

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

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

Ist $\text{ord}(g) = n$ 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 $\text{ord}(g) = \infty$, 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 $\text{ord}(g) = n$ 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.

Beweis von Satz 3.11 (Abschluss)

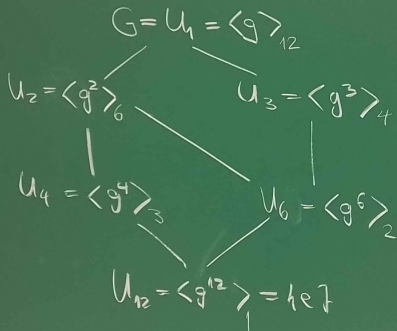
nach z.z.g.: Aus $U_m = U_{m'}$ folgt $m = m'$ (im Fall $\text{ord}(g) = \infty$ für beliebige natürliche Zahlen, im Fall $\text{ord}(g) = n \in \mathbb{N}$ für Teiler $m, m' \in \mathbb{N}$ von n).

Verwende die Äquivalenz $U_m \subseteq U_{m'} \Leftrightarrow m' | m$ für diese m und m' .
 $U_m = U_{m'} \Rightarrow U_m \subseteq U_{m'} \text{ und } U_{m'} \subseteq U_m$
 $\stackrel{\text{s.o.}}{\Rightarrow} m' | m \text{ und } m | m' \xrightarrow{m, m' \in \mathbb{N}} m = m'$

Also sind für $m \neq m'$ die Untergruppen $U_m, U_{m'}$ tatsächlich verschieden. □

Also sind für $m \neq m'$ die Untergruppen $U_m, U_{m'}$

Beispiel. Untergruppen einer zyklischen Gruppe
 $G = \langle g \rangle$ der Ordnung 12 (d.h. $\text{ord}(g) = 12$)



Ordnung der
Untergruppe

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 der Ordnung n

Voraussetzung: Für jeden Teiler $d \in \mathbb{N}$ von n hat G genau eine Untergruppe.

z.zg: G ist zyklisch

1. Schritt: Beweise die Gleichung $\sum_{d|n} \varphi(d) = n$

Sei H eine zyklische Gruppe der Ordnung n .

Satz v. Lagrange $\rightarrow$ Die Ordnung jedes Elements $h \in H$ ist ein Teiler $d \in \mathbb{N}$ von n .

Jedes Element der Ordnung d liegt in der eindeutig bestimmten Untergruppe V_d von H der Ordnung d . Weil V_d zyklisch ist, gibt es in V_d genau $\varphi(d)$ Elemente der Ordnung d , also: Es gibt genau $\varphi(d)$ Elemente der Ordnung d in ganz H . Die Gesamtzahl der Elemente in H muss damit $\sum_{d|n} \varphi(d)$ sein.

Diese Gesamtzahl ist gleich $|H| = n$.

2. Schritt: Beweis der Aussage des Satzes
zeige: Es gibt in G ein $g \in G$ mit
 $\text{ord}(g) = n$. (Dann folgt $G = \langle g \rangle$, d.h.

ein- G ist dann zyklisch.

Ang., es existiert kein solches Element.

Dann ist $\text{ord}(g)$ für jedes $g \in G$ ein echter Teiler von n , also kleiner als n . Für jeden solchen Teiler $d \in \mathbb{N}$ sei a_d die Anzahl der Elemente der Ordnung d in G . Dann gilt $\sum_d a_d = n$.

Ang., für d gibt es mind. ein Element der Ordnung d , bezeichne dieses mit $g \Rightarrow \langle g \rangle$ ist die einzig Untergr. von G der Ordn. $d \Rightarrow a_d = \varphi(d)$, dann diese Untergr. enthält genau $\varphi(d)$ Elemente der Ordn. $d \Rightarrow a_d = 0$ oder $a_d = \varphi(d)$ für jeden echten Teiler

$$d \in \mathbb{N} \text{ von } n \Rightarrow \sum_d a_d \leq \sum_d \varphi(d) < \sum_{d|n} \varphi(d) = n$$

(echte Teiler)
 $\nearrow$
 $\varphi(n) > 0$

$$\hookrightarrow \text{zu } \sum_d a_d = n.$$



Folgerung (3.13)

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

§ 4. 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

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

Beweis von Lemma 4.2:

geg. Gruppen $(G, *)$, $(H, \circ)$, Gruppenhom. $\phi: G \rightarrow H$

z.zg. i) $\phi(e_G) = e_H$ ii) $\phi(g^{-1}) = \phi(g)^{-1} \quad \forall g \in G$

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

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

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

zu ii) Sei $g \in G$. $\phi(g) \circ \phi(g^{-1}) = \phi(g * g^{-1}) =$

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

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

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 $\text{Aut}(G)$.

