Halbgruppen und Monoide

Definition (1.1)

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

(ii) Ein Element $e \in G$ der Halbgruppe wird als Neutralelement bezeichnet, wenn $e * a = a$ und $a * e = a$ für alle $a \in G$ erfüllt ist.

(iii) Eine Halbgruppe mit mindestens einem Neutralelement bezeichnet man als Monoid.

Definition der Gruppen

Definition (1.2)

Sei $(G, *)$ ein Monoid mit dem Neutralelement e_G.

(i) Ein Element $g \in G$ wird invertierbar in $(G, *)$ genannt, wenn ein $h \in G$ mit $g * h = h * g = e_G$ existiert. Man nennt h in diesem Fall ein Inverses von g.

(ii) Ein Monoid $(G, *)$, in dem jedes Element ein Inverses besitzt, wird Gruppe genannt.

(iii) Eine Gruppe G, und ebenso eine Halbgruppe bzw. ein Monoid, wird als kommutativ oder abelsch bezeichnet, wenn die Verknüpfung $*$ kommutativ ist.

Definition der Ringe

Definition (1.6)

Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$, genannt Addition und Multiplikation, so dass die folgenden Bedingungen erfüllt sind:

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

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

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

- Ist $(R, +)$ eine abelsche Gruppe und $(R, \cdot)$ eine nicht-abelsche Halbgruppe, die die beiden Distributivgesetze $a(b + c) = ab + ac$ und $(a + b)c = ac + bc$ für alle $a, b, c \in R$ erfüllt, dann spricht man von einem Schiefring.
- Ist $(R, \cdot)$ ein nicht-kommutatives Monoid, dann spricht man von einem Schiefring mit 1.

Bem: Die Rechenregeln für Gruppenelemente (z.B. $(g \cdot h)^{-1} = h^{-1} g^{-1}$, $(g^{-1})^{-1} = g$ übertragen sich auf die additive Gruppe $(R, +)$ eines Rings, d.h. z.B. $-(a+b) = (-b)+(-a) = (-a)+(-b)$

$-(-a) = a \quad \forall a, b \in R$

Konvention: Statt $a+(-b)$ schreibt man $a-b$.

weitere Rechenregeln in Ringen:

$\forall a, b \in R: \; a \cdot 0_R = 0_R, \; a(-b) = (-a)b = -ab$

$(-a)(-b) = ab$

18.10.2023

Beweis der ersten Gleichung: Sei $a \in R$

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

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

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

18.10.2023

Beispiele für Ringe und Körper.

(i) $\mathbb{Z}$ (mit der gewöhnlichen Addition und Multiplikation) ist ein Ring, darüber hinaus ein Integritätsbereich, aber kein Körper

(ii) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Körper, damit insb. Ringe ($\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$)

(iii) $\mathbb{N}$, $\mathbb{N}_0$ sind keine Ringe (erst recht also keine Körper)

(iv) Der Restklassenring $(\mathbb{Z}/42\mathbb{Z}, +, \cdot)$

18.10.2023

ist ein Ring, aber kein Integritäts-
bereich und auch kein Körper, denn:
Die Gleichung $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$ zeigt,
dass $\bar{2}$ in $\mathbb{Z}/4\mathbb{Z}$ ein Nullteiler ist.
$\Rightarrow \mathbb{Z}/4\mathbb{Z}$ ist kein Integritätsbereich
$\bar{2} \cdot \bar{0} = \bar{0}$, $\bar{2} \cdot \bar{1} = \bar{2}$, $\bar{2} \cdot \bar{2} = \bar{0}$ $\bar{2} \cdot \bar{3} = \bar{2}$
$\Rightarrow \bar{2} \cdot a \neq \bar{1}$ $\forall a \in \mathbb{Z}/4\mathbb{Z} \Rightarrow \bar{2}$ ist
keine Einheit in $\mathbb{Z}/4\mathbb{Z} \Rightarrow \mathbb{Z}/4\mathbb{Z}$
ist kein Körper

18.10.2023

Erinnerung: $\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

wobei $\bar{0} = 0 + 4\mathbb{Z} = 4\mathbb{Z}$, $\bar{1} = 1 + 4\mathbb{Z}$, ...

Regel für die Addition / Multiplikation:

Sind $a, b \in \{0, 1, 2, 3\}$, entsteht $c \in \{0, 1, 2, 3\}$ als Rest nach Division von $a+b$ durch 4, dann ist $\bar{a} + \bar{b} = \bar{c}$.

