# Mathematik III - Wintersemester 14/15

29. Oktober 2014

# Inhaltsverzeichnis

# 1 Algebraische Strukturen mit einer Verknüpfung HALBGRUPPEN, MONOIDE, GRUPPEN

## 1.1 Definition

Sei $X \neq \emptyset$ eine Menge.

Eine *Verknüpfung* oder (abstrakte) Multiplikation auf $X$ ist eine Abbildung

$$\bullet : \begin{array}{l} X \times X \to X \\ (a,b) \mapsto a \bullet b \end{array}$$

$\underset{(ab)}{a \bullet b}$ heißt *Produkt* von $a$ und $b$, muss aber mit der üblichen Multiplikation von Zahlen nichts zu tun haben.

Beschreibung bei endlichen Mengen oft durch Multiplikationstafeln.

## 1.2 Beispiel

a) $X = \{a,b\}$

| $\bullet$ | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $b$ |
| $b$ | $a$ | $a$ |

$(a \bullet a) \bullet a = b \bullet a = a$
$a \bullet (a \bullet a) = a \bullet b = b \qquad \to$ nicht assoziativ

b) $X = \mathbb{Z}^-$ $(= \{0,-1,-2,\dots\})$
Die normale Multiplikation ist auf $\mathbb{Z}^-$ keine Verknüpfung!
(zum Beispiel ist $(-2)\cdot(-3) = 6 \notin \mathbb{Z}^-$)
Aber auf $X = \mathbb{N}, X = \mathbb{Z}$ oder $X = \{1\}, X = \{0,1\}$

## 1.3 Definition

Sei $H \neq \emptyset$ eine Menge mit Verknüpfung.

$(H, \bullet)$ heißt *Halbgruppe*, falls gilt:

$$\forall a,b,c \in H \; : \; (a \bullet b) \bullet c = a \bullet (b \bullet c) \qquad \text{(Assoziativgesetz (AG))}$$

## 1.4 Bemerkung

AG sagt aus: bei endlichen Produkten ist die Klammerung irrelevant, z.B.

$(a \cdot b) \cdot (c \cdot d) = ((a \cdot b) \cdot c) \cdot d = (a \cdot (b \cdot c)) \cdot d$ (usw.)

Deshalb werden Klammern meistens weggelassen.

Die Reihenfolge der Elemente ist i.A. relevant!

## 1.5 Beispiel

a) $(\mathbb{N}, \bullet), (\mathbb{Z}, \bullet), (\mathbb{Q}, \bullet), (\mathbb{R}, \bullet)$ [1] sind Halbgruppen.
   Ebenso $(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ [2]

b) $(\mathbb{Q}\backslash\{0\}, :)$ [3] ist *keine* Halbgruppe, denn z.B. $\begin{array}{rcl} (12:6):2 & = & 1 \\ 12:(6:2) & = & 4 \end{array}$

c) vgl. Vorlesung Theoretische Informatik
   $A \neq \emptyset$ endliche Menge ("Alphabet")
   $A^+ = \cup_{n \in N} A^n$ = Menge aller endlichen Wörter über $A$
   (z.B. $A = \{a, b\}$, dann ist z.B. $\underbrace{(a, a, b)}_{aab} \in A^3$)
   Verknüpfung: Konkatenation (Hintereinanderschreiben)
   z.B. $aab \bullet abab = aababab$
   $A^* = A^+ \cup \{\lambda\}$ $\quad \lambda$ (oder $\epsilon$) ist das leere Wort
   Es gilt: $\lambda \cdot w = w \cdot \lambda = w \ \forall w \in A^*$
   $(A^+, \bullet), (A^*, \bullet)$ *Worthalbgruppe* über $A$

d) $M \neq \emptyset$ Menge, Abb$(M, M)$: Menge aller Abbildungen $M \to M$ mit $\circ$ (Komposition) ist Halbgruppe.

e) (WICHTIG)
   $n \in \mathbb{N}$, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
   Verknüpfung: $\begin{array}{l} \oplus : a \oplus b := (a + b) \mod n \\ \odot : a \odot b := (a \cdot b) \mod n \end{array}$
   $(\mathbb{Z}_n, \oplus), (\mathbb{Z}_n, \odot)$ sind Halbgruppen.

## 1.6 Definition

Eine Halbgruppe $(H, \bullet)$ heißt *kommutativ*, falls gilt:

$$\forall a, b \in H \ : \ a \cdot b = b \cdot a \qquad \text{(Kommutativgesetz, KG)}$$

## 1.7 Beispiel

Beispiele 1.5 a), e) sind kommutative Halbgruppe.
(hallo ≠ ollah, ab ≠ ba, Worthalbgruppe nicht kommutativ)

[1] $\bullet$ normale Multiplikation
[2] + normale Addition
[3] : normale Division

### 1.8 Definition

Sei $(H, \bullet)$ Halbgruppe, $\emptyset \neq U \subseteq H$

$U$ heißt *Unterhalbgruppe* von $H$, falls $u \cdot v \in U \; \forall u, v \in U$ gilt.

