Überblick § 4: Homomorphismen und Faktorgruppen

- Definition der Gruppenhomomorphismen
- Struktur der Automorphismengruppe $\mathrm{Aut}(G)$ 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 $\phi : G \to H$ Epimorphismus und $N = \ker(\phi)$, Isomorphiesätze als Folgerung
- Korrespondenzsatz (Untergruppenstruktur von G/N vs. Untergruppenstruktur von G)

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.

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

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

Satz (4.15)

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

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

Beweis von Satz 4.15:

geg.: $n \in \mathbb{N}$, G zyklische von Ordnung n
$g \in G$ mit $G = \langle g \rangle$

z.Z.: $\Rightarrow \exists\, \mathbb{Z} \to \mathrm{End}(G)$, $a \mapsto \tau_a$
mit τ_a definiert durch $\tau_a(g) = g^a$

Beob.: Sind $a, b \in \mathbb{Z}$ mit $a \equiv b \bmod n$,
dann folgt $\tau_a = \tau_b$.

$a \equiv b \bmod n \rightsquigarrow n \mid (a-b) \Rightarrow \exists k \in \mathbb{Z}$ mit
$kn = a - b \Rightarrow b = a - kn$
$\Rightarrow \tau_b(g) = g^b = g^{a-kn} = g^a \cdot (g^n)^{-k} \overset{\text{ord}(g) = n}{=}$

$g^q \cdot e_G^{-k} = g^q = \tau_a(g) \xrightarrow[\text{Eindeutigkeit Prop. 4.10}]{G=\langle g\rangle} \tau_a = \tau_b$

Aus der Beob. folgt, dass es ein Abb. $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{End}(G)$ mit $\phi(a+n\mathbb{Z}) = \tau_a \; \forall a \in \mathbb{Z}$ gibt.

zu überprüfen: (1) $\phi((\mathbb{Z}/n\mathbb{Z})^\times) = \mathrm{Aut}(G)$

(2) $\phi((a+n\mathbb{Z})\cdot(b+n\mathbb{Z})) = \phi(a+n\mathbb{Z}) \circ \phi(b+n\mathbb{Z})$

$\forall a, b \in \mathbb{Z}$.

Aus (1), (2) folgt dann, dass ϕ einen Isomorphismus zwischen $(\mathbb{Z}/n\mathbb{Z})^\times$ und $\mathrm{Aut}(G)$ definiert.

... Automorphismus von g ist.

Beweis von Satz 4.15 (Rest)

geg G zyklische Gruppe der Ordnung $n \in \mathbb{N}$

$g \in G$ mit $G = \langle g \rangle$

$\phi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{End}(G)$, $a + n\mathbb{Z} \mapsto \tau_a$, wobei

$\tau_a \in \mathrm{End}(G)$ jeweils festgelegt ist durch $\tau_a(g) = g^a$

überprüfe: (1) $\forall a, b \in \mathbb{Z} : \phi((a+n\mathbb{Z})(b+n\mathbb{Z})) =$

$\phi(a+n\mathbb{Z}) \circ \phi(b+n\mathbb{Z})$ ✓

(2) $\phi((\mathbb{Z}/n\mathbb{Z})^\times) = \mathrm{Aut}(G)$ ✓

(3) ϕ ist injektiv

Dann folgt insgesamt: ϕ ist Isom. $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G)$

zu (1) Seien $a, b \in \mathbb{Z}$. z.zg: $\tau_{ab} = \tau_a \circ \tau_b$

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

$\phi(a+n\mathbb{Z}) = \tau_a$, $\phi(b+n\mathbb{Z}) = \tau_b$)

Wegen $G = \langle g \rangle$ genügt es zu überprüfen: $\tau_{ab}(g) = (\tau_a \circ \tau_b)(g)$

Es gilt $(\tau_a \circ \tau_b)(g) = \tau_a(\tau_b(g)) = \tau_a(g^b) = \tau_a(g)^b$

