G .
- (ii) Es gilt $gUg^{-1} \subseteq U$ für alle $g \in G$, wobei $gUg^{-1} = \{gug^{-1} \mid u \in U\}$ ist.
- (iii) Es gilt $gUg^{-1} = U$ für alle $g \in G$.

Beweis von Prop. 4.17:

geg: Gruppe G , $U \leq G$ z.zg: Äquivalenz der drei Aussagen
i) $U \trianglelefteq G$ ii) $\forall g \in G: gUg^{-1} \subseteq U$
iii) $\forall g \in G: gUg^{-1} = U$

"i) $\Rightarrow$ ii)" Sei $g \in G$. z.zg: $gUg^{-1} \subseteq U$

Sei $h \in gUg^{-1} \Rightarrow \exists u \in U: h = gug^{-1}$

Vor. i) $\Rightarrow gU = Ug \quad gu \in gU \Rightarrow gu \in Ug$

$\Rightarrow \exists u' \in U$ mit $gu = u'g \Rightarrow h = (u'g)g^{-1} = u'$

$\Rightarrow h \in U$

"ii) $\Rightarrow$ iii)" Sei $g \in G$. z.zg: $gUg^{-1} = U$

" $\subseteq$ " gilt auf Grund der Vor. ii) " $\supseteq$ " Sei $u \in U$.

Wende (ii) auf $g^{-1}u$ an. $\Rightarrow g^{-1}U(g^{-1})^{-1} \subseteq U$

der $\Rightarrow g^{-1}Ug \subseteq U \Rightarrow g^{-1}ug \in U$

$\subseteq U \Rightarrow u = g(g^{-1}ug)g^{-1} \in gUg^{-1}$

"(iii) $\Rightarrow$ (i)" Sei $g \in G$. z.z.g: $gU = Ug$

" $\subseteq$ " Sei $h \in gU$. $\rightarrow \exists u \in U$ mit $h = gu$

$gug^{-1} \in gUg^{-1} \stackrel{(iii)}{\Rightarrow} gug^{-1} \in U \rightarrow$

$h = gug^{-1}g \in Ug$

" $\supseteq$ " Sei $h \in Ug$. $\rightarrow \exists u \in U$ mit $h = ug$

(iii) $\Rightarrow g^{-1}U(g^{-1})^{-1} = U \rightarrow g^{-1}Ug = U$

$\Rightarrow g^{-1}ug \in U \rightarrow h = gg^{-1}ug \in gU$ □

Satz (4.18)

- (i) Ist G eine Gruppe und U eine Untergruppe mit $(G : U) = 2$, dann gilt $U \trianglelefteq G$.
- (ii) Ist G eine Gruppe und $(N_i)_{i \in I}$ eine Familie von Normalteilern, dann ist auch $N = \bigcap_{i \in I} N_i$ ein Normalteiler von G .
- (iii) Sei nun $\phi : G \rightarrow H$ ein Gruppenhomomorphismus. Ist N ein Normalteiler von H , dann ist $\phi^{-1}(N)$ ein Normalteiler von G .
- (iv) Ist ϕ surjektiv und N Normalteiler von G , dann ist $\phi(N)$ Normalteiler von H .

11 Beweis von Satz 4.18.

zu 1) geg. G Gruppe, $U \leq G$ mit $(G:U)$

□ Beh.: $U \trianglelefteq G$

Erinnerung: Die links- und Rechtsnebenklassen bilden eine Zerlegung von G . Sei $g \in G$.

$$\text{z.z.g.: } gU = Ug$$

$$1. \text{ Fall: } g \in U \Rightarrow gU = U = Ug$$

$$2. \text{ Fall: } g \notin U \Rightarrow gU \neq U \xrightarrow{(G:U)=2} U, gU$$

sind die einzigen linksnebenkl. von $G \Rightarrow$

$\exists$ disj. Zerlegung $G = U \cup gU$ genauso.

