Definition der Gruppen- und Elementordnung

Definition

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.

Charakterisierung der Elementordnung

Satz

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.

Rechenregeln für Elementordnungen

Satz

Sei G eine Gruppe und $g \in G$ mit $n = \mathrm{ord}(g)$, $n \in \mathbb{N}$.

(i) Für beliebiges $m \in \mathbb{Z}$ gilt $\mathrm{ord}(g^m) = n$ genau dann, wenn $\mathrm{ggT}(m, n) = 1$ ist.

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

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

(iv) Ein Element $h \in G$ hat genau dann die Ordnung n, wenn $h^n = e_G$ und für jeden Primteiler p von n jeweils $h^{n/p} \neq e_G$ gilt.

Die Struktur endlicher abelscher Gruppen

Satz (*Chinesischer Restsatz*)

Für alle $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$ gilt

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(mn)\mathbb{Z}.$$

Mit anderen Worten, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ist eine zyklische Gruppe der Ordnung mn.

wichtiger Hinweis:

Im Fall $\mathrm{ggT}(m, n) > 1$ wird die Aussage falsch.

- Zum Beispiel ist $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ nicht isomorph zu $\mathbb{Z}/4\mathbb{Z}$.
- Das direkte Produkt zyklischer Gruppen ist im Allgemeinen nicht zyklisch.

Die Struktur endlicher abelscher Gruppen (Forts.)

Satz (*Hauptsatz über endliche abelsche Gruppen*)

Jede endliche abelsche Gruppe G ist isomorph zu einem direkten Produkt zyklischer Gruppen. Es gibt also ein $r \in \mathbb{N}_0$ und $m_1, ..., m_r \in \mathbb{N}$ mit

$$G \quad \cong \quad \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}.$$

Dabei können die Zahlen m_j so gewählt werden, dass

- es sich um Primzahlpotenzen handelt oder
- für $1 \leq j \leq r-1$ jeweils $m_j \mid m_{j+1}$ gilt.

Ergänzung:

Auch jede endlich erzeugte abelsche Gruppe ist Produkt zyklischer Gruppen, also isomorph zu einer Gruppe der Form

$$\mathbb{Z}^s \times \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}.$$

Anwendungsbeispiel: $2^2 \cdot 5^2 = 100$

Die Isomorphietypen (abelschen) von Gruppen der Ordnung 100 werden repräsentiert durch

$G_1 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$, $G_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,

$G_3 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $G_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

oder auch durch

$H_1 = \mathbb{Z}/100\mathbb{Z}$, $H_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$,

$H_3 = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$, $H_4 = \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

Achtung: Sind G_1 und G_2 zwei endliche Gruppen mit $|G_1| = |G_2|$ und der Eigenschaft, dass für jedes $d \in \mathbb{N}$ die Gruppe G_1 genauso viele Elemente der Ordnung d hat wie G_2, dann folgt daraus im Allgem. nicht $G_1 \cong G_2$.

Bsp: Die Gruppen $G_1 = (\mathbb{Z}/3\mathbb{Z})^3$ und $G_2 = \left\{ \begin{pmatrix} \bar{1} & a & b \\ 0 & \bar{1} & c \\ 0 & 0 & \bar{1} \end{pmatrix} \mid a, b, c \in \mathbb{F}_3 \right\}$ sind beides Gruppen der Ordnung 27 und haben beide 26 Elemente der Ordn. 3 sind aber nicht isomorph (G_1 ist abelsch, G_2 nicht)

F24T2A3

(a) Gibt es eine Gruppe G, die außer dem Neutralelement e genau 4 Elemente der Ordnung 5 und 6 Elemente der Ordnung 2 enthält?

Gesamtzahl der Elemente in G: 1 + 4 + 6 = 11 → G ist Gruppe der Ordnung 11

Jede Elementordn. muss nach dem Satz von Lagrange ein Teiler von |G| = 11 sein, also

in $\mathbb{Z}_{11}, \mathbb{Z}_7$ liegen. Insb. gibt es in einer solchen Gruppe keine El. der Ordn. 5 (oder 2).

