Inhaltsverzeichnis

§1 Gruppen

1.1 Gruppe Eine nicht leere Menge G mit einer Verknüpfung $\circ$ ($\circ$ $G \times G \to G$) heißt Gruppe falls:

Assoziativität $(a \circ b) \circ c = a \circ (b \circ c) \;\; \forall\, a, b, c \in G$

Neutrales Element Es gibt ein $e \in G$ mit $e \circ a = a \circ e = a \;\forall\, a \in G$

Inverses Element Zu jedem $a \in G$ gibts ein $a' \in G$, mit $a \circ a' = a' \circ a = e$

Gilt zudem $a \circ b = b \circ a \;\forall\, a, b \in G$ so nennen wir $(G, \circ)$ *abelsch*

Beispiele

- $(\mathbb{Z}, +), (\mathbb{Q}\backslash\{0\}, \times), (V, +)$ für Vektorraum V abelsche Gruppe.
- $(\mathbb{Z}/_m\mathbb{Z}$ zyklische Gruppe, S_n symmetrische Gruppe (für $n \geq 3$ $S_n$ist nicht abelsch)

1.3 Bemerkung

Wir schreiben a^{-1} für das inverse Element und 1_G für das neutrale Element in G.

1.4 Zykelgruppe Beispiel

Für eine Menge $X \neq \emptyset$ definiert man: $S_n = \{f : X \to X| \; bijektiv\}$ eine Gruppe bezuglich $\circ$ mit id_X als neutrales Element (Umkehrabbildung = Inverses Element)
Bei $X = 1, \ldots, n$ schreiben wir S_n statt S_x (symmetrische Gruppe von Grad n) $|S_n| = n$.

Zykelschreibweise:

Sei $\pi \in S_n$, wir schreiben $(a_1, \ldots, a_n)$ für π falls

$$\pi(a_i) = \begin{cases} a_{i+1}, & \text{falls } 1 \leq i \leq r \\ a_1, & \text{falls} i = r \end{cases}$$

$$\pi(x) = \begin{cases} x, & \text{falls} x \notin a_1, \dots, a_r \end{cases}$$

Zum Beispiel:

$$S_3 \ni (1\,2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$S_3 \ni (1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$(1\,2\,3)(4\,5)$ ist kein *Zykel*, aber das Produkt zweir ***disjunkter*** *Zykel*

1.5 Untergruppe Sei $(G, \circ)$ eine Gruppe und $U \subset G$. Diese Teilmenge U heißt Untergruppe (UG) von Gruppe G (geschrieben $U \leq G$, falls:

- $1_G \in U$
- $U^{-1} \in U \;\forall\, u \in U$
- $u \circ u' \in U \;\forall\, u, u' \in U$

1.6 Bemerkung

1. U ist selbst eine Gruppe $G \leq G$ & $\{1_G\} \leq G$
2. Für eine Familie $\{U_i\}_{i \in I}$ von Untergruppe von G ist $\bigcap_{i \in I} U_i$ eine Untergruppe von G
3. $\bigcup_{i \in I} U_i$ ist **keine** Untergruppe

1.7 Erzeugnis Sei $(G, \circ)$ eine Gruppe und $S \subseteq G$ eine Menge. Weiterhin sei $\{S_i\}$ die Familie von aller möglichen Untergruppen von G . Dann heißt die Untergruppe $\langle S \rangle = \bigcap S_i$ erzeugte Untergruppe oder das Erzeugnis von S

Beispiel

- $\langle \emptyset \rangle \{1_G\}$
- $\langle G \rangle = G$
- $S_n = \langle Zykel \rangle = \langle \{i, j | i \neq j;\; i, j \in \{1, \dots, n\}\} \rangle = \langle \{(i, i+1) | 1 \leq i \leq n\} \rangle = \langle \{(1, 2)(1, 2, \dots, n)\} \rangle$.

Sei $(G, \circ)$ eine Gruppe und $g \in G$. Dann $\langle g \rangle := \langle \{g\} \rangle$. Es gilt $\langle g \rangle = \{g^i : i \in \mathbb{Z}\}$

$$g^i = \begin{cases} \underbrace{g \cdot g \dots g}_{i\ mal}, & \text{falls } i > 0 \\ 1_G, & \text{falls } i = 0 \\ (g^{-i})^{-1}, & \text{falls} i < 0 \end{cases}$$

1.8 Ordnung Für eine Gruppe $(G, \circ)$ mit $g \in G$ heißt $|G|$ die Ordnung von Gund$|\langle g \rangle|$ die Ordnung von g . Wir schreiben $ord(g) = |\langle g \rangle|$.