$= (g^a)^b = g^{ab} = \tau_{ab}(g)$

zu (2) „$\subseteq$" Sei $a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$. $\Rightarrow \exists\, b \in \mathbb{Z}$ mit $(a+n\mathbb{Z})\cdot(b+n\mathbb{Z})$

$= 1+n\mathbb{Z} \overset{(1)}{\Rightarrow} \tau_a \circ \tau_b = \tau_1$ $\tau_1(g) = g^1 = g = id_G(g) \Rightarrow \tau_1 = id_G$

$\Rightarrow \tau_a \circ \tau_b = id_G$ ebenso: $(b+n\mathbb{Z})(a+n\mathbb{Z}) = 1+n\mathbb{Z} \Rightarrow$

$\tau_b \circ \tau_a = id_G$ Daraus folgt, dass $\phi(a+n\mathbb{Z}) = \tau_a$

ein Automorphismus von g ist.

„$\supseteq$" Sei $\tau \in \mathrm{Aut}(G)$ z.zg.: $\exists a \in \mathbb{Z}$ mit $a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*$ und $\phi(a+n\mathbb{Z}) = \tau$

$\tau(g) \in G$, $G = \langle g \rangle \Rightarrow \exists a \in \mathbb{Z}$ mit $\tau(g) = g^a$

$\Rightarrow \tau(g) = g^a = \tau_a(g) \Rightarrow \tau = \tau_a$

τ ist Automorphismus $\Rightarrow \tau(G) = G$

Für alle $m \in \mathbb{Z}$ gilt $\tau(g^m) = \tau(g)^m \in \langle \tau(g) \rangle$

$\Rightarrow \tau(G) \subseteq \langle \tau(g) \rangle \Rightarrow G = \langle \tau(g) \rangle = \langle g^a \rangle$

$\Rightarrow \mathrm{ord}(g^a) = |G| = \mathrm{ord}(g) \overset{\S 3}{\Rightarrow} ggT(a,n) = 1$

$\Rightarrow a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*$ nach Prop. 4.14

also: $\tau \in \phi((\mathbb{Z}/n\mathbb{Z})^*)$

zu (3) genügt zu überprüfen: $\ker(\phi) \subseteq \{1+n\mathbb{Z}\}$

Sei $a+n\mathbb{Z} \in \ker(\phi)$ (mit $a \in \mathbb{Z}$)

$\Rightarrow \tau_a = \phi(a+n\mathbb{Z}) = id_G$

$\Rightarrow g^a = \tau_a(g) = id_G(g) = g^1$

$n = ord(g)$

$\Rightarrow a \equiv 1 \bmod n \Rightarrow a+n\mathbb{Z} = 1+n\mathbb{Z}.$ □

Definition der Normalteiler

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

Kriterien für Normalteiler

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.: G Gruppe, $U \leq G$

z.zg.: Äquivalenz der drei Aussagen

(i) $U \trianglelefteq G$ (d.h. $gU = Ug$)

(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 (mit (i) als Vor.):
$gUg^{-1} \subseteq U$ Sei $h \in gUg^{-1} \Rightarrow \exists u \in U$
mit $h = gug^{-1}$ $gu \in gU \overset{(i)}{\Rightarrow} gu \in Ug$
$\Rightarrow \exists v \in U$ mit $gu = vg \Rightarrow h = (vg)g^{-1}$
$= v(gg^{-1}) = ve = v \Rightarrow h \in U$

n∈ℕ

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

„⊆" gilt auf Grund der Vor. (ii)

also nur noch z.zg: $U \subseteq gUg^{-1}$

Sei $u \in U$. Wegen (ii) gilt $g^{-1}U(g^{-1})^{-1} = g^{-1}Ug \overset{(*)}{\subseteq} U$ Schreibe $u = g(g^{-1}ug)g^{-1}$