Bsp: $3 + 3 = 6 = 1 \cdot 4 + 2 \Rightarrow \bar{3} + \bar{3} = \bar{2}$

Ist $d \in \{0, 1, 2, 3\}$ der Rest nach Div. von ab durch 4, dann ist $\bar{a}\,\bar{b} = \bar{d}$

Bsp: $3 \cdot 3 = 9 = 2 \cdot 4 + 1 \Rightarrow \bar{3}\,\bar{3} = \bar{1}$

18.10.2023

Verknüpfungstabellen für $(\mathbb{Z}/4\mathbb{Z}, +)$ und $(\mathbb{Z}/4\mathbb{Z}, \cdot)$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

18.10.2023

Bem: In einem Ring R kann $0_R = 1_R$ gelten, allerdings nur, wenn $R = \{0_R\}$ gilt. Ein solcher Ring wird Nullring genannt

(denn: Sei R ein Ring mit $0_R = 1_R$ und $a \in R$

$\Rightarrow a = a \cdot 1_R = a \cdot 0_R = 0_R$)

Ein solcher Ring ist kein Integritätsbereich, somit auch kein Körper, denn 0_R ist kein Nullteiler (R wäre Körper, wenn $R^\times = R \setminus \{0_R\}$ gelten würde, aber: $R \setminus \{0_R\} = \emptyset$, $R^\times = \{0_R\}$)

18.10.2023

Unterschiedliche Schreibweisen bei Gruppen

Multiplikative Schreibweise

- wird bei einem punktähnlichen Verknüpfungssymbol wie $\cdot$, $*$ oder $\odot$ verwendet
- Notation für das Neutralelement: auch 1_G statt e_G
- Notation g^{-1} für das Inverse eines Elements $g \in G$
- Notation für die Verknüpfung zweier Elemente auch gh statt $g * h$

Unterschiedliche Schreibweisen bei Gruppen

Additive Schreibweise

- wird bei einem „plusartigen“ Verknüpfungssymbol wie $+$ oder $\oplus$ verwendet
- Notation für das Neutralelement 0_G statt e_G
- Notation $-g$ für das Inverse eines Elements $g \in G$
- nur bei kommutativen Gruppen üblich

Einheiten und Nullteiler

Definition (1.7)

Sei R ein Ring.

(i) Ein Element $a \in R$ heißt Einheit, wenn ein $b \in R$ mit $ab = 1_R$ existiert.
Die Menge der Einheiten von R bezeichnen wir mit $R^\times$.

(ii) Man nennt es Nullteiler, wenn ein Element $b \in R$, $b \neq 0_R$ mit $ab = 0_R$ existiert.

Die Einheiten eines Rings bilden nach Satz 1.5 eine Gruppe, die sog. Einheitengruppe des Rings.

Definition (1.8)

Ein Ring R mit 0_R als einzigem Nullteiler heißt Integritätsbereich.
Gilt $R^\times = R \setminus \{0_R\}$, dann ist R ein Körper.

Regeln für Einheiten und Nullteiler

Lemma (1.9)

(i) Ein Element a in einem Ring R kann nicht zugleich Nullteiler und Einheit sein.

(ii) Jeder Körper ist ein Integritätsbereich.

(iii) In jedem Integritätsbereich R gilt die Kürzungsregel: Sind $a, b, c \in R$ mit $c \neq 0_R$, dann folgt aus $ac = bc$ die Gleichung $a = b$.

Beweis von Lemma 1.9:

zu i) Ang. R ist ein Ring und $a \in R$ zugleich Einheit und Nullteiler. a Nullteiler $\Rightarrow \exists\, b \in R$ mit $b \neq 0_R$ und $a \cdot b = 0_R$ a Einheit $\Rightarrow \exists\, c \in R$ mit $a \cdot c = 1_R$

$\Rightarrow b = b \cdot 1_R = b\,a \cdot c = a \cdot b \cdot c = 0_R \cdot c = 0_R$

$\lightning$ zu $b \neq 0_R$

zu ii) Sei R ein Körper. z.zg.: R ist Integritätsbereich d.h. 0_R ist einziger Nullteiler

R Körper $\Rightarrow R^* \overset{(*)}{=} R \setminus \{0_R\}$ $\exists\, 1_R \in R^* \Rightarrow 1_R \neq 0_R$

außerdem $0_R \cdot 1_R = 0_R$ also: 0_R ist Nullteiler

18.10.2023

Sei nun $a \in R$ ein bel. Nullteiler, zzg:

$a = 0_R$ a Nullteiler $\Rightarrow \exists\, b \in R \setminus \{0_R\}$

mit $a \cdot b = 0_R$ (*) $\Rightarrow$ b ist Einheit

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

zu (iii) Sei R ein Integritätsbereich,

und seien $a, b, c \in R$ mit $c \neq 0_R$,

$ac = bc \Rightarrow ac - bc = 0_R \Rightarrow$

$(a-b)\cdot c = 0_R \overset{\text{c kein Null-teiler}}{\Rightarrow} a - b = 0_R$ □

$\Rightarrow a = b$

18.10.2023

Das Monoid der Abbildungen $X \to X$

Proposition (1.10)

Sei X eine Menge und $\mathrm{Abb}(X)$ die Menge der Abbildungen $X \to X$. Für $f, g \in \mathrm{Abb}(X)$ bezeichnet $f \circ g$ wie immer die Komposition von f und g gegeben durch

$$(f \circ g)(x) \quad = \quad f(g(x)) \qquad \text{für alle} \quad x \in X.$$

Dann ist das Paar $(\mathrm{Abb}(X), \circ)$ ein Monoid. Das Neutralelement ist die Abbildung id_X gegeben durch $\mathrm{id}_X(x) = x$ für alle $x \in X$.

Beweis von Prop 1.10:

geg.: X Menge, $\mathrm{Abb}(X)$ = Menge der Abb. $X \to X$, $\circ$ Komposition auf $\mathrm{Abb}(X)$

zu überprüfen:

(i) Die Verknüpfung $\circ$ ist assoziativ und $(\mathrm{Abb}(X), \circ)$ somit eine Halbgruppe.

(iii) Die Abb. id_X ist Neutralelement in dieser Halbgruppe.

zu (i) Seien $f, g, h \in \mathrm{Abb}(X)$, z.zg.:

$$f \circ (g \circ h) = (f \circ g) \circ h$$

18.10.2023

Sei $x \in X$, z.zg: $(f \circ (g \circ h))(x) = ((f \circ g) \circ h)(x)$ Dies ist offenbar, denn

$(f \circ (g \circ h))(x) = f((g \circ h)(x)) =$

$f(g(h(x))) = (f \circ g)(h(x)) =$

$((f \circ g) \circ h)(x)$

zu ii) Sei $f \in \mathrm{Abb}(X)$, zu überprüfen: $f \circ id_X = f$ und $id_X \circ f = f$

Sei $x \in X$, z.zg: $(f \circ id_X)(x) = f(x)$ und $(id_X \circ f)(x) = f(x)$ Dies ist

18.10.2023

erfüllt, denn $(f \circ id_X)(x) = f(id_X(x))$
$= f(x)$ und $(id_Y \circ f)(x) = id_Y(f(x)) = f(x)$
□

18.10.2023

Die Permutationsgruppe einer Menge

Proposition (1.11)

Eine Abbildung $f \in \mathrm{Abb}(X)$ ist genau dann im Monoid $(\mathrm{Abb}, \circ)$ invertierbar, wenn sie bijektiv ist. In diesem Fall ist das Inverse von f durch die Umkehrabbildung f^{-1} gegeben.

Definition (1.12)

Sei X eine Menge. Dann bildet die Teilmenge $\mathrm{Per}(X) \subseteq \mathrm{Abb}(X)$ bestehend aus den bijektiven Abbildungen $X \to X$ mit der Komposition $\circ$ von Abbildungen eine Gruppe. Man bezeichnet $(\mathrm{Per}(X), \circ)$ als die Permutationsgruppe und die Elemente von $\mathrm{Per}(X)$ als die Permutationen von X.

Ist $n \in \mathbb{N}$ und $M_n = \{1, ..., n\}$, dann ist $S_n = \mathrm{Per}(M_n)$ die bereits aus der Lineare Algebra bekannte symmetrische Gruppe.

Wiederholung zu den symmetrischen Gruppen:

(i) Für jedes $n \in \mathbb{N}$ gilt $|S_n| = n!$.

(ii) Die Elemente von S_n können in Tabellen- oder in Zyklenschreibweise angegeben werden.

Tabellenschreibweise: $\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$

steht für die Abbildung $M_n \to M_n$, $k \mapsto a_k$ $(1 \le k \le n)$ (Damit die Abbildung bijektiv ist, muss $\{a_1, a_2, \dots, a_n\} = \{1, 2, \dots, n\} = M_n$ gelten.)

18.10.2023

Bsp: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ ist die Abb. $\{1,2,3,4\} \to \{1,2,3,4\}$

$1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 4,\ 4 \mapsto 1$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

(Zykelschreibweise: $(1234) \circ (1234) = (13) \circ (24)$)

18.10.2023