Korrektur 2. Zeile: geg.: G Gruppe, $U \leq G$ mit $(G:U) = 2$

$$G = U \cup Ug \text{ (disjunkt)} \Rightarrow gU = G \setminus U = Ug$$

zu iii) siehe Skript

zu iiii) Sei $\phi: G \rightarrow H$ ein Gruppenhom., $N \trianglelefteq H$.

$$\text{z.z.g.: } \phi^{-1}(N) \trianglelefteq G \quad \text{Sei } g \in G.$$

$$\text{z.z.g.: } g \phi^{-1}(N) g^{-1} \subseteq \phi^{-1}(N) \quad \text{Sei } h \in g \phi^{-1}(N) g^{-1}$$

$$\Rightarrow \exists n_1 \in \phi^{-1}(N) \text{ mit } h = g n_1 g^{-1} \quad \text{Es gilt } \phi(h) =$$

$$\phi(g) \phi(n_1) \phi(g)^{-1} \quad \phi(n_1) \in N \quad \Rightarrow \quad \phi(h) \in \phi(g) N \phi(g)^{-1}$$

$$\begin{matrix} N \trianglelefteq H \\ \Rightarrow \end{matrix} \phi(h) \in N \quad \Rightarrow \quad h \in \phi^{-1}(N)$$

zu iv) Sei $\phi: G \rightarrow H$ ein Epimorphismus von Gruppen

z.zg. $g \phi(N) g^{-1} \subseteq \phi(N)$ Sei $h \in g \phi(N) g^{-1}$

$$\Rightarrow \exists n_1 \in \phi^{-1}(N) \text{ mit } h = g n_1 g^{-1} \quad \text{Es gilt } \phi(h) = \phi(g) \phi(n_1) \phi(g)^{-1} \quad \phi(n_1) \in N \quad \Rightarrow \quad \phi(h) \in \phi(g) N \phi(g)^{-1}$$

und $N \trianglelefteq G$. z.zg. $\phi(N) \trianglelefteq H$

Sei $h \in H$. z.zg. $h \phi(N) h^{-1} \subseteq \phi(N)$ Sei $h_1 \in h \phi(N) h^{-1}$

$$\Rightarrow \exists n \in N: h_1 = h \phi(n) h^{-1} \quad \phi \text{ surjektiv} \Rightarrow \exists g \in G \text{ mit } \phi(g) = h \Rightarrow h_1 = \phi(g) \phi(n) \phi(g)^{-1} = \phi(g n g^{-1})$$

$$N \trianglelefteq G, g \in G, n \in N \Rightarrow g n g^{-1} \in N \Rightarrow h_1 \in \phi(N) \quad \square$$

Bem. Aussage (iv) wird falsch, wenn ϕ nicht surjektiv ist.

Betrachte z.B. $G = \langle (12) \rangle \subseteq S_3$, $H = S_3$ und die

Abt. $\phi: G \rightarrow H$ geg. durch $\tau \mapsto \tau$. Sei $N = \langle (12) \rangle$.

Dann gilt $N \trianglelefteq G$ (da jede Gruppe Normalteiler von sich selbst ist)

aber $\phi(N) = N$ ist kein Normalteiler von $H = S_3$ (Nicht jede Linksnebenklasse ist eine Rechtsnebenklasse, siehe § 2.)

Bem. In jeder Gruppe G gilt $\{e\} \trianglelefteq G$ und $G \trianglelefteq G$

Dies sind die trivialen Normalteiler von G . Eine Gruppe

G mit $G \neq \{e\}$, die nur diese beiden Normalteiler enthält, wird eine einfache Gruppe genannt.

(Bsp: $(\mathbb{Z}/p\mathbb{Z}, +)$ ist einfache Gruppe, für jede Primzahl p
später: A_n ist einfach für $n=3$ und alle $n \geq 5$)

$$g = u'n'$$

$$u \in N \cap U$$

Definition (4.19)

Sei G eine Gruppe, und seien $A, B \subseteq G$ beliebige Teilmengen. Dann nennt man die Teilmenge $AB = \{ab \mid a \in A, b \in B\}$ das **Komplexprodukt** von A und B .

Bei Gruppen in additiver Schreibweise verwendet man für das Komplexprodukt die Schreibweise $A + B$ statt AB .

