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 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 mit $U \neq \{e_G\}$

Beh. U ist zyklisch, $U = \langle g^m \rangle$ für ein $m \in \mathbb{N}$

$U \neq \{e_G\} \Rightarrow \exists\, h \in U \setminus \{e_G\}$ $G = \langle g \rangle$, $h \in G$
$\Rightarrow \exists\, r \in \mathbb{Z} \setminus \{0\}$ mit $h = g^r$
Ist $r < 0$, $r = -s$ mit $n \in \mathbb{N}$, dann gilt auch
$g^s = g^{-r} = (g^r)^{-1} = h^{-1} \in U$. also: Auf jeden
Fall existiert ein $s \in \mathbb{N}$ mit $g^s \in U$.

Sei nun $m \in \mathbb{N}$ minimal mit $g^m \in U$, zeige $U = \langle g^m \rangle$.

„$\supseteq$" folgt direkt aus $g^m \in U$ (und der Untergruppen-eigenschaft von U) „$\subseteq$" Sei $h \in U$, z.z.g $h \in \langle g^m \rangle$

$h \in \langle g \rangle$ (da $h \in G$, $G = \langle g \rangle$) $\Rightarrow \exists\, k \in \mathbb{Z}$ mit $h = g^k$

Division mit Rest $\Rightarrow \exists\, q, r \in \mathbb{Z}$ mit $k = qm + r$ und $0 \leq r < m$

1. Fall: $r = 0 \Rightarrow h = g^k = g^{qm} = (g^m)^q \in \langle g^m \rangle$

2 Fall: $0 < r < m \rightarrow g^r = g^{k-qm} = g^k \cdot (g^m)^{-q} = h \cdot (g^m)^{-q}$

$\Rightarrow g^r \in U$ (wegen $g^m, h \in U$) $\lightning$ zur Minimalität von m

($\Rightarrow$ Beh.)

Setze nun voraus, dass $|G| = |\langle g \rangle| = n$ endlich ist.

Beh: Das minimale $m \in \mathbb{N}$ mit $g^m \in U$ ist ein Teiler von n.

Ang. $m \nmid n$. Division mit Rest $\Rightarrow \exists q_1, r_1 \in \mathbb{Z}$ mit $n = q_1 m + r_1$ und $0 \leq r_1 < m$ $m \nmid n$

$\Rightarrow r_1 > 0 \Rightarrow g^{r_1} = g^{n - q_1 m} = g^n \cdot (g^m)^{-q_1}$

$= e_G \cdot (g^m)^{-q_1} = (g^m)^{-q_1} \in \langle g^m \rangle \Rightarrow g^{r_1} \in U$

wg. $\langle g^m \rangle \subseteq U$ $\lightning$ zur Minimalität von m, wg. $0 < r_1 < m$.

□

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 $(m,n) \neq (0,0)$

z.zg $\exists a, b \in \mathbb{Z}$ mit $am + bn = d$, wobei $d = ggT(m,n)$

Betrachte in $(\mathbb{Z}, +)$ die Untergruppe $U = \langle m, n \rangle$

$= \{am + bn \mid a, b \in \mathbb{Z}\}$. $(\mathbb{Z}, +)$ ist zyklisch ($\mathbb{Z} = \langle 1 \rangle$),

es gilt $U \neq \{0\}$, da z.B. $m \in U$. $\overset{\text{Satz 3.7}}{\Rightarrow}$ $\exists d \in \mathbb{N}$

mit $U = \langle d \cdot 1 \rangle = \langle d \rangle$. Beh: $d = ggT(m,n)$

zu überprüfen: (1) $d \mid m$ und $d \mid n$

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

zu (1) $m \in U \Rightarrow m \in \langle d \rangle \Rightarrow \exists k \in \mathbb{Z}: m = k \cdot d \Rightarrow d \mid m$

Zu überprüfen: (1) $d \mid m$ und $d \mid n$

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

Ebenso folgt aus $n \in U$ die Aussage $d \mid n$.

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 $n = l' d' \Rightarrow m, n \in \langle d' \rangle \Rightarrow$

$\langle m, n \rangle \subseteq \langle d' \rangle \Rightarrow U \subseteq \langle d' \rangle \Rightarrow \langle d \rangle \subseteq \langle d' \rangle$ ($S \subseteq U \Rightarrow \langle S \rangle \subseteq U$)

$\Rightarrow d \in \langle d' \rangle \Rightarrow \exists r \in \mathbb{Z}: d = r \cdot d' \Rightarrow d' \mid d$ ($\Rightarrow$ Beh)

$d \in \langle d \rangle \Rightarrow d \in U \Rightarrow \exists a, b \in \mathbb{Z}: am + bn = d$ (und $d = ggT(m, n)$). □

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

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

zu (i) geg. $m \in \mathbb{Z}$ mit $\operatorname{ggT}(m,n) = 1$, z.zg.: $\operatorname{ord}(g^m) = n$

Beh.: $\langle g \rangle = \langle g^m \rangle$ (daraus folgt $\operatorname{ord}(g^m) = |\langle g^m \rangle| = |\langle g \rangle| = n$)

