Ordnung einer Gruppe

Definition Ordnung einer Gruppe

Sei G eine (multiplikative) endliche Gruppe mit neutralem Element 1.

1. Die *Ordnung* von G ist $\mathrm{ord}(G) := |G|$.
2. Die *Ordnung* eines Elements $a \in G$ ist
$$\mathrm{ord}_G(a) := \min\{i \in \mathbb{N} \mid a^i = 1\}.$$
3. $H \subseteq G$ heißt *Untergruppe* von G, falls H eine Gruppe ist.
4. Wir bezeichnen mit $\langle a \rangle := \{a, a^2, a^3, \ldots, a^{\mathrm{ord}_G(a)}\}$ die *von a erzeugte Untergruppe*.
5. Die von einem Element a erzeugten Gruppen heißen *zyklisch*. Das Element a heißt *Generator* oder auch *primitives Element*.

Beispiel für Ordnungen und Untergruppen

Beispiel: $G = \mathbb{Z}_7^*$

- Die Ordnung von $\mathbb{Z}_7^*$ ist $\mathrm{ord}(\mathbb{Z}_7^*) = |\{1,2,3,4,5,6\}| = 6$.
- $\mathrm{ord}_G(4) = 3$, denn $4^1 = 4, 4^2 = 2$ und $4^3 = 1$.
- $H = \{1,2,4\}$ ist eine Untergruppe.
- In H gilt $2 \cdot 4 = 1$, d.h. $2^{-1} = 4$ und $4^{-1} = 2$.
- $H = \langle 4 \rangle$ ist eine zyklische Untergruppe der Ordnung 3 mit Generatoren 2 und 4.
- $\mathbb{Z}_7^* = \langle 3 \rangle$ ist ebenfalls zyklisch.
- $\langle 6 \rangle = \{1,6\}$ ist eine Untergruppe der Ordnung 2.
- $\langle 1 \rangle = \{1\}$ ist eine Untergupppe der Ordnung 1.

Satz von Euler

Satz von Euler

Sei G eine (multiplikative) Gruppe mit neutralem Element 1. Dann gilt für alle $a \in G$ die Identität $a^{|G|} = 1$.

Beweis:

- Sei $G = \{g_1, \ldots, g_n\}$, d.h. $n = \mathrm{ord}(G) = |G|$.
- Wir betrachten die Abbildung $f : G \to G$, $g \mapsto ag$.
- f ist bijektiv mit Umkehrabbildung $f^{-1} : G \to G$, $g \mapsto a^{-1}g$.
- Da f bijektiv ist, gilt $G = f(G)$ bzw. $\{g_1, \ldots, g_n\} = \{ag_1, \ldots, ag_n\}$.
- Daraus folgt $\prod_{i=1}^{n} g_i = \prod_{i=1}^{n} ag_i = a^n \prod_{i=1}^{n} g_i$.
- Damit gilt $a^n = a^{|G|} = 1$.

Elementordnung

Satz Elementordnung

Sei G eine endliche (muliplikative) Gruppe. Dann gilt für alle $a \in G$ die Ungleichung $\mathrm{ord}_G(a) \leq \mathrm{ord}(G)$.

Beweis:

- **Annahme:** Sei a ein Element mit $k = \mathrm{ord}_G(a) \geq |G| + 1$.
- Wir betrachten die Abbildung $f : [k] \to G$, $i \mapsto a^i$.
- Nach Schubfachprinzip muss es $i < j$ mit $i, j \in [k]$ geben mit $f(i) = f(j)$, d.h. $a^i = a^j$.
- Multiplikation mit $(a^i)^{-1}$ liefert $a^{j-i} = 1$ mit $0 < j - i < k$. (Widersprich: $\mathrm{ord}_G(a) = k$ nach Voraussetzung)

Elementordnung teilt Gruppenordnung

Satz Elementordnung teilt Gruppenordnung

Sei G eine endliche (multiplikative) Gruppe. Dann gilt für alle $a \in G$, dass $\mathrm{ord}_G(a) | \mathrm{ord}(G)$.

