

Definition (3.1)

Sei G eine Gruppe.

- Die Anzahl $|G|$ der Elemente von G wird die **Ordnung** von G genannt.
- Ist $g \in G$ ein beliebiges Element, dann bezeichnen wir $\text{ord}(g) = |\langle g \rangle|$ als die Ordnung von g .

Satz (3.3)

Sei G eine Gruppe und $g \in G$ ein beliebiges Element. Dann sind für jedes $n \in \mathbb{N}$ die folgenden Aussagen äquivalent.

- (i) $n = \text{ord}(g)$
- (ii) Es gibt ein $m \in \mathbb{N}$ mit $g^m = e_G$, und darüber hinaus ist n die **minimale** natürliche Zahl mit dieser Eigenschaft.
- (iii) Für alle $m \in \mathbb{Z}$ gilt $g^m = e_G$ genau dann, wenn m ein Vielfaches von n ist.

Satz (3.6)

Sei $n \in \mathbb{N}$ und $\sigma \in S_n$.

- (i) Ist σ ein k -Zykel ($2 \leq k \leq n$), dann gilt $\text{ord}(\sigma) = k$.
- (ii) Ist σ ein Element vom Zerlegungstyp $(k_1, \dots, k_r)$, dann gilt $\text{ord}(\sigma) = \text{kgV}(k_1, \dots, k_r)$.

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.

Beweis von Satz 3.7 (Abschluss)

geg. G Gruppe, $n \in \mathbb{N}$, $g \in G$ mit $G = \langle g \rangle$
und $\text{ord}(g) = n$ ($\Rightarrow |G| = n$)

außerdem: U Untergr. von G , $U \neq \{e\}$

z.z.: Es gibt einen Teiler $m \in \mathbb{N}$ von n mit $U = \langle g^m \rangle$

Sei $m \in \mathbb{N}$ minimal mit $g^m \in U$ (Existenz eines solchen m wurde schon gezeigt). Beh. $m \mid n$

Division mit Rest $\Rightarrow \exists q, r \in \mathbb{Z}$ mit $n = qm + r$
mit $0 \leq r < m$. Ang. m ist kein Teiler von n .

$\Rightarrow r \in \mathbb{N}, r < m$ Es gilt $g^r = g^{r-qm} = g^r \cdot (g^m)^{-q}$
 $= e \cdot (g^m)^{-q} \in U$ wegen $g^m \in U$ $\nmid$ zur Primzahl m
 $\uparrow n = \text{ord}(g)$ □

Satz (3.8)

Seien $m, n \in \mathbb{Z}$, $(m, n) \neq (0, 0)$. Dann gibt es $a, b \in \mathbb{Z}$ mit

$$am + bn = \text{ggT}(m, n).$$

Beweis von Satz 3.8

geg. $m, n \in \mathbb{Z}$ mit $(m, n) = (0, 0)$

Sei $d = \text{ggT}(m, n)$.

Beh.: Es gibt $a, b \in \mathbb{Z}$ mit $am + bn = d$.

Betrachte in der zyklischen Gruppe $(\mathbb{Z}, +)$

die Untergruppe $U = \langle m, n \rangle = \{ km + ln \mid$

$k, l \in \mathbb{Z} \}$. Satz 3.7 $\Rightarrow U$ ist zyklisch

Wegen $(m, n) \neq (0, 0)$ gilt $U \neq \{0\}$.

Satz 3.7 $\Rightarrow \exists d' \in \mathbb{N}$ mit $U = \langle d' \rangle$

zeige: d' besitzt die definierenden Ei-

Eigenschaften des ggT von m und n
definieren zu überprüfen: (i) $d' \mid m, d' \mid n$

(ii) $\forall d'' \in \mathbb{N} : d'' \mid m, d'' \mid n \Rightarrow d'' \mid d'$

zu (i) $\langle d' \rangle = U = \langle m, n \rangle \Rightarrow m \in \langle d' \rangle$ und

$n \in \langle d' \rangle \Rightarrow \exists k, l \in \mathbb{Z} : m = kd', n = ld'$

$\Rightarrow d' \mid m, d' \mid n$

zu (ii) Sei $d'' \in \mathbb{N}$ mit $d'' \mid m, d'' \mid n \Rightarrow$

$\exists k_1, l_1 \in \mathbb{Z}$ mit $m = k_1 d'', n = l_1 d'' \Rightarrow$

$m, n \in \langle d'' \rangle \Rightarrow \langle m, n \rangle \subseteq \langle d'' \rangle \Rightarrow$

$U \subseteq \langle d'' \rangle \Rightarrow \langle d' \rangle \subseteq \langle d'' \rangle \Rightarrow d' \in \langle d'' \rangle$

$\Rightarrow \exists r \in \mathbb{Z}$ mit $d' = r d'' \Rightarrow d'' \mid d'$

Aus dem Gezeigten folgt $d' = \text{ggT}(m, n) = d$.
 $d' \in U \Rightarrow d' \in \langle m, n \rangle \Rightarrow \exists a, b \in \mathbb{Z}$ mit
der Eigenschaft $d' = am + bn$. □

d.

