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 $n \in \mathbb{N}$.

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 $\{g_1, ..., g_r, h_1, ..., h_r\}$ eine Menge in G bestehend aus paarweise vertauschbaren Elementen, dann gilt die Regel
$(g_1 * ... * g_r) * (h_1 * ... * h_r) = (g_1 * h_1) * ... * (g_r * h_r)$ und außerdem $(g_1 * ... * g_r)^m = g_1^m * ... * g_r^m$.

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.

Potenzen in additiver Schreibweise

Sei $(G, +)$ eine abelsche Gruppe. Sei $g \in G$

rekursive Definition der n-ten Potenz

$1 \cdot g = g$, $(n+1) \cdot g = n \cdot g + g$

außerdem: $0 \cdot g = 0_G$, $(-m) \cdot g = -m \cdot g$

Übertragung der übrigen Rechenregeln:

$(m+n) \cdot g = m \cdot g + n \cdot g$, $n \cdot (m \cdot g) = (nm) \cdot g$,

$m \cdot (g+h) = m \cdot g + m \cdot h$, ...

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.

Beweis von Prop. (2.4)

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

Sei $\cdot_U$ die Verknüpfung (auf U), die durch Einschränkung von $\cdot$ auf $U \times U \subseteq G \times G$ entsteht, d.h. es gilt

$$a \cdot_U b = a \cdot b \quad \text{für alle } a, b \in U.$$

Überprüfe nun, dass $(U, \cdot_U)$ eine Gruppe ist

(1) $U \neq \emptyset$ (wegen $e_G \in U$), $\cdot_U$ ist Verknüpfung auf U

(2) Assoziativität: Seien $a, b, c \in U$. ← $\cdot$ assoziative Verknüpfung auf G

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

$$a \cdot (b \cdot c) = a \cdot_U (\underbrace{b \cdot c}_{\in U}) = a \cdot_U (b \cdot_U c)$$

(3) Neutralelement: Sei $a \in U$ Dann gilt $e_G \circ_U a = e_G \circ a = a$ und $a \circ_U e_G = a \circ e_G = a \Rightarrow e_G$ ist Neutralelement in $(U, \circ_U)$, d.h. es ist $e_U = e_G$.

(4) Inverse: Sei $a \in U$. Auf Grund der Untergruppeneig. ist auch a^{-1} in U enthalten. Es gilt $a \circ_U a^{-1} = a \circ a^{-1} = e_G$
$= e_U$, $a^{-1} \circ_U a = a^{-1} \circ a = e_G = e_U$ $\Rightarrow$
a^{-1} ist das Inverse von a in $(U, \circ_U)$
insgesamt: $(U, \circ_U)$ ist eine Gruppe $\square$

Bem: In der alternierenden Gruppe A_4 ist durch $V_4 = \{id, \underbrace{(12)(34), (13)(24), (14)(23)}_{\text{(Doppeltranspositionen)}}\}$ eine Untergruppe gegeben, die Kleinsche Vierergruppe.

Es gilt $V_4 \leq A_4$, denn: $id \in A_4$ wg. $sgn(id) = +1$

ebenso: $sgn((12)(34)) = sgn((12))\,sgn((34))$

$= (-1)(-1) = +1 \Rightarrow (12)(34) \in A_4$,

$(13)(24), (14)(23) \in A_4$ analog.

- Das Neutralelement id von $(A_4, \circ)$ ist in V_4 enthalten.
- noch z.zg: $\forall \sigma, \tau \in V_4 : \sigma \circ \tau, \sigma^{-1} \in V_4$

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

$(12)(34) \circ (12)(34) = (1)(2)(3)(4) = id$

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

Da die Tabelle nur Elemente aus V_4 enthält, ist die Teilmenge $V_4 \subseteq A_4$ bzgl. $\circ$ abgeschlossen.

Die Diagonale zeigt: $\sigma^2 = id$ und somit $\sigma^{-1} = \sigma \in V_4 \quad \forall \sigma \in V_4$.

□

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 Satz 2.6:

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

z.zg.: Es gibt eine Untergruppe U von G mit den Eigenschaften (i) $U \supseteq S$

(ii) Ist V Untergr. von G und $V \supseteq S$, dann folgt $V \supseteq U$.

außerdem: Eindeutigkeit

Sei $\mathcal{U} = (U_i)_{i \in I}$ die Familie alle Untergruppen von G mit $U_i \supseteq S$. (d.h. Ist V eine Untergr. von G mit $V \supseteq S$, dann gilt $V = U_i$ für ein $i \in I$.)

Sei $U = \bigcap_{i \in I} U_i$. Überprüfe, dass U (i), (ii) erfüllt

vorweg: Nach Kap 2.5 ist U eine Untergr. von G.

zu (i) Überprüfe $S \subseteq \bigcap_{i \in I} U_i$. Sei $g \in S$. Dann folgt $g \in U_i$ für jedes $i \in I$, da $S \subseteq U_i$ nach Def von U_i.

