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 $n \in \mathbb{N}$.

Multiplikative versus additive Schreibweise

(1) Multiplikative Schreibweise beim Verkn.-symbol

$\cdot$, $*$ oder $\odot$

mögliche Schreibweisen für das Neutralelement:

e_G , e ; 1_G , 1

Schreibweise für das Inverse von $g \in G$: g^{-1}

(2) Additive Schreibw. bei Verkn.-symbol $+$, $\oplus$

mögl. Schreibw. für das Neutralelement: 0_G, 0

Schreibweise für das Inverse von $g \in G$: $-g$

letztes Mal: Rechenregel für das Inverse

$(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$ in additives Schreibw.: $-(g+h) = (-h) + (-g)$

additive Schreibweise für Potenzen:

schreibe $n \cdot g$ statt g^n

d.h. z.B. $3g$ ist eine Kurzschreibw. für $g + g + g$

und $(-3)g$ eine Kurzschreibw. für $-(g+g+g)$

Übersetzung der Rechenregeln in Lemma (2.2) (i) in additive Schreibweise:

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

$n \cdot (m \cdot g) = (mn)\, g$

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 $\{g_1, ..., g_r, h_1, ..., h_r\}$ 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.

Beweis von Lemma (2.2), nur erste Regel unter (1)

Sei $(G, *)$ eine Halbgruppe und $g \in G$

Sei $m \in \mathbb{N}$. Beh: $\forall n \in \mathbb{N}: g^{m+n} = g^m * g^n$

Bew. durch vollst. Ind über n

Ind.-Anf. $n = 1$: $g^{m+1} = g^m * g$ ist nach Def. von g^{m+1} erfüllt

Ind.-schritt: Sei $n \in \mathbb{N}$, setze $g^{m+n} = g^m * g^n$ voraus

$$\Rightarrow g^{m+(n+1)} = g^{(m+n)+1} = g^{m+n} * g \overset{\text{I.V.}}{=} (g^m * g^n) * g$$

$$= g^m * (g^n * g) = g^m * g^{n+1}$$

Sei nun $(G, *)$ ein Monoid, e_G das Neutralelement.
Sei $g \in G$, und seien $m, n \in \mathbb{N}_0$. z.zg. $g^{m+n} = g^m * g^n$

1. Fall: $m, n \in \mathbb{N}$ bereits erledigt, s.o.

2. Fall: $m = 0$ $\quad g^{m+n} = g^{0+n} = g^n = e_G * g^n = g^0 * g^n = g^m * g^n$

3. Fall: $n = 0$ $\quad g^{m+n} = g^{m+0} = g^m = g^m * e_G = g^m * g^0 = g^m * g^n$

Sei nun g ein invertierbares Element, und seien $m, n \in \mathbb{Z}$.
z.zg: $g^{m+n} \overset{(*)}{=} g^m * g^n$. 1. Fall: $m, n \geq 0$ bereits erledigt
2. Fall: $m \geq 0$, $n < 0 \Rightarrow \exists r \in \mathbb{N}$ mit $n = -r$ Dann ist
$(*)$ äquivalent zu $g^{m+(-r)} = g^m * g^{-r}$ $(*_2)$
Fall 2.1: $m + (-r) \geq 0$ s.o. $\Rightarrow g^{m+(-r)} * g^r = g^{(m+(-r))+r} = g^m$

multipliziere g^{-r} von rechts $\Rightarrow$ $g^m * g^{-r} =$

$(g^{m+(-r)} * g^r) \cdot g^{-r} = g^{m+(-r)} * (g^r * (g^r)^{-1}) =$

$g^{m+(-r)} * e_G = g^{m+(-r)}$ $(\checkmark)$

Fall 2.2 $m+r<0$ Bilde auf beiden Seiten von $(*_2)$ das Inverse, erhalte dadurch die äquivalente Gleichung $g^{r+(-m)} = g^{-m} * g^r$ Gehe nun vor wie unter Fall 2.1

Behandlung der restlichen Fälle: siehe Skript bzw. Übungen

□

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:

Überprüfe für $(U, \circ_U)$ die Gruppenaxiome.

klar: U Menge, $\circ_U$ ist Verknüpfung auf U

Assoziativität: Seien $a, b, c \in U$

$$(a \circ_U b) \circ_U c = (a \circ b) \circ c = a \circ (b \circ c) = a \circ_U (b \circ_U c)$$

↑ Def. von $\circ_U$ ↑ $(G, \circ)$ ist Gpp

Neutralelement: ist geg. durch e_G, denn für alle $a \in U$ gilt $a \circ_U e_G = a \circ e_G = a$, ebenso $e_G \circ_U a = a$

Inverse: Sei $a \in U$. Voraussetzungen $\Rightarrow a^{-1} \in U$

Es gilt $a \circ_U a^{-1} = a \circ a^{-1} = e_G = e_U$, ebenso $a^{-1} \circ_U a = e_U$

Also ist a^{-1} nicht nur in $(G, \circ)$, sondern auch in $(U, \circ_U)$ das Inverse von a. □

Beispiele für Untergr.: (Notation: $U \leq G$ bedeutet: U Untergr. von G)

(1) Für jede Gruppe $(G, \circ)$ sind $\{e_G\}$ und G Untergruppen von G, die sog. **trivialen Untergruppen**.