(+, +)

n/

in

.

>

Er -

Satz (3.9)

Sei G eine Gruppe und $g \in G$ ein Element der Ordnung $n \in \mathbb{N}$.

- (i) Für beliebiges $m \in \mathbb{Z}$ gilt $\text{ord}(g^m) = n$ genau dann, wenn $\text{ggT}(m, n) = 1$ ist.
- (ii) Ist $d \in \mathbb{N}$ ein Teiler von n , dann gilt $\text{ord}(g^d) = \frac{n}{d}$.
- (iii) Für beliebiges $m \in \mathbb{Z}$ gilt $\text{ord}(g^m) = \frac{n}{d}$ mit $d = \text{ggT}(m, n)$.

Aus dem Bezanten folgt $d' = \text{ggT}(m, n) = d$

Beweis von Satz 3.9

geg: Gruppe G , $n \in \mathbb{N}$, $g \in G$ mit $\text{ord}(g) = n$

zu (i) Sei $m \in \mathbb{Z}$ mit $\text{ggT}(m, n) = 1$

z.zg: $\text{ord}(g^m) = n$

Es genügt zu zeigen, dass $\langle g^m \rangle = \langle g \rangle$ gilt.

" $\subseteq$ " klar, denn aus $g^m \in \langle g \rangle$ folgt $\langle g^m \rangle \subseteq \langle g \rangle$

" $\supseteq$ " Lemma von Bezant $\Rightarrow \exists k, l \in \mathbb{Z}$ mit

$$km + ln = 1 \Rightarrow g = g^1 = g^{km+ln} = (g^m)^k (g^n)^l$$

$$= (g^m)^k \cdot e^l = (g^m)^k \in \langle g^m \rangle \Rightarrow \langle g \rangle \subseteq \langle g^m \rangle$$

$\uparrow n = \text{ord}(g)$

zu (ii) Sei $d \in \mathbb{N}$ ein Teiler von n , d.h. es gilt

$$n = kd \text{ für ein } k \in \mathbb{N}$$

Wegen Satz 3.3 gilt die Äquivalenz $g^m = e \iff m \mid n$
für alle $m \in \mathbb{Z}$. z.zg. $\text{ord}(g^d) = \frac{n}{d}$

Sei $m \in \mathbb{Z}$. Dann gilt auch die Äquivalenz

$$(g^d)^m = e \iff g^{dm} = e \stackrel{\text{z.z.}}{\iff} n \mid dm \iff \exists l \in \mathbb{Z} :$$

$$dm = ln \iff \exists l \in \mathbb{Z} : dm = lkd \iff \exists l \in \mathbb{Z} : m = lk$$

$$\iff k \mid m \quad \text{Aus Satz 3.3 folgt } \text{ord}(g^d) = k = \frac{n}{d}$$

zu iii) Sei $m \in \mathbb{Z}$ beliebig, $d = \text{ggT}(m, n)$.

$$\text{z.zg. } \text{ord}(g^m) = \frac{n}{d}$$

Seien $m', n' \in \mathbb{N}$ die natürlichen Zahlen mit $m = m'd$ und
 $n = n'd$. Dann gilt $\text{ggT}(m', n') = 1$

$n = n' d$. Dann gilt $\text{ggT}(m', n') = 1$

Sei $h = g^d$. Regel (ii) ($d \mid n$) $\Rightarrow \text{ord}(h) = \frac{n}{d} = n'$

Regel (i) ($\text{ggT}(m', n') = 1, \text{ord}(h) = n'$) $\Rightarrow \text{ord}(h) = \text{ord}(h^{m'})$

$\Rightarrow$ gilt $g^m = (g^d)^{m'} = h^{m'} \Rightarrow \text{ord}(g^m) = \text{ord}(h^{m'}) =$

$$\text{ord}(h) = \frac{n}{d} = \frac{n}{\text{ggT}(m, n)} \quad \square$$

Die Eulersche φ -Funktion

Die **Eulersche φ -Funktion** ist für jedes $n \in \mathbb{N}$ definiert durch

$$\varphi(n) = |\{k \in \mathbb{Z} \mid 0 \leq k < n, \text{ggT}(k, n) = 1\}|.$$

Sie erfüllt die folgenden Rechenregeln:

- Für alle $m, n \in \mathbb{N}$ mit **$\text{ggT}(m, n) = 1$** gilt $\varphi(mn) = \varphi(m)\varphi(n)$.
- Für jede Primzahl p und jedes $r \in \mathbb{N}$ gilt

$$\varphi(p^r) = p^{r-1}(p-1) = p^r - p^{r-1}.$$

Bedeutung der φ -Funktion für die Gruppentheorie

Sei G eine zyklische Gruppe der Ordnung n und $g \in G$ ein erzeugendes Element.