Beweis:

- **Annahme:** $ord_G(a)$ teilt $\mathrm{ord}(G)$ nicht
- Division mit Rest liefert $\mathrm{ord}(G) = q \cdot \mathrm{ord}_G(a) + r$ mit
$$0 < r < \mathrm{ord}_G(a).$$
- Es gilt $a^r = a^{\mathrm{ord}(G) - q \cdot \mathrm{ord}_G(a)} = (a^{\mathrm{ord}(G)})(a^{\mathrm{ord}_G(a)})^{-q} = 1 \cdot (1^q)^{-1} = 1.$
(Widerspruch zur Minimalität von $\mathrm{ord}_G(a)$)

Nebenklassen von Untergruppen

Definition Nebenklasse

Sei $(G, \cdot)$ eine abelsche Gruppe und $H \subseteq G$ eine Untergruppe von G. Für jedes $b \in G$ heißt $b \cdot H = \{b \cdot h \mid h \in H\}$ *Nebenklasse* von H.

Bsp:

- Betrachte $G = (\mathbb{Z}_8, +)$. $H = \{0, 4\}$ ist eine Untergruppe von G.
- Nebenklassen sind

$$1 + H = \{1, 5\}, 2 + H = \{2, 6\}, 3 + H = \{3, 7\}, 4 + H = H.$$

- Betrachte $G = (\mathbb{Z}_7^*, \cdot)$ mit Untergruppe $H = \{1, 2, 4\}$.
- Nebenklassen sind

$$2H = \{2, 4, 1\} = H = 4H, 3H = \{3, 6, 5\} = 6H = 5H.$$

Eigenschaften von Nebenklassen

Satz Eigenschaften von Nebenklassen

Sei $(G, \cdot)$ eine abelsche Gruppe und $H \subseteq G$ eine Untergruppe.

1. $hH = H$ für alle $h \in H$.
2. Für $a, b \in G$ gilt entweder $aH = bH$ oder $aH \cap bH = \emptyset$.
3. $|aH| = |H|$ für alle $a \in G$.
4. Die Nebenklassen aH für $a \in G$ partitionieren G.

Beweis:

- **ad 1**: Die Abgeschlossenheit von H liefert $hH \subseteq H$.
- Bleibt zu zeigen, dass $H \subseteq hH$. Sei $g \in H$ beliebig.
- Dann gilt $g = 1g = hh^{-1}g = h(h^{-1}g) \in hH$.
- **ad 2**: Sei $a, b \in G$ mit $aH \cap bH \neq \emptyset$.
- Dann gibt es $h_1, h_2 \in H$ mit $ah_1 = bh_2$.
- Damit gilt $aH = (bh_1^{-1}h_2)H = b(h_1^{-1}h_2H) = bH$.

Eigenschaften von Nebenklassen

Beweis Fortsetzung:

- **ad 3**: Sei $a \in G$. Betrachten die Abbildung $f : H \to aH, h \mapsto ah$.
- f ist eine Bijektion in G, d.h. $|H| = |aH|$ nach Gleichheitsregel.
- **ad 4**: $1 \in H$, da H eine Gruppe ist.
- Daher gilt $a \in aH$ für alle $a \in G$. D.h. $G \subseteq \bigcup_{a \in G} aH$.
- Aufgrund der Abgeschlossenheit von G gilt auch $\bigcup_{a \in G} aH \subseteq G$.
- Aufgrund von 2. bilden die Nebenklassen aH eine Partition von H.

Index einer Untergruppe

Definition Index einer Untergruppe

Sei G eine abelsche Gruppe und $H \subseteq G$ eine Untergruppe. Wir bezeichnen mit G/H die Menge der Nebenklassen von G. Die Kardinalität von G/H heißt *Index von H* in G, d.h. $\mathrm{ind}_G(H) = |G/H|$. Alternativ verwendet man für den Index auch die Notation $[G : H]$.