↯ Antwort also: Nein.

(b) Existiert eine abelsche Gruppe, bei der die Anzahl der Elemente bestimmter Ordnung durch folgende Tabelle gegeben ist?

Ordnung	1	2	4
Anzahl	1	3	12

Falls ja, ist die Gruppe eindeutig bestimmt bzw. auch Isomorphie?

F24T2A3 (b)

Vorüberlegung:

Die gesuchte abelsche Gruppe hat die Ordnung $1 + 3 + 12 = 16$. Nach dem Hauptsatz für endliche abelsche Gruppe stimmt G bis auf Isomorphie überein mit einem Produkt zyklischer Gruppen, wobei das Produkt der Ordnungen der zyklischen Faktoren 16 ergeben muss.

Die einzigen möglichen Ordnungen der Faktoren sind 2, 4, 8 und 16 (falls wir triviale Faktoren der Ordnung 1 außer Acht lassen). Weil es in der Gruppe nur Elemente der Ordnung ≤ 4 vorkommen, sind Faktoren der Ordnung 8 und 16 ausgeschlossen. Weil es Elemente der Ordnung 4 gibt, muss mindestens ein Faktor der Ordnung 4 vorkommen.

F24T2A3 (b) (Forts).

Damit bleiben als einzige Möglichkeiten die Isomorphietypen

$$(\mathbb{Z}/4\mathbb{Z})^2 \quad \text{und} \quad \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2.$$

Um unter diesen beiden Möglichkeiten den richtigen Typ zu finden, betrachten wir nun die Anzahl der Elemente der Ordnung 2 in beiden Gruppen. Allgemein gilt: Ist G eine Gruppe der Form

$$\mathbb{Z}/2^{e_1}\mathbb{Z} \times \mathbb{Z}/2^{e_2}\mathbb{Z} \times ... \times \mathbb{Z}/2^{e_r}\mathbb{Z}$$

mit $e_1, ..., e_r \in \mathbb{N}$, dann gibt es in G genau $2^r - 1$ Elemente der Ordnung 2, nämlich die ...

Elemente der Form $(a_1, \dots, a_r)$ mit $a_j \in \{\bar{0}, \bar{2}^{e_j - 1}\}$ für $1 \leq j \leq r$ abzüglich des Neutralelements $\Rightarrow$ 3 Elemente der Ordn. 2 in $(\mathbb{Z}/4\mathbb{Z})^2$, 7 Elemente der Ordn. 2 in $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^2$. $\Rightarrow (\mathbb{Z}/4\mathbb{Z})^2$ ist die gesuchte Gruppe)]

Beh.: Die Gruppe $(\mathbb{Z}/4\mathbb{Z})^2$ hat die gewünschte Eigenschaft.

- Einziges Element der Ordnung 1 ist das Neutralelement $(\bar{0}, \bar{0})$.
- Wegen $4 \cdot (a, b) = (\bar{0}, \bar{0}) \quad \forall (a, b) \in (\mathbb{Z}/4\mathbb{Z})^2$ ist die Ordnung jedes Elements ein Teiler von 4.

d.h. es sind nur drei Elementordn. 1, 2 oder 4 möglich.

- Ist $a \in \{\bar{1}, \bar{3}\}$ oder $b \in \{\bar{1}, \bar{3}\}$, dann ist (a, b) von Ordnung 4, denn wegen $2 \cdot \bar{1} = \bar{2} \neq \bar{0}$ oder $\bar{2} \cdot \bar{3} = \bar{6} = \bar{2} \neq \bar{0}$ ist $2 \cdot (a, b) = (\bar{0}, \bar{0})$ für ein solches Element ausgeschlossen. Anzahl dieser Elemente:

$$16 - 4 = 12$$

$|(\mathbb{Z}/4\mathbb{Z})^2|$ — Anzahl der Elt (a,b) mit $a, b \notin \{\bar{1}, \bar{3}\}$ $(\Rightarrow a, b \in \{\bar{0}, \bar{2}\})$

- Die übrigen drei Elemente ($16 - 1 - 12 = 3$) müssen also von Ordnung 2 sein.