„$\supseteq$" $g^m \in \langle g \rangle \Rightarrow \langle g^m \rangle \subseteq \langle g \rangle$

„$\subseteq$" genügt z.zg.: $g \in \langle g^m \rangle$ (dann folgt $\langle g \rangle \subseteq \langle g^m \rangle$)

$\operatorname{ggT}(m,n) = 1 \overset{\text{Lemma von Bézout}}{\Rightarrow} \exists a, b \in \mathbb{Z}$ mit $1 = am + bn$

$\Rightarrow g = g^1 = g^{am+bn} = (g^m)^a \cdot (g^n)^b = (g^m)^a \cdot e^b$ (mit $e = n = \operatorname{ord}(g)$)

$= (g^m)^a \in \langle g^m \rangle$

zu (ii) Sei nun $d \in \mathbb{N}$ ein Teiler von n.

z.Zg.: $\operatorname{ord}(g^d) = \frac{n}{d}$ Es gilt die Äquivalenz

$\operatorname{ord}(g^d) = \frac{n}{d} \overset{\text{Satz 3.3}}{\Longleftrightarrow} \left(\forall k \in \mathbb{Z} : (g^d)^k = e_G \overset{(*)}{\Longleftrightarrow} \frac{n}{d} \mid k \right)$

Sei also $k \in \mathbb{Z}$, zeige die Äquivalenz (*)

$(g^d)^k = e_G \Longleftrightarrow g^{dk} = e_G \overset{\text{Satz 3.3}}{\underset{n = \operatorname{ord}(g)}{\Longleftrightarrow}} n \mid dk$

$\Longleftrightarrow \exists l \in \mathbb{Z} : dk = ln \Longleftrightarrow \exists l \in \mathbb{Z} : k = l \frac{n}{d}$

$\Longleftrightarrow \frac{n}{d} \mid k$.

zu (iii) Sei $m \in \mathbb{Z}$. Beh.: $\operatorname{ord}(g^m) = \frac{n}{d}$ mit $d = ggT(m,n)$

Sei $m' = \frac{m}{d}$ und $n' = \frac{n}{d}$. Dann gilt $ggT(m',n') = 1$, denn:

Ang. $k > 1$ ist Teiler von m' und n'. $\Rightarrow kd$ ist gem. Teiler von $m = dm'$ und $n = dn'$ $\lightning$ zu $d = ggT(m,n)$

Setze $g_1 = g^d$. Regel (ii) $\rightarrow$ $\operatorname{ord}(g_1) = \frac{n}{d} = n'$

$\Rightarrow \operatorname{ord}(g_1)$ ist teilerfremd zu m' Regel (i) $\rightarrow$

$\operatorname{ord}(g_1) = \operatorname{ord}(g_1^{m'})$. Es gilt $g_1^{m'} = g_1^{m/d} = (g^d)^{m/d}$

$= g^m$. also: $\operatorname{ord}(g^m) = \operatorname{ord}(g_1^{m'}) = \operatorname{ord}(g_1) = \frac{n}{d}$ □

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, $g \in G$. Gilt $g^{48} = e$, $g^{24} \neq e$ und $g^{16} \neq e$, dann folgt $\operatorname{ord}(g) = 48$. (denn: $48 = 16 \cdot 3 = 2^4 \cdot 3^1 \Rightarrow$ einzige Teiler von 48 sind 2, 3, und $\frac{48}{2} = 24$, $\frac{48}{3} = 16$)

Schnelle Berechnung von g^{16}, g^{24}, g^{48}:

$g^4 = (g^2)^2$, $g^8 = (g^4)^2$, $g^{16} = (g^8)^2$, $g^{24} = g^{16} \cdot g^8$

$g^{48} = (g^{24})^2$ (allgemein: Schreibe den Exponenten als Summe von Zweierpotenzen, z.B. $37 = 32 + 4 + 1 \Rightarrow$ erhalte g^{37} durch $g^{32} = (g^{16})^2$, $g^{37} = g^{32} \cdot g^4 \cdot g$)

Beweis von Satz 3.10

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

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

„$\Rightarrow$" $\operatorname{ord}(g) = n \overset{\text{Satz 3.3}}{\Rightarrow} g^n = e$ Ang p Primteiler von n, $g^{n/p} = e$

$\overset{\text{Satz 3.3}}{\Rightarrow} \operatorname{ord}(g) \mid \frac{n}{p}$ ↯ zu $n = \operatorname{ord}(g)$

„$\Leftarrow$" $g^n = e \overset{\text{Satz 3.3}}{\Rightarrow} \operatorname{ord}(g) \mid n$ Ang $\operatorname{ord}(g) < n$. $\Rightarrow \frac{n}{\operatorname{ord}(g)} > 1$

Sei p ein Primteiler von $\frac{n}{m}$, wobei $m = \operatorname{ord}(g)$

$\Rightarrow \exists k \in \mathbb{N}: \frac{n}{m} = k \cdot p \Rightarrow \frac{n}{p} = k \cdot m \Rightarrow g^{n/p} = g^{km} = (g^m)^k$

