Zwei Schreibweisen für Gruppen

(1) Multiplikative Schreibweise

Wird verwendet bei einem „punktartigen“ Verknüpfungssymbol, z.B. $\cdot$, $*$, $\odot$

Bezeichnung für das Neutralelement: $e, e_G, 1, 1_G$

Bezeichnung für das Inverse eines Elements a : a^{-1}

(2) Additive Schreibweise bei „plusartigem“

Verknüpfungssymbol, $+$, $\oplus$, $\boxplus$

Neutralelement $0, 0_G$ (nur üblich bei abelschen

Inverses von a : $-a$ Gruppen)

§ 2. Untergruppen und der Satz von Lagrange

Definition (2.1)

Ist $(G, *)$ eine Halbgruppe und $g \in G$ ein beliebiges Element, dann definiert man rekursiv $g^1 = g$ und $g^{n+1} = g^n * g$ für alle $n \in \mathbb{N}$.

- Ist $(G, *)$ ein **Monoid**, dann setzt man $g^0 = e_G$.
- Ist g darüber hinaus invertierbar, dann setzt man $g^{-n} = (g^n)^{-1}$ für alle $n \in \mathbb{N}$.

Bezeichnung für das Inverse eines Elements a : a^{-1}

Definition der Potenzen in additiver

Schreibweise Sei $(G, \oplus)$ eine Halbgruppe

• rekursive Def. $1 \cdot g = g$, $(n+1)g = n \cdot g \oplus g$

für $g \in G$, $n \in \mathbb{N}$

• falls G Monoid $0 \cdot g = 0_G$

• falls $g \in G$ invertierbar $(-n) \cdot g = -(n \cdot g)$

für $n \in \mathbb{N}$

In multiplikativer Schreibweise steht g^{-3} für $(g^3)^{-1}$ bzw. $(g \cdot g \cdot g)^{-1}$. In additiver Schreibweise steht $(-3) \cdot g$ für $-(3 \cdot g)$ bzw. $-(g \oplus g \oplus g)$.

Rechenregeln für Potenzen

Lemma (2.2)

Sei $(G, *)$ eine Halbgruppe.

- (i) Für alle $g \in G$ und $m, n \in \mathbb{N}$ gilt $g^m * g^n = g^{m+n}$ und $(g^m)^n = g^{mn}$.
- (ii) Sind $g, h \in G$ vertauschbare Elemente, gilt also $g * h = h * g$, dann folgt $(g * h)^n = g^n * h^n$ für $g, h \in G$ und $n \in \mathbb{N}$.
- (iii) Ist allgemeiner $\{g_1, \dots, g_r, h_1, \dots, h_r\}$ eine Menge in G bestehend aus paarweise vertauschbaren Elementen, dann gilt die Regel $(g_1 * \dots * g_r) * (h_1 * \dots * h_r) = (g_1 * h_1) * \dots * (g_r * h_r)$ und außerdem $(g_1 * \dots * g_r)^m = g_1^m * \dots * g_r^m$.

In einem Monoid gelten alle Regeln entsprechend für $m, n \in \mathbb{N}_0$, im Falle invertierbarer Elemente g, h für $m, n \in \mathbb{Z}$.

Liegt die Halbgruppe in additiver Schreibweise vor, dann muss auch die Notation der Rechenregeln entsprechend angepasst werden.

Definition der Untergruppen

Definition (2.3)

Sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $U \subseteq G$ wird **Untergruppe** von G genannt, wenn e_G in U liegt und für alle $a, b \in U$ auch die Elemente $a \cdot b$ und a^{-1} in U liegen.

Wie in §1 ausgeführt, erhält man somit durch Einschränkung eine Verknüpfung $\cdot_U$ auf U .

Proposition (2.4)

Das Paar $(U, \cdot_U)$ ist eine Gruppe.

wichtiges Beispiel für eine Untergruppe
von A_4 (bzw. S_4)

Klein'sche Vierergruppe

$$V_4 = \{ \text{id}, (12)(34), (13)(24), (14)(23) \}$$

$\circ$	$(12)(34)$	$(13)(24)$	$(14)(23)$
$(12)(34)$	id	$(14)(23)$	$(13)(24)$
$(13)(24)$	$(14)(23)$	id	$(12)(34)$
$(14)(23)$	$(13)(24)$	$(12)(34)$	id

$$(13)(24) \circ (14)(23) = (12)(34)$$

isotabelt
(G...)

Die Tabelle zeigt, dass für beliebig
 $\sigma, \tau \in V_4 \setminus \{\text{id}\}$ jeweils $\sigma \circ \tau \in V_4$ gilt

außerdem offensichtlich; $\sigma \circ \text{id} = \sigma \in V_4$

für alle $\sigma \in V_4$ insgesamt; $\sigma \circ \tau \in V_4$

für alle $\sigma, \tau \in V_4$

außerdem, $\text{id} \in V_4$ (Neutralement)

Die Tabelle zeigt auch $\sigma^{-1} = \sigma \in V_4 \forall \sigma \in V_4 \setminus \{\text{id}\}$,

für $\sigma = \text{id}$ offensichtlich.

insgesamt: V_4 ist Untergruppe

Die Symmetrie zeigt, dass V_4 eine
abelsche Gruppe ist.