$(U, \odot)$ ist dann selbst Halbgruppe.

### 1.9 Beispiel

$(\mathbb{Z}, +)$ Halbgruppe

$G$ = Menge aller gerade ganzen Zahlen $\subseteq \mathbb{Z}$
$(G, +)$ ist Unterhalbgruppe von $(\mathbb{Z}, +)$

$U$ = Menge aller ungerade Zahlen $\subseteq \mathbb{Z}$
$(U, +)$ ist keine Unterhalbgruppe!

### 1.10 Lemma

Sei $(H, \bullet)$ Halbgruppe, $e_1, e_2 \in H$ mit $^{(*)} e_1 \cdot x = x \cdot e_1 = x$ und $^{(**)} e_2 \cdot x = x \cdot e_2 = x \; \forall x \in H$

Dann ist $e_1 = e_2$

*Beweis.* $e_1 \overset{(**)}{=} e_1 \cdot e_2 \overset{(*)}{=} e_2$ □

### 1.11 Definition

Eine Halbgruppe $(H, \bullet)$ heißt *Monoid*, falls $e \in H$ existiert mit $e \cdot x = x \cdot e = x \; \forall x \in H$

$e$ heißt *neutrales Element* / Einselement / Eins in $H$.
Schreibweise: $(H, \bullet, e)$

Für additive Verknüpfung oft 0 für $e$ (Nullelement)
multiplikative 1

Nach 1.10 ist das neutrale Element eindeutig!

### 1.12 Beispiele

a) $(\mathbb{N}, \bullet)$ Monoid mit $e = 1$
$(\mathbb{N}, +)$ kein Monoid
$(\mathbb{N}_0, +)$ Monoid mit $e = 0$
$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ Monoide mit $e = 0$
$(\mathbb{Z}, \bullet), (\mathbb{N}_0, \bullet), (\mathbb{Q}, \bullet), (\mathbb{R}, \bullet)$ Monoide mit $e = 1$

b) $(\mathrm{Abb}(M, M), \circ)$ Monoid, $e = \mathrm{id}$

c) $(\mathbb{Z}_n, \oplus)$ Monoid, $e = 0$
$(\mathbb{Z}_n, \odot)$ Monoid, $e = 1$

d) $(A^*, \bullet)$ Monoid, $e = \lambda$ (hallo$\lambda$ = $\lambda$hallo = hallo)

### 1.13 Definition

Sei $(M, \bullet, e)$ Monoid. Eine Teilmenge $\emptyset \neq U \subseteq M$ heißt *Untermonoid* von $M$, falls $U$ mit $\bullet$ selbst ein Monoid mit neutralem Element $e$ ist (also $e \in U$)

### 1.14 Lemma

Sei $(H, \bullet, e)$ Monoid und es gebe zu jedem Element $h \in H$ Elemente $x, y \in H$ mit $h \cdot x \overset{(*)}{=} e \overset{(**)}{=} y \cdot h$.

Dann ist $x = y$

*Beweis.* $y = y \cdot e \overset{(*)}{=} y \cdot (h \cdot x) \overset{(\mathrm{AG})}{=} (y \cdot h) \cdot x \overset{(**)}{=} e \cdot x = x$ □

### 1.15 Definition

(i) $(H, \bullet, e)$ Monoid, $h \in H$

Falls ein $x \in H$ existiert mit $hx = xh = e$, so nennt man $h$ *invertierbar* und $x$ das *Inverse* zu $h$, bez. $h^{-1}$ (bei additiven Verknüpfungen oft auch $-h$)

Nach 1.14 ist $h^{-1}$ eindeutig bestimmt!

Es gilt: $e$ ist immer invertierbar, $e^{-1} = e$

(ii) Ein Monoid $(G, \bullet, e)$ heißt *Gruppe*, falls <u>jedes</u> Element in $G$ invertierbar ist.

(iii) Für eine endliche Gruppe $G$ heißt die Anzahl der Elemente in $G$ die *Ordnung* von $G$, $|G|$

### 1.16 Bemerkung

$(H, \bullet, e)$ Monoid.

Sei $G$ die Menge aller invertierbaren Elemente von $H$, dann ist $(G, \bullet, e)$ eine Gruppe.

Es gilt: $e$ invertierbar $(e^{-1} = e)$

und falls $g$ invertierbar, dann ist auch $g^{-1}$ invertierbar: $(g^{-1})^{-1} = g$

falls $g, h$ invertierbar, dann auch $g \cdot h$: $\quad (g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$

### 1.17 Beispiel

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ x = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ - Was ist $x$?