1.9 Beispiel

a) Für $G = S_4$ gilt:

$$ord((1\,2)) = 2$$

$$ord((1\,2\,3)) = 3$$

$$ord((1\,2\,3\,4)) = 4$$

Für $G = S_{10}$ gilt:

$$ord((1\,2\,3\,4\,5)(6\,7)) = 10$$

$$ord(\underbrace{(1\,2\,3\,4\,5)(1\,6)}_{disjunkt}) = ord((1\,6\,2\,3\,4\,5)) = 6$$

b) G heißt zyklisch, falls $G = \langle g \rangle$ für eine $g \in G$

Alle Untergruppe von $(\mathbb{Z}, +)$

Behauptung: Alle Untergruppe von $\mathbb{Z}, +)$ sind in der Form $m\mathbb{Z}$

Beweis. Sei $U \leq \mathbb{Z}$ falls $U = \{0_G\}$ (trivale Untergruppe) dann $U = 0\mathbb{Z}$, ansonsten sei m minimal im $U \cap (\mathbb{N}\ 0)$. Somit $m \in U$ und $m\mathbb{Z} \in U$ da $m + m \in U, 2m + m \in U, -m \in U$.
Sei $n \in U/m\mathbb{Z}$. Dann $n = am + r$ mit $r \in 1, \ldots, m-1$ (Kann nicht 0 sein, da $n \in U/m\mathbb{Z}$. Dann $r = n - m\dot{a} = \underbrace{n}_{\in U} + \underbrace{(-ma)}_{\in m\mathbb{Z}} \in U$. Wobei $r < m$. Wiederspruch zur Definition von m . Also $U = m\mathbb{Z}$

□

1.10 Gruppenhomomorphismus Seien $(G, \cdot)$ und $(H, *)$ Gruppen. Wir nenne $\gamma : G \to H$ Gruppenhomomorphismus falls

$$\gamma\,(g_1 \cdot g_2) = \gamma(g_1) * \gamma(g_2) \quad \forall g_1, g_2 \in G$$

$G \cong H$ (G und H sind isomorph) falls eine bijektiven Gruppenhomomorphismus gibt.

Beispiel

Sei $\gamma : (\mathbb{Z}, +) \to (\mathbb{R}_{>0}, \circ), \quad x \mapsto e^x$ ist ein Gruppenhomomorphismus

1.11 Lemma Sei $\emptyset \neq S \subset G$ Dann $\langle S \rangle = \{s_1, \ldots, s_r |\ r \leq 1, s_i \in S \cup S^{-1}\} =: H$. Wobei
$A^{-1} := \{a^{-1} |\ a \in A\}$ für $A, B \subset G$
$AB = \{ab |\ a \in A, b \in B\}$

Beweis. Plan: $H \leq G, S \subseteq H, \langle S \rangle = H$

- $1_G = s_1 s_1^{-1} \in H$ für $s_1 \in S$
- $H \cdot H \subseteq H$, da $(s_1, \ldots, s_r)(s_1', \ldots s_2') = s_1, \ldots, s_r s_1', \ldots s_2' \in H$
- Sei $h \in H$ mit $h = s_1 \ldots s_r$. Dann $h^{-1} = (s_1, \ldots, s_r)^{-1}.\ \underbrace{S_r^{-1}}_{\in S \cup S^{-1}} \ \ldots\ \underbrace{S_1^{-1}}_{\in S \cup S^{-1}} \in H$.

Insgesamt $H \leq G$ und $S \subseteq H$.
Sei U jetzt eine Untergruppe mit $S \subset U$. Dann $H \subseteq U$ (da U ein Gruppe ist.)

$$\langle S \rangle = \bigcap_{\substack{U \leq G \\ S \subseteq U}} U = H \cap H = H \implies \langle S \rangle = H$$

□

Bemerkung

Sei $G = \langle g \rangle$ (zyklisch) mit $|G| < \inf$. Gilt $g^n = 1_G$ für ein $n \in \mathbb{Z}$, dann $|G| \mid n$.

Beweis. Sei $d \in \mathbb{N}$ mit $g^d = \{1_G, g^1, g^2, \ldots\}$. Division mit Rest liefert wieder $n = a \cdot d + 0$. Somit $d \mid n$ □

1.12 Satz Sei $(G, \circ)$ eine Gruppe und $U \leq G$

a) Wir definieren $\sim_u$ auf G

$$a \sim_u b \iff a^{-1} b \in U$$

b) Die Menge der Äquivalenzklassen G/U ist Linksnebenklassen

$$\{aU \mid a \in G\}$$

c) Ist T eine Vertretungssystem der Äquivalenzklassen, so gilt $G = \dot{\bigcup}_{t \in T} tU$

d) $|aU| = |u| \quad \forall a \in G$

Bemerkung

a) Mit '$\sim_u$' gegeben durch $a \sim'_u b \iff ab^{-1} \in U$ wird wieder eine Äquivalenzrelation auf G definiert mit Ut (Rechtsnebenklassen) als Äquivalenzklassen.

b) G/U ist die Menge der Linksnebenklassen und U
G ist die Menge der Rechtsnebenklassen

c) $|G/U|$ ist die Index von U in G

1.13 Satz von Lagrange Für eine endliche Gruppe G mit $U \leq G$ gitl $|G| = |U|\,|G/U|$, insbesondere $|U| \mid |G|$

Beweis. Sei $T = \{t_1, \ldots, t_r\}$eine Vertretersystem der Äquivalenzklasse, das heißt $G = UtU \rightsquigarrow |G| = \sum_{t \in T} |tU| = \sum_{t \in T} |U| = |T|\,|U|$ □

Beispiel

a) Ist $U \leq S_3$, dann $|U| \in \{1, 2, 3, 6\}$

b) Sei $g \in G$, dann $ord\,(g) = \langle g \rangle \mid |G|$ In S_10 gibt es keine Untergruppe der Ordunug 11

Index