Beweis von Proposition 2.4

geg: Gruppe $(G, \cdot)$, Untergruppe $U \subseteq G$

Nach Def. gilt $a \cdot u \cdot b = a \cdot b \quad \forall a, b \in U$

Beh: $(U, \cdot_U)$ ist eine Gruppe

(1) Assoziativität: Seien $a, b, c \in U$.

$$(a \cdot_U b) \cdot_U c = (a \cdot b) \cdot c \stackrel{\substack{\cdot \text{ assoziativ} \\ \text{auf } G}}{=} a \cdot (b \cdot c)$$

$$a \cdot (b \cdot c) = a \cdot_U (b \cdot_U c)$$

(2) Neutralement: Nach Def gilt $e_G \in U$.

$$\text{Sei } a \in U. \quad e_G \cdot_U a = e_G \cdot a = a$$

$\uparrow e_G$ Neutralement
in $(G, \cdot)$

$$a \cdot_U e_G = a \cdot e_G = a$$

$\rightarrow e_G$ ist Neutralelement in $(U, \circ_U)$, d.h.
 $\Leftrightarrow$ ist $e_U = e_G$

(3) Inverse: Sei $a \in U$. Nach Def. der Untergruppen gilt $a^{-1} \in U$, außerdem:

$$a \circ_U a^{-1} = a \circ a^{-1} = e_G = e_U$$

$$a^{-1} \circ_U a = a^{-1} \circ a = e_G = e_U$$

$\rightarrow a^{-1}$ ist Inverses von a in $(U, \circ_U)$. $\square$

Die
abel

Existenz und Eindeutigkeit der erzeugten Untergruppe

Proposition (2.5)

Sei $(G, \cdot)$ eine Gruppe, und sei $(U_i)_{i \in I}$ eine Familie von Untergruppen von G . Dann ist auch $U = \bigcap_{i \in I} U_i$ eine Untergruppe von G .

Satz (2.6)

Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Dann gibt es eine eindeutig bestimmte Untergruppe U von G mit den folgenden Eigenschaften.

(i) $U \supseteq S$

(ii) Ist V eine weitere Untergruppe von G mit $V \supseteq S$, dann folgt $V \supseteq U$.

Beide Bedingungen lassen sich zusammenfassen in der Aussage, dass U die **kleinste** Untergruppe von G ist, die S als Teilmenge enthält.

Beweis von Proposition 2.5

geg. Gruppe $(G, \cdot)$, Familie $(U_i)_{i \in I}$ von Untergruppen

Sei $U = \bigcap_{i \in I} U_i$. Beh. U ist Untergruppe von G

z.z. (1) $e_G \in U$ (2) $\forall a, b \in U, a \cdot b \in U, a^{-1} \in U$

zu (1) $\forall i \in I, U_i$ ist Untergrp. von $(G, \cdot)$

$\Rightarrow \forall i \in I, e_G \in U_i \Rightarrow e_G \in \bigcap_{i \in I} U_i \Rightarrow e_G \in U$

zu (2) Seien $a, b \in U$.

$a \in \bigcap_{i \in I} U_i \Rightarrow \forall i \in I, a \in U_i, b \in \bigcap_{i \in I} U_i \Rightarrow$

$\forall i \in I, b \in U_i$

z.zg. $ab \in \bigcap_{i \in I} U_i$ und $a^{-1} \in \bigcap_{i \in I} U_i$

gleichbedeutend: $\forall i \in I, ab \in U_i$ und $\forall i \in I, a^{-1} \in U_i$

Sei $i \in I, a, b \in U_i, U_i$ Untergr. $\rightarrow ab \in U_i$
und $a^{-1} \in U_i$

Beweis von Satz 2.6

geg: Gruppe $(G, \cdot)$, Teilmenge $S \subseteq G$

z.zg: Es gibt eine eindeutig bestimmte Untergruppe U von G mit

- (1) $U \supseteq S$ (2) V Untergr. von G , $V \supseteq S$
 $\Rightarrow V \supseteq U$

Eindeutigkeit:

Ang. U, V sind Untergruppen von G , beide erfüllen (1) und (2).

Beh: $U = V$

$U \geq S$, wende (2) auf die Untergr. V an
(zulässig, da $V \geq S$) $\Rightarrow V \geq U$

$V \geq S$, wende (2) auf die Untergr. U an
(zulässig, da $U \geq S$) $\Rightarrow U \geq V$

$V \geq U, U \geq V \Rightarrow U = V$

Existenz Sei $(U_i)_{i \in I}$ die Familie

aller Untergruppen von $(G, \cdot)$ mit $U_i \geq S$.

Sei $U = \bigcap_{i \in I} U_i$. Prop. 2.5 $\Rightarrow U$ ist Unter-
gruppe von $(G, \cdot)$. noch z.z. U erfüllt die
Bedingungen (1) und (2).

am
zu (1) z.zg. $S \subseteq U$ Sei $s \in S$

$\forall i \in I: S \subseteq U_i \Rightarrow \forall i \in I: s \in U_i$

$\Rightarrow s \in \bigcap_{i \in I} U_i \Rightarrow s \in U$

U am
zu (2) Sei V eine bel. Untergruppe von $(G, \cdot)$

mit $V \supseteq S$ z.zg. $V \supseteq U$ Nach Def.

der Familie $(U_i)_{i \in I}$ existiert ein $i_0 \in I$ mit

$V = U_{i_0}$. Da offenbar $\bigcap_{i \in I} U_i \subseteq U_{i_0}$

gilt, folgt $U \subseteq V$.

□

z.S.
Unter-
fall die

Definition der erzeugten Untergruppe $\langle S \rangle$

Definition (2.7)

Die Untergruppe U aus Satz (2.6) wird die von S **erzeugte** Untergruppe genannt und mit $\langle S \rangle$ bezeichnet. Ist V eine beliebige Untergruppe von G , dann wird jede Teilmenge T von G mit $V = \langle T \rangle$ ein **Erzeugendensystem** von V genannt.