Lemma (4.20)

Sei G eine Gruppe, und seien U und N Untergruppen von G .

- (i) Gilt $U \cap N = \{e\}$, dann hat jedes Element $g \in UN$ eine eindeutige Darstellung der Form $g = un$, mit $u \in U$ und $n \in N$.
- (ii) Gilt $U \subseteq N$, dann folgt $UN = N$.
- (iii) Gilt $UN = NU$, dann ist UN eine Untergruppe von G .
Ersteres ist insbesondere dann gegeben, wenn N ein Normalteiler von G ist.
- (iv) Sind N und U Normalteiler von G , dann folgt $UN \trianglelefteq G$.

Bem: Ist G eine Gruppe und sind $U, V \leq G$,
dann ist das Komplexprodukt UV im All-
gemeinen keine Untergruppe von G .

Bsp: $G = S_3$, $U = \langle (12) \rangle = \{\text{id}, (12)\}$,

$V = \langle (13) \rangle = \{\text{id}, (13)\}$. Dann gilt

$$UV = \{\text{id} \circ \text{id}, \text{id} \circ (13), (12) \circ \text{id}, (12) \circ (13)\}$$

$$= \{\text{id}, (13), (12), (132)\}$$

Dies ist keine
Untergruppe von S_3 , da $|UV| = 4$ kein
Teiler von $|S_3| = 6$ ist.

Beweis von Lemma 4.20

geg. G Gruppe, $N, U \leq G$

zu i) Vor: $U \cap N = \{e\}$ z.zg. Jedes $g \in UN$ hat eine eindeutige Darstellung der Form $g = un$ mit $u \in U, n \in N$. Sei $g \in G$. Die Existenz einer solchen Darstellung folgt direkt aus der Def von UN zur Eindeutigkeit:

Seien $u, u' \in U, n, n' \in N$ mit $un = g = u'n'$

$$\Rightarrow n = u^{-1}u'n' \Rightarrow n(n')^{-1} = u^{-1}u' \in N \cap U$$

$$\xrightarrow{N \cap U = \{e\}} n(n')^{-1} = e \text{ und } u^{-1}u' = e \Rightarrow$$

$$n' = n, u' = u$$

zu ii) Vor: $U \subseteq N$ z.zg: $UN = N$

"1" Sei $h \in UN \Rightarrow \exists u \in U, n \in N: h = un$

$U \subseteq N \Rightarrow u, n \in N \Rightarrow h \in N$

"2" Sei $n \in N, U \leq G \Rightarrow e_G \in U$

$\Rightarrow n = e_G n \in UN$

zu iii) Setze $UN = NU$ woraus Beh: $UN \leq G$

zu überprüfen (1) $e_G \in UN$ (2) $\forall g, h \in UN: gh, g^{-1} \in UN$

zu (1) $U, N \leq G \Rightarrow e_G \in U$ und $e_G \in N \Rightarrow e_G = e_G e_G \in UN$

zu (2) Seien $g, h \in UN \Rightarrow \exists u, u' \in U, n, n' \in N$ mit
 $g = un, h = u'n' \Rightarrow gh = un u'n' \quad nu' \in NU$

$NU = UN$
 $nu' \in UN \Rightarrow \exists n'' \in N, u'' \in U \text{ mit } nu' = u''n''$
einsetzen $\Rightarrow gh = uu''n''n' \Rightarrow gh \in UN$, wegen $uu'' \in U$
und $n''n' \in N$

ebenso: $g^{-1} = (un)^{-1} = n^{-1}u^{-1} \in NU \xrightarrow{NU=UN} g^{-1} \in UN$

zeige: Unter der Voraussetzung $N \trianglelefteq G$ gilt $NU = UN$

" $\subseteq$ " Sei $h \in NU \Rightarrow \exists n \in N, u \in U : h = nu$

$N \trianglelefteq G, u \in G \Rightarrow Nu = uN$ also: $h \in Nu \Rightarrow h \in uN$

$\Rightarrow \exists n' \in N : h = un' \Rightarrow h \in UN$

" $\supseteq$ " analog

zu (iv) siehe Skript