Wegen (*) gilt $g^{-1}ug \in U \Rightarrow u \in gUg^{-1}$

□

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

„⊆" Sei $h \in gU \Rightarrow \exists u \in U$ mit $h = gu$

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

$h = \underbrace{gug^{-1}}_{\in U} g \in Ug$ „⊇" Sei $h \in Ug \Rightarrow$

$\exists u \in U$ mit $h = ug$ $g^{-1}ug \in g^{-1}Ug \overset{(iii)}{\Rightarrow}$

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

$\underbrace{\phantom{g^{-1}ug}}_{\in U}$

Eigenschaften von Normalteilern

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 $\phi : G \to H$ 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.

Beweis von Prop 4.18

zu (i) Sei G eine Gruppe und $U \leq G$ mit $(G:U) = 2$

Beh. $U \trianglelefteq G$ Sei $g \in G \setminus U$ (existiert, da $(G:U) > 1$ und somit $U \subsetneq G$) Wegen $(G:U)$ sind U und gU die einzigen Elemente von G/U. Da $\{U, gU\}$ eine Zerlegung von G ist, gilt $gU = G \setminus U$ (Mengendifferenz) ebenso: $(G:U) = 2$

$\Rightarrow$ U, Ug sind die einzigen Elemente von $U \setminus G$

$\Rightarrow$ $Ug = G \setminus U = gU$ damit gezeigt: $\forall g \in G \setminus U : gU = Ug$

Für alle $g \in U$ gilt offenbar $gU = U = Ug$ insgesamt:

$gU = Ug \; \forall g \in G \Rightarrow U \trianglelefteq G$.

Beweis von Satz 4.18 (Forts.)

zu (ii) siehe Skript

zu (iii) geg: $\phi : G \to H$ Gruppenhom., $N \trianglelefteq H$

zzg: $\phi^{-1}(N) \trianglelefteq G$

bereits bekannt: $\phi^{-1}(N) \leq G$ noch zzg

$\forall g \in G: \; g\phi^{-1}(N)g^{-1} \subseteq \phi^{-1}(N)$

Sei $h \in g\phi^{-1}(N)g^{-1} \Rightarrow \exists m \in \phi^{-1}(N): h = gmg^{-1}$

$m \in \phi^{-1}(N) \Rightarrow \phi(m) \in N \Rightarrow \phi(h) = \phi(gmg^{-1}) =$

$\phi(g)\phi(m)\phi(g)^{-1} \in \phi(g)N\phi(g)^{-1} \overset{N \trianglelefteq H}{\Rightarrow}$

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

zu (iv) geg: surjektiver Gruppenhom. $\phi: G \to H$, $N \trianglelefteq G$

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

Sei $k \in h\phi(N)h^{-1} \Rightarrow \exists n \in N: k = h\phi(n)h^{-1}$

ϕ surj. $\Rightarrow \exists g \in G$ mit $h = \phi(g) \Rightarrow k = \phi(g)\phi(n)\phi(g^{-1}) = \phi(gng^{-1})$

$N \trianglelefteq G \Rightarrow gng^{-1} \in N \Rightarrow k = \phi(gng^{-1}) \in \phi(N)$ □

Bem. Teil (iv) gilt nicht ohne die Vor. der Surjektivität

Sei $G = S_3$, $U = \langle (12) \rangle = \{id, (12)\}$. Betrachte den Hom $\phi: U \to S_3$, $\tau \mapsto \tau$. U ist Normalteiler von U, aber $\phi(U) = U$ ist kein Normalteiler von S_3, da z.B $(13)U = \{(13), (123)\} \Rightarrow (13)U \neq U(13) = \{(13), (132)\}$ □

Definition der Komplexprodukte

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 beides Normalteiler von G, dann folgt $UN \trianglelefteq G$.