Übung:

- F25T3A2 (V) Zeigen Sie, dass es 10 paarweise nicht isomorphe abelsche Gruppen der Ordnung 2025 gibt.
- H24T3A1

F12T2A2 Sei G eine endliche Gruppe und p eine Primzahl. Zeigen Sie, dass die Anzahl der Elemente der Ordnung p durch $p-1$ teilbar ist.
(Übung: F25T1A4 verwendet Gruppenoperationen)

Elemente der Ordnung p durch $p-1$ teilbar ist.

[Erinnerung: Die Anzahl der Elemente der Ordnung n in einer zykl. Gruppe der Ordn. n beträgt $\varphi(n)$.
($G = \langle g \rangle$, $\operatorname{ord}(g) = n \Rightarrow \operatorname{ord}(g^m) = n$ für $0 \leq m < n$ mit $\operatorname{ggT}(m, n) = 1$. p Primzahl $\Rightarrow \varphi(p) = p - 1$]

Es sei $\mathcal{E}$ die Menge der Elemente $g \in G$ mit $\operatorname{ord}(g) = p$ und $\mathcal{U}$ die Menge der Untergr. $U \leq G$ mit $|U| = p$.
Dann ist durch $g \mapsto \langle g \rangle$ offenbar eine Abbildung $\phi : \mathcal{E} \to \mathcal{U}$ definiert. Da jede Untergruppe der Ordnung p zyklisch ist (da p Primzahl) ist die Abb. ϕ surjektiv.

Für jedes $g \in \mathcal{E}$ gilt $\phi^{-1}(\langle g \rangle) \overset{(*)}{=} \langle g \rangle \setminus \{e\}$,
d.h. es werden jeweils $p-1$ Elemente aus $\mathcal{E}$ auf
dasselbe Element in $\mathcal{U}$ abgebildet, wg. $|\langle g \rangle \setminus \{e\}|$
$= |\langle g \rangle| - 1 = p - 1$.

Nachweis von $(*)$, für geg. $g \in \mathcal{E}$:

„$\supseteq$" Sei $h \in \langle g \rangle \setminus \{e\}$, z.zg.: $\phi(h) = \langle g \rangle$

gleichbed.: $\langle h \rangle = \langle g \rangle$ $\quad h \in \langle g \rangle \Rightarrow$

$\langle h \rangle \subseteq \langle g \rangle \overset{|\langle h \rangle| = |\langle g \rangle| = p}{\Longrightarrow} \langle g \rangle = \langle h \rangle$

„$\subseteq$" Sei $h \in \phi^{-1}(\langle g \rangle)$. $\Rightarrow \langle h \rangle = \phi(h) = \langle g \rangle$

$\Rightarrow h \in \langle g \rangle$ Wegen $\operatorname{ord}(h) = p$ gilt $h \neq e$.

$\langle h \rangle \subseteq \langle g \rangle \overset{|\langle h \rangle| = |\langle g \rangle| = p}{\Rightarrow} \langle g \rangle = \langle h \rangle$

$\Rightarrow h \in \langle g \rangle \setminus \{e\}$ ($\Rightarrow$ Beh.)

also: $|\Sigma| = \left| \bigcup_{u \in U} \phi^{-1}(u) \right| = \sum_{u \in U} |\phi^{-1}(u)|$

ϕ surj.

s.o. $= \sum_{u \in U} (p-1) = |U| \cdot (p-1)$ (**)

Weil G endlich ist, muss auch U endl. sein.

Aus (**) folgt also $(p-1) \mid |\Sigma|$. □

Regeln für die φ-Funktion:

- $\varphi(mn) = \varphi(m)\,\varphi(n)$ $\forall\, m, n \in \mathbb{N}$ mit $ggT(m,n) = 1$
- $\varphi(p^e) = p^{e-1}(p-1)$ falls p Primzahl, $e \in \mathbb{N}$