Die Untergruppen einer zyklischen Gruppe, Teil II

Satz (3.11)

Sei G eine zyklische Gruppe und $g \in G$ mit $G = \langle g \rangle$.

(i) Ist $\operatorname{ord}(g) = \infty$, dann sind die verschiedenen Untergruppen von G gegeben durch $U_0 = \{e_G\}$ und $U_m = \langle g^m \rangle$, wobei m die natürlichen Zahlen durchläuft.

(ii) Ist $\operatorname{ord}(g) = n$ endlich, dann sind $U_d = \langle g^d \rangle$ die verschiedenen Untergruppen von G, wobei d die Teiler von n durchläuft. Dabei gilt jeweils $|U_d| = \frac{n}{d}$.

In (i) und (ii) gilt $U_m \subseteq U_{m'}$ für $m, m' \in \mathbb{N}$ genau dann, wenn m' ein Teiler von m ist.

Charakterisierung der zyklischen Gruppen

Satz (3.12)

Sei G eine endliche Gruppe der Ordnung n mit der Eigenschaft, dass G für jedes Teiler $d \in \mathbb{N}$ von n genau eine Untergruppe U_d mit $|U_d| = d$ besitzt. Dann ist G eine zyklische Gruppe.

Beweis von Satz 3.12

Zeige zunächst: Für jedes $n \in \mathbb{N}$ gilt $n = \sum_{d \mid n} \varphi(d)$, wobei d die Teiler von n in $\mathbb{N}$ durchläuft.

[$6 = \underset{1}{\varphi(1)} + \underset{1}{\varphi(2)} + \underset{2}{\varphi(3)} + \underset{2}{\varphi(6)}$]

Ansatz: Überprüfe, dass $\sum_{d \mid n} \varphi(d)$ die Elementezahl in einer zyklischen Gruppe G der Ordnung n ist.

Sei also G eine Gruppe und $g \in G$ mit $G = \langle g \rangle$ sowie $n = \operatorname{ord}(g)$. Für jeden Teiler $d \in \mathbb{N}$ von n sei $G_d = \{ g \in G \mid \operatorname{ord}(g) = d \}$. Weil diese Mengen disjunkt

sind und jede Elementordnung in G ein Teiler von n ist, erhalten wir eine (disjunkte) Zerlegung $G = \bigcup_{d \mid n} G_d$, und somit $n = |G| = \sum |G_d|$. $\Rightarrow$ genügt z.Z.: $|G_d| = \varphi(d)$ für jeden Teiler $d \in \mathbb{N}^{d \mid n}$ von n. Nach Satz 3.11 gibt es für jedes solche d in G eine Untergr. U mit $|U| = d$. Diese ist zyklisch, enthält also $\varphi(d)$ Elemente der Ordnung d.
$\Rightarrow |G_d| \geq \varphi(d)$ Wäre $|G_d| > \varphi(d)$, dann müsste es mehr als eine Untergr. der Ordnung d geben. ($\lightning$ zu Satz 3.11)

Sei nun G eine Gruppe mit $n = |G|$ und der Eigenschaft, dass es zu jedem Teiler d von n genau eine Untergr. U_d mit $|U_d| = d$ gibt. Jedes Element $g \in G$ der Ordnung d ($d \in \mathbb{N}, d \mid n$) muss in

Ud liegen (und es gilt dann $U_d = \langle g \rangle$).

Setzen wir wieder $G_d = \{ g \in G \mid \mathrm{ord}(g) = d \}$,

dann gilt also für jeden Teiler d von n entweder $G_d = \emptyset$ oder $|G_d| = \varphi(d)$ (weil U_d dann zyklisch ist und somit genau $\varphi(d)$ Element der Ordn. d enthält).

Es gilt also $n = |G| = \sum_{d|n} |G_d| \leq$

$\sum_{d|n} \varphi(d) \overset{\text{s.o.}}{=} n \Rightarrow |G_d| = \varphi(d)$ für jeden Teiler d von n, insb. für n selbst. $\Rightarrow G_n \neq \emptyset$

$\Rightarrow G$ besitzt ein $g \in G$ mit $\mathrm{ord}(g) = n \Rightarrow G = \langle g \rangle$, d.h. G ist zyklisch $\square$

Der Kleine Satz von Fermat

Folgerung (3.13)

Für jede Primzahl p und alle $a \in \mathbb{Z}$ gilt $a^p \equiv a \mod p$. Ist p kein Teiler von a, dann gilt darüber hinaus $a^{p-1} \equiv 1 \mod p$.

