Definition (5.1)

Eine Verknüpfung auf einer Menge A ist eine Abbildung $A \times A \to A$.

- Beispiele für Verknüpfungen auf $\mathbb{R}$ sind die Addition, die Subtraktion oder die Multiplikation.
- Man unterscheidet bei Verknüpfungen zwischen multiplikativer und additiver Schreibweise. Additive („plusartige“) Verknüpfungssymbole sind $+$, $\oplus$ oder $\boxplus$. Multiplikative Verknüpfungssymbole sind $\cdot$, $\odot$ oder $*$.

Eigenschaften von Verknüpfungen

Definition (5.2)

Eine Verknüpfung $\cdot$ auf einer Menge A bezeichnet man als

(i) kommutativ, wenn $ab = ba$ für alle $a, b \in A$

(ii) assoziativ, wenn $a(bc) = (ab)c$ für alle $a, b, c \in A$ erfüllt ist.

Man bezeichnet eine Teilmenge $B \subseteq A$ als abgeschlossen unter der Verknüpfung $\cdot$, wenn für alle $b, b' \in B$ jeweils $bb' \in B$ gilt. Man erhält in diesem Fall eine Verknüpfung $\cdot_B$ auf B, indem man $b \cdot_B b' = bb'$ für alle $b, b' \in B$ setzt.

Definition (5.3)

(i) Eine Halbgruppe ist ein Paar $(G, \cdot)$ bestehend aus einer nichtleeren Menge G und einer assoziativen Verknüpfung $\cdot$ auf der Menge G.

(ii) Ein Element $e \in G$ in einer Halbgruppe wird Neutralelement genannt, wenn $g \cdot e = e \cdot g = g$ für alle $g \in G$ erfüllt ist.

(iii) Eine Halbgruppe $(G, \cdot)$, in der ein Neutralelement existiert, wird Monoid genannt.

Beispiele für Monoide

invertierbare Elemente:

(i) $(\mathbb{N}, \cdot)$ (Neutralelement: 1) — nur 1

(ii) $(\mathbb{N}_0, +)$ (Neutralelement: 0) — nur 0

(iii) $(\mathbb{Z}, +)$ (Neutralelement: 0) — alle

(iv) X Menge, $M = \mathrm{Abb}(X)$ = Menge der Abbildungen $X \to X$ — invertierbar: die bijektiven Abb.

Dort ist $\circ : M \times M \to M$, $(f, g) \mapsto f \circ g$ eine Verknüpfung bereits bekannt:

Für alle $f, g, h \in M$ gilt $f \circ (g \circ h) = (f \circ g) \circ h$
somit ist die Verknüpfung assoziativ
Die identische Abbildung $id_X : X \to X, x \mapsto x$
ist in der Halbgruppe $(M, \circ)$ ein Neutralelement.
überprüfe: Für jedes $f \in M$ gilt $f \circ id_X = f$
und $id_X \circ f = f$. Grund: Für alle $x \in X$ gilt
$(f \circ id_X)(x) = f(id_X(x)) = f(x)$ und
$(id_X \circ f)(x) = id_X(f(x)) = f(x)$

Bem.: Ist X eine Menge mit $|X| \geq 3$, dann ist das Monoid $(\mathrm{Abb}(X), \circ)$ nicht kommutativ.

$|X| \geq 3 \to \exists$ drei verschiedene Elemente $a, b, c \in X$. Betrachte die Abbildungen τ_{ab} und τ_{ac}.

(Erinnerung: $\tau_{ab}(x) = \begin{cases} b & \text{falls } x = a \\ a & \text{falls } x = b \\ x & \text{sonst} \end{cases}$)

$(\tau_{ab} \circ \tau_{ac})(a) = \tau_{ab}(\tau_{ac}(a)) =$

$\tau_{ab}(c) = c$

$(\tau_{ac} \circ \tau_{ab})(a) = \tau_{ac}(\tau_{ab}(a)) =$

$\tau_{ac}(b) = b \implies \tau_{ab} \circ \tau_{ac} \neq \tau_{ac} \circ \tau_{ab}$

$=$

zu (

und

$b =$

$=$

Genau

werde

zu (iv)

zu (v)

Bel. (1)

Definition (5.4)

(i) Ein Element g in einem Monoid $(G, \cdot)$ mit Neutralelement e heißt invertierbar, wenn ein $h \in G$ existierst, so dass die Gleichungen $g \cdot h = h \cdot g = e$ erfüllt sind.

(ii) Eine Gruppe ist ein Monoid, in dem jedes Element invertierbar ist.