Beweis von Lemma 4.20:

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

zu (i) Vor.: $N \cap U = \{e\}$ z.zg.: Jedes $g \in UN$ hat eine eind. Darst. $g = un$ mit $u \in U$, $n \in N$. Sei also $g \in UN$. Die Existenz ist nach Def. von UN erfüllt. zur Eindeutigkeit: Seien $u, u' \in U$ und $n, n' \in N$ mit $un = u'n'$

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

Vor. $\Rightarrow (u')^{-1} u = e, \; n' n^{-1} = e \Rightarrow u = u', \; n = n'$

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

„$\supseteq$" Sei $n \in N \overset{e \in U}{\Rightarrow} n = e \cdot n \in UN$

„$\subseteq$" Sei $h \in UN \Rightarrow \exists u \in U, n \in N$ mit $h = un$

$u, n \in N \Rightarrow h = un \in N$

$N \leq G$

zu (iii) z.Zg. (1) $UN = NU \Rightarrow NU \leq G$

(2) $N \trianglelefteq G \Rightarrow UN = NU$

zu (1) überprüfe: (i) $e \in NU$

(ii) $\forall g, h \in NU: gh \in NU, g^{-1} \in NU$

zu (i) $N, U \leq G \Rightarrow e \in N$ und $e \in U \Rightarrow$

$e = e\,e \in NU$

zu (ii) Seien $g, h \in NU \Rightarrow \exists n, n' \in N$ und

$u, u' \in U$ mit $g = nu$, $h = n'u' \Rightarrow$

$gh = nun'u'$ $un' \in UN \overset{V_0}{\Rightarrow} un' \in NU$

$\Rightarrow \exists n_1 \in N, u_1 \in U$ mit $un' = n u_1 \Rightarrow$

$gh = n(un')u' = n(n_1u_1)u' = (nn_1)(u_1u') \in NU$

$g^{-1} = (nu)^{-1} = u^{-1}n^{-1} \in UN \overset{\text{Vss.}}{\Rightarrow} g^{-1} \in NU$

zu (2) $N \trianglelefteq G$ z.zg.: $UN = NU$ „$\subseteq$"

Sei $g \in UN \Rightarrow \exists u \in U, n \in N$ mit $g = un$

$N \trianglelefteq G \Rightarrow unu^{-1} \in N \Rightarrow g = \underbrace{unu^{-1}}_{\in N} u \in NU$

„$\supseteq$" analog

zu (iv) siehe Skript

□

Bem. Ist G eine Gruppe und $U, V \leq G$, dann ist das Komplexprodukt im Allg. keine Untergruppe von G.

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

$V = \langle (13) \rangle = \{id, (13)\} \Rightarrow UV$

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

$= \{id, (12), (13), (132)\}$ Nach dem Satz v. Lagrange kann dies keine Untergruppe von S_3 sein (denn $|UV| = 4$ ist kein Teiler von $|S_3| = 6$).

Definition des Normalisators

Definition (4.21)

Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann nennt man $N_G(U) = \{g \in G \mid gUg^{-1} = U\}$ den Normalisator von U in G.

Die Bedeutung des Normalisators wird durch die folgende Proposition deutlich.

Proposition (4.22)

Sei G eine Gruppe und U eine Untergruppe. Dann ist $N_G(U)$ die größte Untergruppe H von G mit der Eigenschaft, dass U Normalteiler von H ist.

Innere direkte Produkte

Definition (4.23)

Sei G eine Gruppe, und seien U, N Untergruppen von G. Wir bezeichnen G als inneres direktes Produkt von U und N, wenn gilt

- $U \trianglelefteq G$ und $N \trianglelefteq G$,
- $G = UN$ und
- $U \cap N = \{e\}$.

Ist lediglich N eine Normalteiler von G, aber nicht notwendigerweise die Untergruppe U, dann spricht man von einem inneren semidirekten Produkt.

Proposition (4.24)

Sei G eine Gruppe und inneres direktes Produkt ihrer Untergruppen U und N. Dann gilt $G \cong U \times N$.