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 $\mathrm{ord}(g) = |\langle g \rangle|$ als die Ordnung von g.

Aus dem Satz von Lagrange folgt unmittelbar: Ist $n = |G|$ endlich, dann ist $\mathrm{ord}(g)$ für jedes $g \in G$ stets ein Teiler von n.

Charakterisierung der Elementordnung

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) $n = \mathrm{ord}(g)$

(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.

Die Ordnung der Permutationen

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 $\mathrm{ord}(\sigma) = k$.

(ii) Ist σ ein Element vom Zerlegungtyp $(k_1, ..., k_r)$, dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(k_1, ..., k_r)$.

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.

Beweis von Satz 3.7:

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

U Untergruppe von G mit $U \neq \{e_G\}$

z.zg: $U = \langle g^m \rangle$ für ein $m \in \mathbb{N}$

Beh: Es gibt ein $m \in \mathbb{N}$ mit $g^m \in U$.

$G = \langle g \rangle \Rightarrow G = \{g^a \mid a \in \mathbb{Z}\}$

$U \neq \{e_G\} \Rightarrow \exists r \in \mathbb{Z} \setminus \{0\}$ mit $g^r \in U$

1. Fall: $r > 0$ nichts zu zeigen (da $r \in \mathbb{N}$)

2. Fall: $r < 0$ Setze $m = -r \Rightarrow m \in \mathbb{N}$ und

$(g^r)^{-1} = g^{-r} = g^m$ Da U eine Untergr. von G ist, folgt aus $g^r \in U$, dass $(g^r)^{-1} = g^m \in U$ ($\Rightarrow$ Beh.)

Sei nun $m \in \mathbb{N}$ minimal mit der Eigenschaft $g^m \in U$

Beh.: $U = \langle g^m \rangle$ „$\supseteq$" folgt aus $g^m \in U$ und der Definition von $\langle g^m \rangle$

„$\subseteq$" Sei $h \in U$. $\overset{h \in G}{\Longrightarrow}$ $\exists\, a \in \mathbb{Z}$ mit $h = g^a$. Division mit Rest $\Rightarrow \exists\, q, r \in \mathbb{Z}$ mit $a = qm + r$ und $0 \leq r < m$

Ang. $r > 0$ (d.h. $r \in \mathbb{N}$) Es gilt $g^r = g^{a - qm} = g^a \cdot (g^m)^{-q} \in U$ ↯ zur Minimalität von m (da $r < m$)

$\in U$ $g^m \in U$

also: $r = 0$, $a = qm \Rightarrow h = g^a = (g^m)^q \in \langle g^m \rangle$

($\Rightarrow$ Beh.)

Setze nun voraus, dass $n = \mathrm{ord}(g)$ endlich ist. Zeige: Dann ist unser minimales m ein Teiler von n. Angenommen, das ist nicht der Fall. Division mit Rest $\Rightarrow \exists\, q_1, r_1 \in \mathbb{Z}$ mit $n = q_1 m + r_1$ und $0 < r_1 < m$. $\Rightarrow$

$$g^{r_1} = g^{n - q_1 m} = g^n (g^m)^{-q_1} = e_G (g^m)^{-q_1}$$

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

$= (g^m)^{-q_1} \in U \lightning$ zur Minimalität von m. $\square$

Das Lemma von Bézout

Satz (3.8)

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

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

Beweis von Satz 3.8:

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

Sei $d = ggT(m,n) \in \mathbb{N}$

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

Betrachte in $(\mathbb{Z}, +)$ die Untergruppe

$U = \langle m, n \rangle \overset{\S 2}{=} \{ km + ln \mid k, l \in \mathbb{Z} \}$

$(m,n) \neq (0,0) \Rightarrow U \neq \{0\}$

Satz 3.7 $\Rightarrow \exists d_1 \in \mathbb{N}$ mit $U = \langle d_1 \rangle$

Überprüfe: d_1 besitzt die definierenden Eigenschaften des ggT von m und n

(Daraus folgt dann also $d_1 = d$.)