(iii) Eine Halbgruppe, und ebenso ein Monoid und eine Gruppe, wird kommutativ oder abelsch genannt, wenn die zugehörige Verknüpfung kommutativ ist.

Rechenregeln in Monoiden

Lemma (5.5)

Sei $(G, \cdot)$ ein Monoid, und sei e ein Neutralelement des Monoids.

(i) Das Monoid besitzt keine weiteren Neutralelemente. Man bezeichnet e deshalb als *das* Neutralelement des Monoids, und bezeichnet es mit e_G.

(ii) Zu jedem invertierbaren Element $a \in G$ gibt es genau ein Element $b \in G$ mit $ab = ba = e_G$. Man nennt b das zu a inverse Element, und bezeichnet es mit a^{-1}.

(iii) Ist a invertierbar und $b \in G$ ein Element mit $ab = e_G$, dann folgt daraus bereits $b = a^{-1}$. Ebenso folgt bereits aus der Gleichung $ba = e_G$, dass b das Inverse von a ist.

(iv) Das Neutralelement ist invertierbar, und es gilt $e_G^{-1} = e_G$.

(v) Sind a und b invertierbare Elemente des Monoids, dann sind auch ab und a^{-1} invertierbar, und es gilt $(ab)^{-1} = b^{-1}a^{-1}$ und $(a^{-1})^{-1} = a$.

Beweis von Lemma 5.5

geg.: Monoid $(G, \cdot)$

zu (i) Eindeutigkeit des Neutralelements

Ang.: e und e' sind beides Neutralelemente.

$$e \underset{\text{da } e' \text{ Neutralelement}}{=} e \cdot e' \overset{\text{da } e \text{ Neutralelement}}{=} e'$$

zu (ii) Sei $a \in G$. Ang.: b und c sind Elemente mit $a \cdot b = e$, $\boxed{b \cdot a = e}$ und $\boxed{a \cdot c = e}$, $c \cdot a = e$

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

$= e \cdot c = c$

<u>zu (iii)</u> Sei a ein invertierbares Element und $b \in G$ mit $a \cdot b = e$. <u>Beh.:</u> $b = a^{-1}$

$$b = e \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b)$$
$$= a^{-1} \cdot e = a^{-1}$$

Genauso kann $b = a^{-1}$ aus $b \cdot a = e$ gefolgert werden.

<u>zu (iv)</u> Aus $e \cdot e = e$ folgt nach Def., dass e das Inverse von e ist.

<u>zu (v)</u> Seien a und b invertierbare Elt.

<u>Beh.:</u> (1) ab ist invertierbar, und $(ab)^{-1} = b^{-1} a^{-1}$

(2) a^{-1} ist invertierbar, und $(a^{-1})^{-1} = a$.

<u>zu (1)</u> Sei $c = b^{-1}a^{-1}$. Dann gilt: $(ab)\cdot c =$
$(ab)\cdot(b^{-1}a^{-1}) = a\cdot\left(b\cdot(b^{-1}a^{-1})\right) = a\left((bb^{-1})a^{-1}\right)$
$= a\cdot(e\cdot a^{-1}) = aa^{-1} = e$ und $c\cdot(ab) =$
$b^{-1}a^{-1}ab = b^{-1}e\cdot b = b^{-1}b = e$

Aus $(ab)c = e$ und $c\cdot(ab) = e$ folgt, dass ab invertierbar und $c = b^{-1}a^{-1}$ das Inverse von ab ist.

<u>zu(2)</u> Sei $d = a$. $a^{-1}\cdot d = a^{-1}\cdot a = e$

und $d \cdot a^{-1} = a \cdot a^{-1} = e$. Die Gleichungen zeigen, dass $d = a$ das Inverse von a^{-1} ist, d.h. $(a^{-1})^{-1} = d = a$.

Hinweis zur Klammerung

Beim Beweis von Lemma 5.5 (v) wird deutlich, wie mühsam es werden kann, jede einzelne Anwendung des Assoziativgesetzes explizit anzugeben. Für eine vollständige und korrekte Darstellung des Beweises ist das notwendig, da wir streng genommen die Bedeutung eines Ausdrucks wie $a \cdot b \cdot b^{-1} \cdot a^{-1}$ nicht definiert haben, sondern nur Ausdrücke wie $(a \cdot b) \cdot (b^{-1} \cdot a^{-1})$ oder $a \cdot (b \cdot (b^{-1}) \cdot a^{-1}))$ definiert sind.

