Die Untergruppen einer zyklischen Gruppe, Teil I

Satz (3.7)

Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer gilt: Sei G eine zyklische Gruppe, g ein Element mit $G = \langle g \rangle$ und U eine Untergruppe $\neq \{e_G\}$. Dann gibt es ein $m \in \mathbb{N}$ mit

$$U \quad = \quad \langle g^m \rangle.$$

Ist $\mathrm{ord}(g) = n$ endlich, dann kann die Zahl m so gewählt werden, dass sie ein Teiler von n ist.

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.

$\Rightarrow \exists k \in \mathbb{Z} : g^{m'} = (g^m)^k = g^{mk}$ $\quad l \mapsto g^l$ injektiv $\quad m = m'k$

Beweis von Satz 3.11

gegeben eine zyklische Gruppe G, $g \in G$ mit $G = \langle g \rangle$

Definiere

- im Fall $\operatorname{ord}(g) = \infty$: $U_m = \langle g^m \rangle$ $\forall m \in \mathbb{N}$ und $U_0 = \{e_G\}$
- im Fall $\operatorname{ord}(g) = n$, $n \in \mathbb{N}$: $U_m = \langle g^m \rangle$ für jeden Teiler $m \in \mathbb{N}$ von n

Wenn wir gezeigt haben, dass für alle $m, m' \in \mathbb{N}$, für die $U_m, U_{m'}$ definiert sind, jeweils die

Äquivalenz (*) $U_m \subseteq U_{m'} \iff m' \mid m$

gilt, dann folgt automatisch, dass die U_m für die einzelnen Werte von m alle verschieden sind, denn:

$U_m = U_{m'} \Rightarrow U_m \subseteq U_{m'}$ und $U_{m'} \subseteq U_m$

$\overset{(*)}{\Rightarrow} m' \mid m$ und $m \mid m' \Rightarrow m = m'$

Beweis von (*): 1. Fall $\operatorname{ord}(g) = \infty$

„$\Leftarrow$" $m' \mid m \Rightarrow \exists k \in \mathbb{N}$ mit $m = k m' \Rightarrow g^m = (g^{m'})^k \in \langle g^{m'} \rangle = U_{m'} \Rightarrow U_m = \langle g^m \rangle \subseteq U_{m'}$

„$\Rightarrow$" Vor.: $U_m \subseteq U_{m'} \Rightarrow \langle g^m \rangle \subseteq \langle g^{m'} \rangle \Rightarrow g^m \in \langle g^{m'} \rangle$

$\Rightarrow \exists k \in \mathbb{Z}: g^m = (g^{m'})^k = g^{m'k} \overset{\operatorname{ord}(g)=\infty,\ l \mapsto g^l \text{ injektiv}}{\Longrightarrow} m = m'k$

Also gilt $m' \mid m$

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

Dann sind m, m' Teiler von n.

„$\Longleftarrow$" wie im 1. Fall

„$\Longrightarrow$" $U_m \subseteq U_{m'} \Rightarrow \langle g^m \rangle \subseteq \langle g^{m'} \rangle$

$\Rightarrow g^m \in \langle g^{m'} \rangle \Rightarrow \exists k \in \mathbb{Z}$ mit

$g^m = (g^{m'})^k = g^{km'} \quad \cdot g^{-km'} \Rightarrow$

$g^{m-km'} = e \overset{\operatorname{ord}(g)=n}{\underset{\text{Satz 3.3}}{\Longrightarrow}} n \mid (m - km')$

$\Rightarrow \exists\, l \in \mathbb{Z}$ mit $ln = m - km'$

$\Rightarrow km' = m - ln$ Wegen $m' \mid n$

gilt $n = jm'$ für ein $j \in \mathbb{Z}$. $\Rightarrow$

$km' = m - ljm' \Rightarrow$

$km' + ljm' = m \Rightarrow$

$(k + lj)m' = m \Rightarrow m' \mid m$

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

geg.: $n \in \mathbb{N}$, G Gruppe mit $|G| = n$

Vor.: Für jeden Teiler $d \in \mathbb{N}$ von n gibt es genau eine Untergruppe U_d von G mit $|U_d| = d$. Beh.: Dann ist G zyklisch.