Bsp:

- Sei $G = (\mathbb{Z}_8, +)$ und $H = \{0, 4\}$.
- Dann gilt $G/H = \{H, 1 + H, 2 + H, 3 + H\}$, d.h. $\mathrm{ind}_G(H) = 4$.
- Sei $G = (\mathbb{Z}_7^*, \cdot)$ und $H = \{1, 2, 4\}$.
- Dann gilt $G/H = \{H, 3H\}$, d.h. $\mathrm{ind}_G(H) = 2$.

Untergruppenordnung teilt Gruppenordnung

Satz von Lagrange

Sei G eine abelsche Gruppe und $H \subseteq G$ eine Untergruppe. Dann gilt $|G| = |H| \cdot \mathrm{ind}_G(H)$, d.h. insbesondere $\mathrm{ord}_G(H)$ teilt $\mathrm{ord}(G)$.

Beweis:

- Alle Nebenklassen von H besitzen dieselbe Kardinalität $|H|$.
- Es gibt $\mathrm{ind}_G(H)$ viele verschiedene Nebenklassen von H in G.
- Alle Nebenklassen bilden eine Partition von G.

Die Faktorgruppe G/H

Satz Faktorgruppe G/H

Sei G eine abelsche Gruppe mit Untergruppe $H \subseteq G$. Dann ist G/H zusammen mit der Multiplikation $\cdot : G/H \times G/H \to G/H$, $(aH, bH) \mapsto abH$ eine Gruppe, die sogenannte *Faktorgruppe*.

Beweis:

- Wir zeigen zunächst die Repräsentanten-Unabhängigkeit der Multiplikation, d.h. die Multiplikation ist wohldefiniert.
- Seien $aH = a'H$, $bH = b'H$.
- Es gilt $a \in aH = a'H$ und $b \in bH = bH'$.
- Damit gibt es $h_1, h_2 \in H$, so dass $a = a'h_1$ und $b = b'h_2$.
- Es folgt $abH = (a'h_1b'h_2)H = a'b'(h_1h_2H) = a'b'H$.
- Damit ist die Multiplikation unabhängig von den Repräsentanten.
- **Neutrales** Element von G/H ist H, denn $aH \cdot H = aH$.
- **Inverses** Element von aH in G/H ist $a^{-1}H$, wobei a^{-1} das inverse Element von a in G ist. Es gilt $a^{-1}H \cdot aH = a^{-1}aH = H$.

Beispiele für Faktorgruppen

Bsp:

- $G = (\mathbb{Z}, +)$ mit Untergruppe $H = 3\mathbb{Z}$.
- Nebenklassen sind $H = 3\mathbb{Z}, 1 + H = 1 + 3\mathbb{Z}$ und $2 + H = 2 + 3\mathbb{Z}$.
- Repräsentanten-Unabhängigkeit: $H = 6 + H$ und $2 + H = 5 + H$.
- Dann gilt $H + 2 + H = 2 + H = (6 - 6 + 5 - 3) + H$
  $= 6 + 5 + (-6 - 3 + H) = 6 + 5 + H$.
- Neutrales Element ist H, denn $H + a + H = a + H$.
- Inverses Element zu $a + H \neq H$ ist $(-a) + H$, denn
  $a + H + (-a) + H = 0 + H = H$.
- **Man beachte:** Unsere Gruppe $(\mathbb{Z}_m, +)$ ist lediglich eine alternative Notation für die Faktorgruppe $(\mathbb{Z}/m\mathbb{Z}, +)$.

- $G = \mathbb{Z}_7^*$ mit Untergruppe $H = \{1, 2, 4\} = 2H = 4H$
- Nebenklassen sind H und $H_2 = \{3, 5, 6\} = 3H = 5H = 6H$.
- H ist neutrales Element, denn $H \cdot H = H$ und $H \cdot H_2 = H_2$.
- $(H_2)^{-1} = (3^{-1}H) = 5H = H_2$, denn $H_2 \cdot H_2 = H$.