$a \cdot x = b \Leftrightarrow x = a^{-1} \cdot b$

$\lambda = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}^{-1} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

### 1.18 Definition

$(G,\cdot)$ Gruppe, $\emptyset \neq U \subseteq G$ Teilmenge.

$U$ heißt *Untergruppe* von $G$ ($U \leqslant G$), falls $u$ bzgl. $\cdot$ selbst eine Gruppe ist.

Insbesondere gilt dann: $\forall u, v \in U$ ist $u \cdot v \in U$.
$e$ von $G$ ist auch neutrales Element von $u$.
Inversen in $U$ sind die gleichen wie in $G$.

Angenommen $e$ neutrales Element in $G$, aber $f$ neutrales Element in $U$, $f^{-1}$ Inverses von $f$ in $G$.
Dann ist $f^{-1} \cdot f = f \cdot f^{-1} = e$ und $f \cdot f = f$.
$\Rightarrow f = e \cdot f = (f^{-1} \cdot f) \cdot f = f^{-1} \cdot (f \cdot f) = f^{-1} \cdot f = e$

### 1.19 Beispiele

a) $(\mathbb{Z},+) \leqslant (\mathbb{Q},+) \leqslant (\mathbb{R},+)$

b) $(\{-1,1\},\cdot) \leqslant (\mathbb{Q}\backslash\{0\},\cdot) \leqslant (\mathbb{R}\backslash\{0\},\cdot)$

c) $(e,\cdot)$ ist Untergruppe jeder beliebigen Gruppe mit Verknüpfung $\cdot$ und neutralem Element $e$.

d) $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$, $\pi = \pi^{-1}, \pi^{-1} \circ \pi = \mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
$\Rightarrow (\pi, \mathrm{id}) \leqslant S_3$

### 1.20 Satz und Definition

$G$ Gruppe, $U \leqslant G$

(a) Durch $x \sim y \Leftrightarrow x \cdot y^{-1} \in U$
TODO "Das muss unter die obere Zeile: bei additiver Verknüpfung: $x + (-y) \in U (x - y \in U)$
wird auf $G$ eine Äquivalenzrelation definiert
Beweis:
$\sim$ ist reflexiv: $x \sim x$ gilt $\forall x \in G$, denn $x \cdot x^{-1} = e \in U$ ✓
$\sim$ ist symmetrisch: $x \sim y \Rightarrow y \sim x$
Sei $x \sim y$, also $x \cdot y^{-1} \in U$ (zzg.: $y \sim x$, also $y \cdot x^{-1} \in U$) dann ist $y \cdot x^{-1} = (x \cdot y^{-1})^{-1} \in U$, da auch $x \sim y \Leftrightarrow x \cdot y^{-1} \in U$.
$\sim$ ist transitiv: $x \sim y, y \sim z \Rightarrow x \sim z$
Sei $x \sim y$, also $x \cdot y^{-1} \in U$ und $y \sim z$, also $y \cdot z^{-1} \in U$ (zzg.: $x \sim z$, d.h. $x \cdot z^{-1} \in U$)
$x \cdot z^{-1} = (\underbrace{x \cdot y^{-1}}_{\in U}) \cdot (\underbrace{y \cdot z^{-1}}_{\in U}) \in U$, also $x \sim z$.

(b) Für $x \in G$ ist $Ux = \{u \cdot x | u \in U\}$ die Äquivalenzklasse von $x$ bzgl. $\sim$ und heißt Rechtsnebenklasse von $U$ in $G$.
Also (Eigenschaften von Äquivalenzklassen siehe Mathe I):

i. $Ux = Uy \Leftrightarrow x \sim y$, also $x \cdot y^{-1} \in U$
ii. $x, y \in G$, dann ist entweder $Ux = Uy$ oder $Ux \cap Uy = \emptyset$

Beweis:

i. Seit $x \sim y \Rightarrow y \sim x \Rightarrow y \cdot x^{-1} \in U \Rightarrow y = y(x^{-1} \cdot x) = \underbrace{(y \cdot x^{-1})}_{\in U} x \in Ux$

ii. Sei $y \in Ux$, dann zeige: $x \sim y$
$y \in Ux \Rightarrow y = u \cdot x$ für ein $u \in U$
$\Rightarrow x \cdot y^{-1} = x \cdot (ux)^{-1} = x \cdot x^{-1} \cdot u^{-1} = u^{-1} \in U$
Es wurde gezeigt, dass $x \sim y$ gilt.