1. Schritt: Es gilt $n = \sum_{d \mid n} \varphi(d)$. (**)

(Beispiel: $6 = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6)$.)

Sei H eine zyklische Gruppe der Ordnung n und $h \in H$ mit $H = \langle h \rangle$.

Zeige: $|H| = \sum_{d \mid n} \varphi(d)$ (*)

Für jedes $h \in H$ gilt $\operatorname{ord}(h) \mid n$, d.h. $\operatorname{ord}(h) = d$ für ein $d \mid n$. Beh.: Für jeden Teiler d gibt es genau $\varphi(d)$ Elemente der Ordnung d in H.

(Ist das gezeigt, dann folgt (*) unmittelbar aus $|H| = \sum_{d \mid n} |M_d| = \sum_{d \mid n} \varphi(d)$, wobei $M_d \subseteq H$ jeweils die Menge der Elemente der Ordnung d bezeichnet.)

Sei $d \in \mathbb{N}$ ein Teiler von n bekannt: H hat eine eind. bestimmte Untergruppe der Ordn. d. Diese ist zyklisch und hat somit genau $\varphi(d)$ Elemente der

Ordnung d. Außerdem darf in U kein Element $h \in H$ der Ordnung d gelten, da dann $\langle h \rangle$ eine weitere Untergruppe der Ordnung d wäre. ($\Rightarrow$ Beh.)

Damit ist (**) bewiesen.

Zeige nun, dass G zyklisch ist.

Sei d ein echter Teiler von n. Dann gibt es in G höchstens $\varphi(d)$ Elemente der Ordnung d.

denn: Ist $g \in G$ mit $\mathrm{ord}(g) = d$, dann enthält $\langle g \rangle$ bereits $\varphi(d)$ Elemente der Ordnung d. Wäre die Anzahl insgesamt größer, dann gäbe es ein $g' \in G \setminus \langle g \rangle$

höchstens $\varphi(d)$ Elemente der Ordnung d

mit $\operatorname{ord}(g') = d \Rightarrow \langle g \rangle, \langle g' \rangle$ wären zwei verschiedene Untergr. der Ordnung d $\lightning$ zur Voraussetzung

Ang.: G enthält kein Element der Ordnung n. Dann folgt

$$|G| \leq \sum_{\substack{d \mid n \\ d \neq n}} \varphi(d) < \sum_{d \mid n} \varphi(d) \overset{\text{s.o.}}{=} n = |G| \quad \lightning$$

also: G besitzt ein Elt. der Ordn. $n \Rightarrow G$ ist zyklisch

□

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

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

Beweis von Lemma 4.2

Sei $\phi : G \to H$ ein Gruppenhom. zu zeigen

(i) $\phi(e_G) = e_H$ (ii) $\phi(g^{-1}) = \phi(g)^{-1}$

zu (i) $\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) \circ \phi(e_G)$

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

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

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

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

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

Dies zeigt, dass $\phi(g^{-1})$ das Inverse von $\phi(g)$ in $(H, \circ)$ ist, also $\phi(g^{-1}) = \phi(g)^{-1}$ gilt. $\square$

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 $\mathrm{Aut}(G)$.

Anwendung von Homomorphismen und Potenzierung

Lemma (4.4)

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

Beweis von Lemma 4.4

Sei $\phi : G \to H$ ein Gruppenhom und $g \in G$. Beh.: $\phi(g^n) = \phi(g)^n \quad \forall n \in \mathbb{Z}$

Zeige zunächst durch vollst. Ind., dass die Gleichung für alle $n \in \mathbb{N}_0$ gilt.

Ind.-Anf.: $\phi(g^0) = \phi(e_G) \overset{(4.2)}{=} e_H$

$= \phi(g)^0$

Ind.-Schritt: $n \mapsto n+1$

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

Beh.

überp

$\overset{\text{Ind.-V.}}{=} \phi(g)^n \circ \phi(g) = \phi(g)^{n+1}$

Zeige nun, dass die Gleichung auch für negative ganze Zahlen gilt. Sei $n \in \mathbb{N}$

$$\phi(g^{-n}) = \phi\left((g^n)^{-1}\right) \overset{(4.2)}{=} \phi(g^n)^{-1} \overset{\text{s.o.}}{=}$$

$$(\phi(g)^n)^{-1} = \phi(g)^{-n}$$

□

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.