(2) $\mathbb{Z} \leq (\mathbb{Q}, +)$, $\mathbb{Q} \leq (\mathbb{R}, +)$, $\mathbb{R} \leq (\mathbb{C}, +)$

(3) $A_n \leq (S_n, \circ)$ für alle $n \in \mathbb{N}$

Im Fall $n = 4$ hat A_n eine Untergr. aus vier Elementen, die sog. **Kleinsche Vierergruppe** $V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$

(4) $SL_n(K) \leq GL_n(K)$ für jedes $n \in \mathbb{N}$ und jeden Körper K

$O(n) \leq GL_n(\mathbb{R})$, $U(n) \leq GL_n(\mathbb{C})$ für jedes $n \in \mathbb{N}$

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 Prop. 2.5

geg.: Familie $(U_i)_{i \in I}$ von Untergp., $U = \bigcap_{i \in I} U_i$

zu überprüfen: (1) $e_G \in U$

(2) $\forall u, v \in U : uv \in U, u^{-1} \in U$

zu (1) Jedes U_i ist Untergp. von G $\Rightarrow$ $\forall i \in I : e_G \in U_i$

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

zu (2) Seien $u, v \in U \Rightarrow u, v \in \bigcap_{i \in I} U_i \Rightarrow$

$\forall i \in I : u, v \in U_i \xrightarrow[\text{ist Untergp.}]{\text{Jedes } U_i} \forall i \in I : uv \in U_i, u^{-1} \in U_i$

$\Rightarrow uv, u^{-1} \in \bigcap_{i \in I} U_i \Rightarrow uv, u^{-1} \in U$ □

Beweis von Satz 2.6:

Existenz: Betrachte die Gesamtheit aller Untergr. U_i von G mit $U_i \supseteq S$. fasse diese zu einer Familie $(U_i)_{i \in I}$ zusammen. Definiere nun $U = \bigcap_{i \in I} U_i$. Kap. (2.5) $\Rightarrow U \leq G$

Zeige nun, dass (i) und (ii) durch U erfüllt werden.

zu (i) z.zg.: $S \subseteq U$ Sei $s \in S$. $S \subseteq U_i \ \forall i \in I \Rightarrow$

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

zu (ii) Sei $V \leq G$ mit $V \supseteq S$. z.zg.: $U \subseteq V$

Nach Def der Familie gilt $V = U_{i_0}$ für ein $i_0 \in I$.

Sei nun $u \in U$. $\Rightarrow u \in \bigcap_{i \in I} U_i \Rightarrow \forall i \in I : u \in U_i$

$\Rightarrow u \in U_{i_0} \Rightarrow u \in V$. Also ist $U \subseteq V$ erfüllt.

Eindeutigkeit: Ang., U, V seien Untergruppen von G, die beide (i) und (ii) erfüllen.

U erfüllt (ii), $V \leq G$ mit $V \supseteq S \Rightarrow U \leq V$

V erfüllt (ii), $U \leq G$ mit $U \supseteq S \Rightarrow V \leq U$

Insgesamt gilt also $U = V$. □

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 $\langle g \rangle = \{ g^e \mid e \in \mathbb{Z} \}$. (in additiver Schreibweise: $\langle g \rangle = \{ e \cdot g \mid e \in \mathbb{Z} \}$)

Nachweis (für die multiplikative Schreibw.):

Sei $U = \{ g^e \mid e \in \mathbb{Z} \}$. zu überprüfen:

(1) $U \leq G$ ✓ (2) $U \supseteq \{g\}$ (3) $V \leq G$, $V \supseteq \{g\} \Rightarrow V \supseteq U$

zu (1) $e_G = g^0$, $0 \in \mathbb{Z} \Rightarrow e_G \in U$

Seien $h, h' \in U$. $\Rightarrow \exists e, e' \in \mathbb{Z} : h = g^e$, $h' = g^{e'}$

$\Rightarrow h \cdot h' = g^e \cdot g^{e'} = g^{e+e'}$, $e+e' \in \mathbb{Z} \Rightarrow h \cdot h' \in U$

$h^{-1} = (g^e)^{-1} = g^{-e}$, $-e \in \mathbb{Z} \Rightarrow h^{-1} \in U$

zu (2) klar, da $g = g^1$, $1 \in \mathbb{Z}$

□

zu (3) $V \leq G$, $\langle g \rangle \subseteq V$, z.zg. $U \subseteq V$

Sei $h \in U \Rightarrow \exists e \in \mathbb{Z}: h = g^e$

$> 0 \Rightarrow g \in V$ Da V Untergr. von G ist, liegt auch jede Potenz von g in V, insb. $h = g^e \in V$. □