Beweis von Folgerung 3.13.

Sei p eine Primzahl und $a \in \mathbb{Z}$, wobei wir zunächst $p \nmid a$ voraussetzen. Die Gruppe $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{\bar{0}\}$ (mit $\cdot$ als Verknüpfung) ist von Ordnung $p-1$. Sei $\bar{a} = a + p\mathbb{Z}$, also das Bild von a in $\mathbb{F}_p$. Dann ist $\bar{a} \neq \bar{0}$ (sonst $a \equiv 0 \bmod p$, also $p \mid a$), d.h. $\bar{a} \in \mathbb{F}_p^\times$. Satz v. Lagrange $\Rightarrow \operatorname{ord}(a) \mid (p-1)$. Satz 3.3 $\Rightarrow \bar{a}^{p-1} = \bar{1}$

$\Rightarrow a^{p-1} \equiv 1 \bmod p$. Ebenso: $\bar{a}^p = \bar{a} \rightsquigarrow a^p \equiv a \bmod p$. Im Fall $p \mid a$ gilt auch $p \mid a^p$, also $a^p \equiv 0 \equiv a \bmod p$. $\square$

§ 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.

Lemma (4.2)

Sei ϕ ein Homomorphismus zwischen den Gruppen $(G, *)$ und $(H, \circ)$. Dann gilt $\phi(e_G) = e_H$ und $\phi(g^{-1}) = \phi(g)^{-1}$ für alle $g \in G$.

Lemma (4.4)

Ist $\phi : G \to H$ ein Gruppenhomomorphismus, dann gilt $\phi(g^n) = \phi(g)^n$ für alle $g \in G$ und $n \in \mathbb{Z}$.

Damit gilt $\phi(a+b) = (a+b, 0) = (a,0) * (b,0) =$

Beweis von Lemma 4.2.

Beh.: $\phi(e_G) = e_H$ Es gilt $\phi(e_G) = \phi(e_G * e_G) =$

$\phi(e_G) \circ \phi(e_G) \rightarrow \phi(e_G) \circ \phi(e_G)^{-1} = \phi(e_G) \circ \phi(e_G) \circ \phi(e_G)^{-1}$

$\Rightarrow e_H = \phi(e_G) \circ e_H = \phi(e_G)$

Sei nun $g \in G$. Beh.: $\phi(g^{-1}) = \phi(g)^{-1}$

$e_H = \phi(e_G) = \phi(g * g^{-1}) = \phi(g) \circ \phi(g^{-1})$

$\Rightarrow \phi(g)^{-1} \circ e_H = \phi(g)^{-1} \circ \phi(g) \circ \phi(g^{-1}) \Rightarrow$

$\phi(g)^{-1} = e_H \circ \phi(g^{-1}) = \phi(g^{-1})$ $\square$

Beweis von Lemma 4.4

Zeige durch vollst. Ind.: $\forall n \in \mathbb{N}_0 : \phi(g^n) = \phi(g)^n$

Ind-anf.: $\phi(g^0) = \phi(e_G) = e_H = \phi(g)^0$

Ind-Schritt: Sei $n \in \mathbb{N}_0$, setze $\phi(g^n) = \phi(g)^n$ voraus

$\Rightarrow \phi(g^{n+1}) = \phi(g^n \cdot g) \overset{\phi \text{ Hom}}{=} \phi(g^n) * \phi(g) \overset{\text{Ind.-V.}}{=}$

$\phi(g)^n * \phi(g) = \phi(g)^{n+1}$.

Zeige nun, dass die Gleichung auch für negatives n gilt.

Sei $r \in \mathbb{N}$, z.zg.: $\phi(g^{-r}) = \phi(g)^{-r}$ Es gilt:

$\phi(g^{-r}) = \phi((g^r)^{-1}) \overset{\text{Lemma 4.2}}{=} \phi(g^r)^{-1} \overset{\text{s.o.}}{=} (\phi(g)^r)^{-1} = \phi(g)^{-r}$ □

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 $\mathrm{Aut}(G)$.

Isomorphie von Permutationsgruppen

Satz (4.5)

Seien X, Y Mengen und $\phi : X \to Y$ eine Bijektion. Dann ist durch die Abbildung

$$\hat{\phi} : \mathrm{Per}(X) \to \mathrm{Per}(Y) \quad , \quad \sigma \mapsto \phi \circ \sigma \circ \phi^{-1}$$

ein Isomorphismus von Gruppen definiert.