Über prüfe dafür: (1) $d_1 \mid m$, $d_1 \mid n$

(2) $d' \in \mathbb{N}$, $d' \mid m$, $d' \mid n \Rightarrow d' \mid d_1$

zu (1) $\langle d_1 \rangle = U = \langle m, n \rangle \Rightarrow m \in \langle d_1 \rangle$

und $n \in \langle d_1 \rangle \Rightarrow \exists k, l \in \mathbb{Z}: m = k d_1, n = l d_1$

$\Rightarrow d_1 \mid m$ und $d_1 \mid n$

zu (2) Sei $d' \in \mathbb{N}$ mit $d' \mid m$ und $d' \mid n$

$\Rightarrow \exists k, l \in \mathbb{Z}$ mit $m = k d'$ und $n = l d'$

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

$\langle d' \rangle \Rightarrow U = \langle m, n \rangle \subseteq \langle d' \rangle \Rightarrow$

$\langle d_1 \rangle \subseteq \langle d' \rangle \Rightarrow d_1 \in \langle d' \rangle \Rightarrow \exists r \in \mathbb{Z}:$

$d_n = r\,d' \Rightarrow d' \mid d_1$

Damit ist gezeigt: $\langle d \rangle = U = \langle m, n \rangle$

$\Rightarrow d \in \langle m, n \rangle \Rightarrow \exists a, b \in \mathbb{Z}: d = am + bn$ □

Rechenregeln für Elementordnungen

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 $\operatorname{ord}(g^m) = n$ genau dann, wenn $\operatorname{ggT}(m, n) = 1$ ist.

(ii) Ist $d \in \mathbb{N}$ ein Teiler von n, dann gilt $\operatorname{ord}(g^d) = \frac{n}{d}$.

(iii) Für beliebiges $m \in \mathbb{Z}$ gilt $\operatorname{ord}(g^m) = \frac{n}{d}$ mit $d = \operatorname{ggT}(m, n)$.

Beweis von Satz 3.9 (nur (i), (ii))

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

zu (i) Sei $m \in \mathbb{Z}$. Beh.: $\operatorname{ord}(g^m) = n \iff \operatorname{ggT}(m,n) = 1$

„$\Leftarrow$" zeige: $\langle g \rangle = \langle g^m \rangle$ (dann folgt $n = \operatorname{ord}(g)$
$= |\langle g \rangle| = |\langle g^m \rangle| = \operatorname{ord}(g^m)$)

„$\supseteq$" $g \in \langle g \rangle$, $\langle g \rangle$ ist Untergr. von $G \Rightarrow g^m \in \langle g \rangle$
$\Rightarrow \langle g^m \rangle \subseteq \langle g \rangle$

„$\subseteq$" Lemma von Bézout $\Rightarrow \exists a, b \in \mathbb{Z}$ mit
$a m + b n = \operatorname{ggT}(m,n) = 1 \Rightarrow g = g^{1} = g^{am+bn}$
$= (g^m)^a (g^n)^b = (g^m)^a e^b = (g^m)^a \in \langle g^m \rangle$
($\operatorname{ord}(g) = n$)

$\Rightarrow \langle g^m \rangle \subseteq \langle g \rangle$

Daraus folgt $\langle g \rangle \subseteq \langle g^m \rangle$

„$\Rightarrow$" Vor.: $\operatorname{ord}(g^m) = n$ z.zg.: $ggT(m,n) = 1$

Sei $d \in \mathbb{N}$ ein gemeinsamer Teiler von m und n. z.zg.: $d = 1$

$g^m \in \langle g \rangle \Rightarrow \langle g^m \rangle \overset{(*)}{\subseteq} \langle g \rangle$ Auf Grund der Vor. gilt

$|\langle g^m \rangle| = |\langle g \rangle| \overset{(*)}{\Longrightarrow} \langle g^m \rangle = \langle g \rangle \Rightarrow g \in \langle g^m \rangle \Rightarrow$

$\exists a \in \mathbb{Z}$ mit $g = (g^m)^a = g^{m \cdot a} \Rightarrow g^{1-ma} = e \overset{\text{Satz 3.3}}{\Longrightarrow}$

$n \mid (1-ma) \Rightarrow \exists b \in \mathbb{Z} : bn = 1 - ma \Rightarrow ma + bn = 1$

$d \mid m, d \mid n \Longrightarrow d \mid 1 \overset{d \in \mathbb{N}}{\Rightarrow} d = 1$

Beweis von Satz 3.9, Teil (ii)

geg. G Gruppe, $g \in G$, $n = \operatorname{ord}(g)$

$d \in \mathbb{N}$ Teiler von n, d.h. $n = k \cdot d$ für ein $k \in \mathbb{N}$

Beh. $\operatorname{ord}(g^d) = \frac{n}{d} = k$

Nach Teil (iii) von Satz 3.3 reicht es zu zeigen:

$$\forall l \in \mathbb{Z}: \quad (g^d)^l = e \iff k \mid l$$

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

$$(g^d)^l = e \iff g^{dl} = e \overset{\text{Satz 3.3 (ii.)}}{\underset{n = \operatorname{ord}(g)}{\iff}} n \mid dl$$

$n = \mathrm{ord}(g)$

$\Rightarrow \exists r \in \mathbb{Z} : dl = rn \Rightarrow \exists r \in \mathbb{Z} : l = r\frac{n}{d} = rk$

$\Rightarrow k \mid l$ $\square$

Die Eulersche φ-Funktion

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

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

Sie erfüllt die folgenden Rechenregeln:

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

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

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 $G = \langle h \rangle$.