Lemma (4.4)

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

$$\text{zu ii)} \quad \phi(e_G) \circ \phi(e_G) = \phi(e_G * e_G) = \phi(e_G)$$

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

Beweis von Lemma 4.4

geg. Gruppenhom. $\phi: G \rightarrow H$, $g \in G$

Beh. $\phi(g^n) = \phi(g)^n \quad \forall n \in \mathbb{Z}$

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

Induktion. Ind.-Fall: $\phi(g^0) = \phi(e_G) \stackrel{\text{Lemma 4.2}}{=} e_H = \phi(g)^0$

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

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

Zeige die Gleichung noch für negative ganze Zahlen.

$$\begin{aligned} \text{Sei } n \in \mathbb{N}. \text{ Dann gilt } \phi(g^{-n}) &= \phi((g^n)^{-1}) \stackrel{\text{Lemma 4.2}}{=} \phi(g^n)^{-1} \\ &= (\phi(g)^n)^{-1} = \phi(g)^{-n} \end{aligned}$$

□

Satz (4.5)

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

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

ein Isomorphismus von Gruppen definiert.

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

Beweis von Satz 4.5

geg. Mengen X, Y , Bijektion $\phi: X \rightarrow Y$

Für jedes $\sigma \in \text{Per}(X)$ ist $\phi \circ \sigma \circ \phi^{-1}$ ein
 $\begin{matrix} X \rightarrow Y & X \rightarrow X & Y \rightarrow X \\ \downarrow & \downarrow & \downarrow \\ Y & X & Y \end{matrix}$

Element von $\text{Per}(Y)$, denn die Komposition
bijektiver Abbildungen ist bijektiv.

$\Rightarrow$ erhalte durch $\hat{\phi}(\sigma) = \phi \circ \sigma \circ \phi^{-1}$
eine Abbildung $\text{Per}(X) \rightarrow \text{Per}(Y)$

noch z.zg: i) $\hat{\phi}$ ist ein Gruppenhom.

ii) $\hat{\phi}$ ist bijektiv

zu i) Seien $\sigma, \tau \in \text{Per}(X)$, z.zg:

noch z.z.zg: (i) ϕ ist ein Gruppenkom

$$\hat{\phi}(\sigma \circ \tau) = \hat{\phi}(\sigma) \circ \hat{\phi}(\tau) \quad \text{Es gilt}$$

$$\begin{aligned} \hat{\phi}(\sigma \circ \tau) &= \phi \circ \sigma \circ \tau \circ \phi^{-1} = \phi \circ \sigma \circ \text{id}_X \circ \tau \circ \phi^{-1} \\ &= (\phi \circ \sigma \circ \phi^{-1}) \circ (\phi \circ \tau \circ \phi^{-1}) = \hat{\phi}(\sigma) \circ \hat{\phi}(\tau) \end{aligned}$$

zu (ii) überprüfe: $\psi: P_G(Y) \rightarrow P_G(X)$, $\tau \mapsto \phi^{-1} \circ \tau \circ \phi$ ist eine Umkehrabb. von $\hat{\phi}$

zu überprüfen: (iii) $\psi \circ \hat{\phi} = \text{id}_{P_G(X)}$

(iv) $\hat{\phi} \circ \psi = \text{id}_{P_G(Y)}$

zu (iii) Sei $\sigma \in P_G(X)$. Dann gilt $(\psi \circ \hat{\phi})(\sigma)$

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

$$\text{id}_X \circ \sigma \circ \text{id}_X = \sigma \quad \text{zu (iv) analog} \quad \square$$

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 .

Beweis von Proposition 4.6

Sei G eine Gruppe und $\phi \in \text{End}(G)$.

Beh.: $\phi \in \text{Aut}(G) \iff \phi$ invertierbar im Monoid $(\text{End}(G), \circ)$

" $\Leftarrow$ " ϕ invertierbar $\Rightarrow \exists \psi \in \text{End}(G)$ mit $\psi \circ \phi = \text{id}_G$ und $\phi \circ \psi = \text{id}_G \Rightarrow \psi$ ist die Umkehrabbildung von $\phi \Rightarrow \phi$ ist ein bijektiver Endomorphismus von $G \Rightarrow \phi$ ist ein Automorphismus von G .

$\Rightarrow$ " Sei $\phi \in \text{Aut}(G) \Rightarrow \phi \in \text{End}(G)$ und ϕ ist bijektiv. zeige: Die Umkehrabbildung ϕ^{-1} von ϕ liegt in $\text{End}(G)$. (Damit ist ϕ^{-1} das Inversese von ϕ in $(\text{End}(G), \circ)$, ϕ also invertierbar.)

Seien $g, h \in G$, $g' = \phi^{-1}(g)$, $h' = \phi^{-1}(h)$

$$\phi \in \text{End}(G) \Rightarrow \phi(g' \cdot h') = \phi(g') \cdot \phi(h')$$

Anwendung

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

von ϕ^{-1}

$$\Rightarrow \phi^{-1}(g) \phi^{-1}(h) = \phi^{-1}(g \cdot h)$$

□

□

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