Auf Grund des Satzes gilt $\mathrm{Per}(X) \cong S_n$ für jede n-elementige Menge X.

Sei $r \in \mathbb{N}$, zzg: $\phi(g^{-r}) = \phi(g)^{-r}$ Es gilt

Lemma 4.2

Beweis von Satz 4.5:

geg: Mengen X, Y, Bijektion $\phi: X \to Y$

Beh.: $\hat{\phi}: \mathrm{Per}(X) \to \mathrm{Per}(Y)$, $\sigma \mapsto \phi \circ \sigma \circ \phi^{-1}$

ist ein Isomorphismus von Gruppen. $Y \to Y$ $X \to X$ $Y \to X$

(Bem: Für jedes $\sigma \in \mathrm{Per}(X)$ ist $\hat{\phi}(\sigma)$ tatsächlich eine bijektive Abbildung $Y \to Y$, weil die Komposition von bij. Abbildungen wieder bij. ist.)

zu überprüfen: (1) $\hat{\phi}$ ist ein Gruppenhom. (2) $\hat{\phi}$ ist bijektiv

zu(1) Seien $\sigma, \tau \in \mathrm{Per}(X)$, zzg.: $\hat{\phi}(\sigma \circ \tau) = \hat{\phi}(\sigma) \circ \hat{\phi}(\tau)$

Es gilt $\hat{\phi}(\sigma \circ \tau) = \phi \circ \sigma \circ \tau \circ \phi^{-1} = \phi \circ \sigma \circ \mathrm{id}_X \circ \tau \circ \phi^{-1}$

$= \phi \circ \sigma \circ \phi^{-1} \circ \phi \circ \tau \circ \phi^{-1} = \hat{\phi}(\sigma) \circ \hat{\phi}(\tau)$

zu (2) genügt z.zg.: Die Abbildung $\Psi : Per(Y) \to Per(X)$, $\sigma \mapsto \phi^{-1} \circ \sigma \circ \phi$ ist eine Umkehrabb. von $\hat{\phi}$.
$Y \to X \quad Y \to Y \quad X \to Y$

Überprüfe dafür: (2.1) $\Psi \circ \hat{\phi} = id_{Per(X)}$

(2.2) $\hat{\phi} \circ \Psi = id_{Per(Y)}$

zu (2.1) Sei $\sigma \in Per(X)$.

$$(\Psi \circ \hat{\phi})(\sigma) = \Psi(\hat{\phi}(\sigma)) = \Psi(\phi \circ \sigma \circ \phi^{-1})$$

$$= \phi^{-1} \circ \phi \circ \sigma \circ \phi^{-1} \circ \phi = id_X \circ \sigma \circ id_X = \sigma$$

$$= id_{Per(X)}(\sigma)$$

zu (2.2) analog zu 2.1

□

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.

Beweis von Proposition 4.6:

- Jedes invertierbare Element σ in $\mathrm{End}(G)$ ist ein Automorphismus von G, denn: σ invertierbar $\Rightarrow \exists \tau \in \mathrm{End}(G)$ mit $\tau \circ \sigma = id_G$, $\sigma \circ \tau = id_G \Rightarrow \tau$ ist Umkehrabbildung von σ, und σ somit bijektiv. Insgesamt ist σ also ein Automorphismus von G.
- Sei umgekehrt $\sigma \in \mathrm{Aut}(G)$. Beh.: Die Umkehrabbildung σ^{-1} von σ liegt in $\mathrm{End}(G)$. (Daraus folgt wegen $\sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = id_G$, dass σ^{-1} ein Inverses von σ in $\mathrm{End}(G)$ ist.)

□

Seien $h, h' \in G$

z.Zg.: $\sigma^{-1}(h \cdot h') = \sigma^{-1}(h) \cdot \sigma^{-1}(h')$

σ ist Gp. $\Rightarrow \exists\, g, g' \in G$ mit $\sigma(g) = h$,

$\sigma(g') = h'$ $\quad \sigma \in \mathrm{End}(G) \Rightarrow$

$\sigma(g \cdot g') = \sigma(g) \cdot \sigma(g') \Rightarrow$

$\sigma^{-1}(h \cdot h') = \sigma^{-1}(\sigma(g) \cdot \sigma(g')) =$

$\sigma^{-1}(\sigma(g \cdot g')) = g \cdot g' = \sigma^{-1}(h) \cdot \sigma^{-1}(h')$ $\square$