Auf Grund des Assoziativgesetzes ist aber die Bedeutung eines Produkts unabhängig von der Beklammerung, und deshalb wird aus Bequemlichkeit oft darauf verzichtet. Der zweite Teil des Beweises von Lemma 5.5 (v) zeigt ja, um wieviel kürzer die Rechnung ausfällt, wenn man vom genauen Nachhalten der Beklammerung absieht.

Bem.: Die Rechenregeln für das Inverse

($(ab)^{-1} = b^{-1}a^{-1}$ und $(a^{-1})^{-1} = a$) lauten

in additiver Schreibweise

$$-(a+b) = (-b)+(-a), \quad -(-a) = a$$

Die Gruppe der invertierbaren Elemente

Folgerung (5.6)

Sei $(G, \cdot)$ ein Monoid, und sei $G^\times \subseteq G$ die Teilmenge der invertierbaren Elemente. Dann ist $G^\times$ bezüglich $\cdot$ abgeschlossen, und $(G^\times, \cdot_{G^\times})$ ist eine Gruppe.

Definition der Ringe

Definition (5.7)

Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+$ und $\cdot$ auf R mit folgenden Eigenschaften.

(i) Das Paar $(R, +)$ ist eine abelsche Gruppe.

(ii) Das Paar $(R, \cdot)$ ist ein abelsches Monoid.

(iii) Es gilt das Distributivgesetz $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

Ergänzungen zur Ringdefinition

Sei $(R, +, \cdot)$ ein Ring.

- Das Neutralelement der Gruppe $(R, +)$ wird das Nullelement des Rings genannt und mit 0_R bezeichnet.
- Das Neutralelement des Monoids $(R, \cdot)$ nennt man das Einselement des Rings und bezeichnet es mit 1_R.
- Wenn die Menge $R^\times$ der invertierbaren Elemente des Monoids $(R, \cdot)$ mit $R \setminus \{0_R\}$ übereinstimmt, dann bezeichnet man den Ring auch als Körper.

Ergänzung zur Notation:

Ist R ein Ring, dann schreibt man für $a, b \in R$ statt $a+(-b)$ auch einfach $a-b$.

Ist K Körper und $a \in K$, $b \in K \setminus \{0\}$, dann schreibt man statt $a b^{-1}$ auch $\frac{a}{b}$.

Rechenregeln in Ringen

Proposition (5.8)

Sei $(R, +, \cdot)$ ein Ring, und seien $a, b \in R$. Dann gilt

(i) $-0_R = 0_R$, $-(-a) = a$ und $-(a+b) = (-a)+(-b)$,

(ii) $0_R \cdot a = 0_R$, $a(-b) = (-a)b = -(ab)$ und $ab = (-a)(-b)$,

(iii) $1_R^{-1} = 1_R$, $(a^{-1})^{-1} = a$ und $(ab)^{-1} = a^{-1}b^{-1}$, sofern a und b in $(R, \cdot)$ invertierbar sind.

(iv) Ist R sogar ein Körper, dann folgt aus $ab = 0_R$ immer $a = 0_R$ oder $b = 0_R$.

Beweis von Prop. 5.8

zu (ii) Seien $a, b \in R$

(1) Bew. von $0_R \cdot a = 0_R$

$$0_R \cdot a = (0_R + 0_R) \cdot a = 0_R a + 0_R \cdot a$$

$$\Rightarrow 0_R \cdot a + (-0_R \cdot a) = 0_R a + 0_R a + (-0_R \cdot a)$$

$$\Rightarrow 0_R = 0_R \cdot a + 0_R$$

$$\Rightarrow 0_R = 0_R \cdot a$$

R a

$-0_R \cdot a)$

<u>zu (iv)</u> Vor.: R ist Körper, geg. $a, b \in R$ mit $a \cdot b = 0_R$. z.zg.: $a = 0_R$ oder $b = 0_R$

Ang., es gilt $a \cdot b = 0_R$, aber $a \neq 0_R$ und $b \neq 0_R$.

Dann ist a und b in $(R, \cdot)$ invertierbar.

$\Rightarrow b^{-1} \cdot a^{-1} \cdot a \cdot b = b^{-1} a^{-1} \cdot 0_R = 0_R$

$\Rightarrow b^{-1} \cdot 1_R \cdot b = 0_R \Rightarrow 1_R = 0_R$

1_R Neutralelement in $(R, \cdot) \Rightarrow 1_R$ invertierbar

$\Rightarrow 0_R$ invertierbar $\lightning$ denn da R Körper ist, ist $R \setminus \{0_R\}$ die Menge der invertierbaren Elemente. 0_R also <u>nicht</u> invertierbar.