Weitere Rechenregel für die Elementordnung

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 zu Satz 3.10:

Sei G eine Gruppe und $g \in G$.

Gilt $g^{48} = e_G$, $g^{24} \neq e_G$, $g^{16} \neq e_G$,

dann folgt $\operatorname{ord}(g) = 48$. (denn:

$48 = 2^4 \cdot 3$, $48/2 = 24$, $48/3 = 16$)

Bem.: Hohe Potenzen von Elementen können durch schnelle Exponentiation ausgerechnet werden. Stelle den Exponenten als Summe von Zweierpotenzen

da, $47 = 32 + 8 + 4 + 2 + 1 =$

$2^5 + 2^3 + 2^2 + 2^1 + 2^0$. Berechnung von g^{47}.

- Berechne erst g^2, $g^4 = (g^2)^2$, $g^8 = (g^4)^2$, $g^{16} = (g^8)^2$, $g^{32} = (g^{16})^2$.
- Berechne $g^{47} = g^{32} \cdot g^8 \cdot g^4 \cdot g^2 \cdot g^1$

Beweis von Satz 3.10:

geg.: Gruppe G, $n \in \mathbb{N}$, $g \in G$

Beh.: $n = \operatorname{ord}(g) \iff g^n = e_G$ und $g^{n/p} \neq e_G$ für jeden Primteiler p von n.

„$\Rightarrow$" $n = \operatorname{ord}(g) \Rightarrow g^n = e_G$

Ang. $g^{n/p} = e_G$ für einen Primteiler p von n

$\Rightarrow \operatorname{ord}(g) \mid \frac{n}{p}$ ↯ zu $n = \operatorname{ord}(g)$

„$\Leftarrow$" Sei $m = \operatorname{ord}(g)$, z.zg.: $m = n$

$g^n = e_G \Rightarrow m \mid n \Rightarrow \exists k \in \mathbb{N}$ mit $n = km$

Ang. $m < n \Rightarrow k > 1 \Rightarrow$ Die Zahl k hat einen Primteiler p. $\Rightarrow \exists\, l \in \mathbb{N}$ mit $k = p \cdot l \Rightarrow n = p\,l\,m$ $\quad m = \mathrm{ord}(g)$

$$\Rightarrow g^{n/p} = g^{\frac{p\,l\,m}{p}} = g^{l\,m} = (g^m)^l \overset{\leftarrow}{=} e_G$$

$\lightning$ zur Voraussetzung $g^{n/p} \neq e_G$ $\square$.

Die Untergruppen einer zyklischen Gruppe, Teil II

Satz (3.11)

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

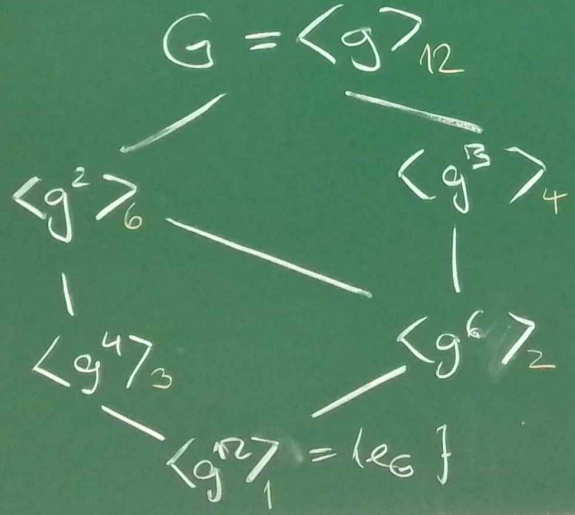
(i) Ist $\operatorname{ord}(g) = \infty$, dann sind die verschiedenen Untergruppen von G gegeben durch $U_0 = \{e_G\}$ und $U_m = \langle g^m \rangle$, wobei m die natürlichen Zahlen durchläuft.

(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.

Beispiel zu Satz 3.11:

Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung 12.
Dann sind $\langle g \rangle$, $\langle g^2 \rangle$, $\langle g^3 \rangle$, $\langle g^4 \rangle$, $\langle g^6 \rangle$ und $\langle g^{12} \rangle$
die Untergruppen von G. Gruppendiagramm:



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.