- Nach Folgerung (3.4) sind g^k mit $0 \leq k < n$ die n verschiedenen Elemente von G .
- Aus Satz (3.9) (i) kann daher abgeleitet werden, dass G insgesamt $\varphi(n)$ Elemente der vollen Ordnung n enthält. Mit anderen Worten, es gibt genau $\varphi(n)$ Elemente h in G mit der Eigenschaft $G = \langle h \rangle$.

Satz (3.10)

Sei G eine Gruppe und $n \in \mathbb{N}$. Ein Element $g \in G$ hat genau dann die Ordnung n , wenn $g^n = e_G$ und für jeden Primteiler p von n jeweils $g^{n/p} \neq e_G$ gilt.

Anwendungsbeispiel für Satz 3.10

Sei G eine Gruppe und $g \in G$ mit $g^{48} = e$,
 $g^{24} \neq e$ und $g^{16} \neq e$. Dann gilt $\text{ord}(g) = 48$.

(denn: 2 und 3 sind die einzigen Primteiler von $48 = 2^4 \cdot 3$
und es ist $\frac{48}{2} = 24$, $\frac{48}{3} = 16$)

Wichtige Anmerkung: Ist G eine endliche Gruppe,
dann ist $\text{ord}(g)$ für jedes $g \in G$ stets ein Teiler von $|G|$.
(Bem.: Satz von Lagrange, angewendet auf $U = \langle g \rangle$)

Beweis von Satz 3.10

geg. G Gruppe, $g \in G$, $n \in \mathbb{N}$ mit $g^n = e$ und
 $g^{n/p} \neq e$ für jeden Primteiler p von n

z.zg: $\text{ord}(g) = n$

$g^n = e$, Satz 3.3 $\Rightarrow \text{ord}(g)$ ist Teiler von n

Ang., $d = \text{ord}(g)$ ist kleiner als n . $\Rightarrow d$ ist Teiler von n kleiner als n , d.h. $\frac{n}{d} \in \mathbb{N}$ und $\frac{n}{d} > 1$. Sei p ein Primteiler von $\frac{n}{d}$.

$\Rightarrow \exists k \in \mathbb{N}$ mit $\frac{n}{d} = kp \Rightarrow n = dkp \Rightarrow g^{n/p} =$

$$g^{\frac{dkp}{p}} = g^{dk} = (g^d)^k \underset{d = \text{ord}(g)}{=} e^k = e \quad \nparallel \text{ zur Vor.} \quad \square$$

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

geg.: zyklische Gruppe G , $g \in G$ ein Element mit $G = \langle g \rangle$

Für jedes $m \in \mathbb{N}$ sei $U_m = \langle g^m \rangle$, außerdem $U_0 = \{e_G\}$. Seien $m, m' \in \mathbb{N}$.

Beh.: $U_m \subseteq U_{m'} \iff m' \mid m$

$$m' \mid m \Rightarrow \exists k \in \mathbb{N} \text{ mit } m = km'$$

$$g^m = g^{km'} = (g^{m'})^k \subseteq \langle g^{m'} \rangle = U_{m'}$$

$$\Rightarrow U_m = \langle g^m \rangle \subseteq U_{m'}$$

Aus
der
 $g^{m'}$
folgt
 $m' \mid m$
und
gilt

Beh.: Unter der Voraussetzung $\text{ord}(g) = \infty$
gilt auch die Umkehrung, d.h. aus
 $U_m \subseteq U_{m'}$ folgt $m' \mid m$.

Setze also $\text{ord}(g) = \infty$ und $U_m \subseteq U_{m'}$
voraus. z. z. $m' \mid m$

$$\begin{aligned} U_m \subseteq U_{m'}, U_m = \langle g^m \rangle &\Rightarrow g^m \in U_{m'} \\ \Rightarrow g^m \in \langle g^{m'} \rangle &\Rightarrow \exists k \in \mathbb{Z} \text{ mit } g^m \\ &= (g^{m'})^k = g^{km'} \quad \text{Nach Satz 3.5 ist} \\ &\text{die Abb. } \mathbb{Z} \rightarrow G, a \mapsto g^a \text{ injektiv.} \\ \text{also: } g^m = g^{km'} &\Rightarrow m = km' \Rightarrow m' \mid m \end{aligned}$$

Betrachte nun den Fall, dass $n = \text{ord}(g)$ endlich
und m, m' beides Teiler von n sind.

Beh. Auch dann gilt die Implikation

$$U_m \leq U_{m'} \Rightarrow m' \mid m$$

Aus $U_m \leq U_{m'}$ folgt wie oben, dass ein $k \in \mathbb{Z}$ mit
der Eigenschaft $g^m = g^{km'}$ existiert. $\Rightarrow$

$$g^{m - km'} = e \quad \text{Wegen Satz 3.3 und } n = \text{ord}(g)$$

folgt daraus $n \mid (m - km')$. $\Rightarrow \exists l \in \mathbb{Z}$ mit

$$m - km' = ln \Rightarrow m = km' + ln \quad \text{Da } km'$$

und ln Vielfache von m' sind (Voraussetzung $m' \mid n$),
gilt dasselbe für m . $\Rightarrow m' \mid m$.