### 1.21 Beispiel

$G = (\mathbb{Z}, +), 3\mathbb{Z} = \{\dots, -3, 0, 3, 6, \dots\}$
$U = (3\mathbb{Z}, +) \leqslant G$ (ÜA, Blatt 2)
Inverses zu y in $(\mathbb{Z}, +)$ ist $-y$.
$x \sim y \Leftrightarrow \underbrace{x \cdot y^{-1} \in U}_{\text{bzw.: } x-y \in U}$
$x = 0 : U + 0 = \{u + 0 | u \in U\} = \{\dots, -3, 0, 3, 6, \dots\}$
$x = 1 : U + 1 = \{u + 1 | u \in U\} = \{\dots\}$

### 1.22 Beispiel

a) Wir können annehmen, dass $1 \leq a < n$ (denn $a^{\Phi(n)} \mod n = (a \mod n)^{\Phi(n)}$)
wegen $\mathrm{ggT}(a, n) = 1$ ist $a \in \mathbb{Z}_n^*$, das ist eine ednliche Gruooe.
$\Rightarrow a^{|\mathbb{Z}_n^*|} = 1 (= e)$ $\qquad a \odot a \odot \dots$
$\Rightarrow a^{\Phi(n)} \equiv 1 (\mod n)$ $\qquad a \cdot a \cdot \dots$

b) Folgt aus (i) ($n = p$, $\varphi(p) = -1$)

## 2 Algebraische Strukturen mit 2 Verknüpfungen: Ringe und Körper

### 2.1 Definition

Sei $R \neq \emptyset$ eine Menge mit zwei Verknüpfungen $+$ und $\cdot$.

a) Wir nennen $(R, +, \cdot)$ einen *Ring*, falls gilt:

(a) $(R, +)$ ist eine abelsche Gruppe (Eselsbrücke: KAIN)
Das neutrale Element bezeichnen wir hier mit 0, das zu $a \in \mathbb{R}$ Inverse mit $-a$ (schreibe auch $a - b$ für $a = (-b)$.

(b) $(R, \cdot)$ ist eine Halbgurppe.

(c) Es gelten die Distributivgesetze:
$a \cdot (b + c) = (a \cdot b) + (a \cdot c) = ab + ac$
$(a + b) \cdot c - (a \cdot c) + (b \cdot c) = ac = bc$

b) Ein Ring $(R, +, \cdot)$ heißt *kommutativ* falls $\cdot$ ebenfalls kommutativ ist, also falls $\forall a, b \in \mathbb{R} : a \cdot b = b \cdot a$

c) Ein Ring $(R, +, \cdot)$ heißt *Ring mit Eins*, falls $(R, \cdot)$ ein Monoid ist mit neutralen Element $1 \neq 0$ $(\forall a \in R : a \cdot 1 = 1 \cdot a = a)$.

d) Ist $(R, +, \cdot)$ Ring mit Eins, dann heißen die bezüglich $\cdot$ invertierbaren Elemente *Einheiten*. Das zu $a$ bezügliche $\cdot$ invertierbare Elemente bezeichnen wir mit $a^{-1}$.
$R^*$ := Menge der Einheiten in $R$.

## 2.2 Beispiel

a) $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring mit Eins (1)
$\mathbb{Z}^* = \{1, -1\}$
$(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ ebenso
$\mathbb{Q}^* = \mathbb{Q} \backslash \{0\}, \mathbb{R}^* = \mathbb{R} \backslash \{0\}$.

b) $(2\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring ohne Eins

c) trivialer Ring $(\{0\}, +, \cdot)$ ohne Eins

d) $n \in \mathbb{N}, n \geq (\mathbb{Z}_n, \oplus, \odot)$ kommutativer Ring mit Eins

e) $(\mathbb{R}, \underbrace{+, \cdot}_{\text{Komponentenweise}})$; allgemein: $R_1, \dots, R_n$ Ringe, dann $R_1, \times \cdots \times R_n$ Ring.

f) $Mn(\mathbb{R})$ - Menge aller $n \times n$-Matrizen über $\mathbb{R}$, mit Matrixaddition und -multiplikation ist Ring mit Eins ($=E_n$), nicht kommutativ für $n \geq 2$.

## 2.3 Satz (Rechnen mit Ringen)

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

a) $a \times 0 = 0 \times a = 0$

b) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

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

Beweis:

a) $a \cdot 0 = a \cdot (0 + 0) \underset{2.1(3)}{=} a \cdot 0 + a \cdot 0$
addiere $-(a \cdot 0)$ (Inverses von $a \cdot 0$) auf beiden Seiten $\Rightarrow$ erhalte $0 = a \cdot 0$
Analog $0 \cdot a = 0$

b) $(-a) \cdot b + a \cdot b \underset{2.1(3)}{=} (-a + a) \cdot b = 0 \cdot b \overset{(i)}{=} 0$
also ist $(-a \cdot b)$ Inverses zu $a \cdot b$, also $= -(a \cdot b)$