$= e^k = e$

$\Sigma m = \operatorname{ord}(g)$ ↯ zu $g^{n/p} \neq e$. □

Die Untergruppen einer zyklischen Gruppe, Teil II

Satz (3.11)

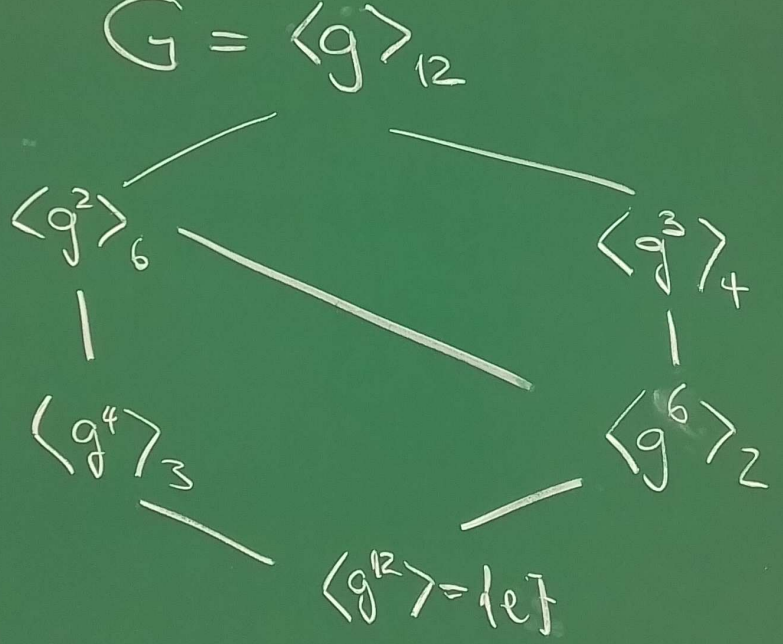
Sei G eine zyklische Gruppe und $g \in G$ mit $G = \langle g \rangle$.

(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.

Untergruppen einer zyklischen Gruppe $G = \langle g \rangle$ der Ordnung 12:



$= g^m$. also: $\operatorname{ord}(g^m) = \operatorname{ord}(g_1^{m'}) = \operatorname{ord}(g_1) = \frac{n}{d}$. □

Beweis von Satz 3.11:

zu (i) Bereits bekannt. Alle Untergruppen von G zyklisch hier haben die Form $\langle g^m \rangle$ mit $m \in \mathbb{N}$. Um zu zeigen, dass die Gruppen $U_m = \langle g^m \rangle$ mit $m \in \mathbb{N}$ alle verschieden sind, genügt es z.Zg: $\forall m, m' \in \mathbb{N}: U_m \subseteq U_{m'} \overset{(*)}{\iff} m' \mid m$

(denn: Seien $m, m' \in \mathbb{N}$ mit $U_m = U_{m'} \Rightarrow U_m \subseteq U_{m'}$ und $U_{m'} \subseteq U_m$ $\Rightarrow m' \mid m$ und $m \mid m' \overset{m, m' \in \mathbb{N}}{\Rightarrow} m = m'$)

Seien also $m, m' \in \mathbb{N}$. „$\Leftarrow$" Vor. $\Rightarrow \exists k \in \mathbb{N}: m = k m'$

z.Zg: $\langle g^m \rangle \subseteq \langle g^{m'} \rangle$, genügt: $g^m \in \langle g^{m'} \rangle$ Dies ist erfüllt, wegen $g^m = g^{km'} = (g^{m'})^k \in \langle g^{m'} \rangle$

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

$\Rightarrow \exists k \in \mathbb{Z} : g^m = (g^{m'})^k = g^{m'k}$

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

$\Rightarrow$ $m = m'k \Rightarrow m' \mid m$

Satz 3.5
$\mathbb{Z} \to G, k \mapsto g^k$
ist injektiv

zu (ii) Es genügt, für bel. Teiler $d, d' \in \mathbb{N}$ von n folgende Äquivalenz zu zeigen:

$$U_d \subseteq U_{d'} \iff d' \mid d$$

„$\Leftarrow$" läuft wie unter (i)

„$\Rightarrow$" $U_d \subseteq U_{d'} \Rightarrow \langle g^d \rangle \subseteq \langle g^{d'} \rangle \Rightarrow$

$g^d \in \langle g^{d'} \rangle \Rightarrow \exists k \in \mathbb{N}$ mit $g^d = (g^{d'})^k =$

$g^{kd'} \Rightarrow g^d \cdot (g^{kd'})^{-1} = e \Rightarrow g^{d-kd'} = e$

Satz 3.3 $\Rightarrow n \mid (d-kd') \Rightarrow \exists l \in \mathbb{Z} : nl = d-kd'$

$d' \mid n \rightarrow \exists s \in \mathbb{N} : n = sd' \Rightarrow sd'l = d-kd'$

$\Rightarrow sd'l + kd' = d \rightarrow d'(sl+k) = d$

$\Rightarrow d' \mid d$