$\forall i \in I : g \in U_i \Rightarrow g \in \bigcap_{i \in I} U_i$.

zu (ii) Sei V eine bel. Untergr. von G mit $V \supseteq S$. z.zg.:

$V \supseteq U$ s.o. $\rightarrow \exists i_0 \in I$ mit $V = U_{i_0}$

Offenbar gilt $U_{i_0} \supseteq \bigcap_{i \in I} U_i \rightarrow V \supseteq S$

zur Eindeutigkeit. Ang. U' ist eine Untergr., die (i) und (ii) ebenfalls erfüllt. z.zg.: $U = U'$

U erfüllt (i), (ii) kann auf $V = U'$ angewendet werden $\Rightarrow U' \supseteq U$

U' erfüllt (i), (ii) kann auf $V = U$ angew. werden $\Rightarrow U \supseteq U'$

insgesamt: $U = U'$ □

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.

Zyklische und endlich erzeugte Gruppen

Definition (2.8)

Eine Gruppe G wird zyklisch genannt, wenn ein $g \in G$ mit $G = \langle g \rangle$ existiert. Existiert eine endliche Teilmenge $S \subseteq G$ mit $G = \langle S \rangle$, dann nennt man G eine endlich erzeugte Gruppe.

Bem.: Ist G eine Gruppe und $g \in G$, dann gilt $\langle g \rangle = \{ g^a \mid a \in \mathbb{Z} \}$.

Sei $U = \{ g^a \mid a \in \mathbb{Z} \}$. Überprüfe, dass U die definierenden Bedingungen von $\langle g \rangle$ erfüllt, im Einzelnen

(0) U ist Untergruppe von G

(1) $g \in U$ (äquivalent: $\{g\} \subseteq U$)

(2) Ist V eine bel. Untergruppe von G mit $g \in V$, dann folgt $U \subseteq V$.

zu (0) $e_G = g^0 \ (\mathrm{mod}\ 0 \in \mathbb{Z}) \Rightarrow e_G \in U$

Seien nun $u, v \in U$. überprüfe: $uv, u^{-1} \in U$

$u, v \in U \rightarrow \exists a, b \in \mathbb{Z} : u = g^a, v = g^b$

$\Rightarrow u \cdot v = g^a \cdot g^b = g^{a+b}, \mathrm{mod}\ a+b \in \mathbb{Z}$

$\Rightarrow u \cdot v \in U$

$u = g^a \Rightarrow u^{-1} = (g^a)^{-1} = g^{-a}, \mathrm{mod}\ -a \in \mathbb{Z}$

$\Rightarrow u^{-1} \in U$

zu (1) klar, da $g = g^1 \ (\mathrm{mod}\ 1 \in \mathbb{Z})$

zu (2) Sei V eine Untergr. von G mit $g \in V$.

z.zg: $U \leq V$ gleichbedeutend: $g^a \in V \ \forall a \in \mathbb{Z}$

überprüfe $g^m \in V \ \forall m \in \mathbb{N}_0$ durch vollst. Ind.

Ind.-Anf.: $g^0 = e_G \in V$ (da V Untergr. von G)

Ind.-Schritt $m \mapsto m+1$: Ind.-V. $\Rightarrow g^m \in V$

$g^m \in V$, $g \in V \Rightarrow g^{m+1} = g^m \cdot g \in V$
(V Untergr.)

Zeige nun noch $g^{-m} \in V \ \forall m \in \mathbb{N}$. Sei $m \in \mathbb{N}$.

Bereits gezeigt: $g^m \in V \overset{V \text{ Untergr.}}{\Longrightarrow} (g^m)^{-1} \in V$

$\rightarrow g^{-m} \in V$.

also insgesamt: $g^a \in V \ \forall a \in \mathbb{Z}$. $\square$

Die Elemente von endlich erzeugten Untergruppen

Satz (2.9)

Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge.

(i) Die Elemente von $\langle S \rangle$ sind gegeben durch

$$\langle S \rangle = \{g_1^{\varepsilon_1} \cdot \ldots \cdot g_r^{\varepsilon_r} \mid r \in \mathbb{N}_0, g_1, \ldots, g_r \in S, \varepsilon_k \in \{\pm 1\} \text{ für } 1 \leq k \leq r\}.$$

(ii) Sei S endlich, $S = \{g_1, \ldots, g_m\}$ für ein $m \in \mathbb{N}_0$, und setzen wir voraus, dass jedes Element der Menge S mit jedem anderen vertauschbar ist. Dann gilt

$$\langle S \rangle = \{g_1^{e_1} \cdot \ldots \cdot g_m^{e_m} \mid e_k \in \mathbb{Z} \text{ für } 1 \leq k \leq m\}.$$