Beweis von Satz 4.5

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

klar: Für alle $\sigma \in \mathrm{Per}(X)$ ist durch $\phi \circ \sigma \circ \phi^{-1}$ eine bijektive Abb. $Y \to Y$, also ein Element von $\mathrm{Per}(Y)$, gegeben

$\Rightarrow \hat{\phi} : \sigma \mapsto \phi \circ \sigma \circ \phi^{-1}$ ist eine Abbildung $\mathrm{Per}(X) \to \mathrm{Per}(Y)$

Beh.: $\hat{\phi}$ ist ein Isomorphismus

überprüfe: (1) $\hat{\phi}(\sigma \circ \tau) = \hat{\phi}(\sigma) \circ \hat{\phi}(\tau)$

für alle $\sigma, \tau \in \mathrm{Deck}(X)$

(2) $\hat{\phi}$ ist Gruppenhom

zu (1) Seien $\sigma, \tau \in \mathrm{Deck}(X)$. Dann gilt

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

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

zu (2) überprüfe: $\Psi : \mathrm{Deck}(Y) \to \mathrm{Deck}(X)$,
$\rho \mapsto \phi^{-1} \circ \rho \circ \phi$ ist Umkehrabbildung von $\hat{\phi}$. (klar: $\rho \in \mathrm{Deck}(Y) \Rightarrow \phi^{-1} \circ \rho \circ \phi \in \mathrm{Deck}(X)$)

Nachzurechnen: $\psi \circ \hat{\phi} = \mathrm{id}_{\mathrm{Po}(X)}$, $\hat{\phi} \circ \psi = \mathrm{id}_{\mathrm{Rel}(X)}$

Sei $\sigma \in \mathrm{Po}(X)$. Dann gilt $(\psi \circ \hat{\phi})(\sigma) =$

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

$= \mathrm{id}_X \circ \sigma \circ \mathrm{id}_X = \sigma$. Der Beweis der zweiten Gleichung läuft analog. □

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 Prop. 4.6

Sei $(G, \circ)$ eine Gruppe und $\phi \in \mathrm{End}(G)$.

Beh.: ϕ ist invertierbar im Monoid $(\mathrm{End}(G), \circ)$ $\Longleftrightarrow$ $\phi \in \mathrm{Aut}(G)$

„$\Rightarrow$" ϕ invertierbar $\Rightarrow \exists\, \psi \in \mathrm{End}(G)$ mit $\psi \circ \phi = \mathrm{id}_G$ und $\phi \circ \psi = \mathrm{id}_G$ $\Rightarrow$ ψ ist Umkehrabb. von ϕ $\Rightarrow$ ϕ ist Gruppenhom. $\quad \phi \in \mathrm{End}(G) \wedge \phi$ Gruppenhom. $\Rightarrow \phi \in \mathrm{Aut}(G)$

„$\Leftarrow$" Sei $\phi \in \mathrm{Aut}(G)$. zeige: Dann ist auch die Umkehrabb. ϕ^{-1} von ϕ in $\mathrm{End}(G)$ enthalten. (Dann ist ϕ^{-1} wegen $\phi^{-1} \circ \phi = \phi \circ \phi^{-1} = \mathrm{id}_G$ ein Inverses von ϕ in $(\mathrm{End}(G), \circ)$, also ϕ ein invertierbares Element.)

Um zu zeigen, dass ϕ^{-1} in $\mathrm{End}(G)$ liegt, müssen wir überprüfen: $\phi^{-1}(g) \cdot \phi^{-1}(g') = \phi^{-1}(gg') \quad \forall g, g' \in G$.

Seien $a = \phi^{-1}(g)$, $b = \phi^{-1}(g')$. $\phi \in \mathrm{End}(G) \Rightarrow$

$\phi(ab) = \phi(a) \cdot \phi(b) \Rightarrow \phi^{-1}(\phi(ab)) = \phi^{-1}(\phi(a)\phi(b))$

$\Rightarrow ab = \phi^{-1}(\phi(a)\phi(b)) \Rightarrow \phi^{-1}(g)\phi^{-1}(g') = \phi^{-1}(gg')$

□

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 $\phi^{-1} : H \to G$.