Mathematik in Medien und Informatik

Zahlen und Rechenbereiche (algebraische Strukturen) 2

Prof. Dr. Thomas Schneider

Stand: 05.10.2022

HOCHSCHULE FURTWANGEN UNIVERSITY | HFU

Inhalt

Vorbemerkungen

Zahlenmengen und Rechenbereiche

Sie kennen die folgenden Rechenbereiche:

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$	Menge der natürlichen Zahlen
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$	Menge der ganzen Zahlen
$\mathbb{Q} = \left\{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\}\right\}$	Menge der rationalen Zahlen
$\mathbb{R} = \mathbb{Q} \cup \left\{\sqrt{2}, \sqrt[3]{7}, \dots, e, \pi, \dots\right\}$	Menge der reellen Zahlen.

Bemerkung

$\mathbb{R}$ enthält alle rationalen und (ungeheuer viele) irrationale Zahlen.

Vorbemerkungen
Rechenoperationen in Zahlenmengen

Erinnerung

- Welche Rechenoperationen sind in $\mathbb{N}$ bzw. $\mathbb{Z}$ bzw. $\mathbb{Q}$ (oder $\mathbb{R}$) sind möglich, ohne den jeweiligen Rechenbereich zu verlassen?
- Welche Rechengesetze gelten hierbei?

Vorbemerkungen

Rechenoperationen in Zahlenmengen

Rechen-bereich	Rechen-operationen	Rechengesetze / Beobachtungen
$\mathbb{N}$	$+,\ \cdot$	$2+0=2=0+2$ $3\cdot 1=3=1\cdot 3$
$\mathbb{Z}$	$+,\ \cdot,\ -$	$2+(-2)=0=-2+2$
$\mathbb{Q}$	$+,\ \cdot,\ -,\ ^{-1}$	$\left(\frac{2}{3}\right)^{-1}=\frac{3}{2}\leftrightarrow\frac{2}{3}\cdot\frac{3}{2}=1=\frac{3}{2}\cdot\frac{2}{3}$
$\mathbb{R}$	$+,\ \cdot,\ -,\ ^{-1}$	$\left(\sqrt{2}\right)^{-1}=\frac{1}{\sqrt{2}}$
$\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$		$(2+3)+5=2+(3+5)$ $(3\cdot 4)\cdot 5=3\cdot(4\cdot 5)$
$\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$		$3\cdot(4+5)=3\cdot 4+3\cdot 5$ $(4+5)\cdot 3=4\cdot 3+5\cdot 3$
$\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$		$2+5=5+2$ $3\cdot 4=4\cdot 3$

Eigenschaften bekannter Rechenbereiche

Die Addition bzw. Multiplikation in $\mathbb{N}$ (und auch in $\mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$) haben die folgenden Eigenschaften:

- Für jede beliebige Kombination a, b, c gilt:

$$(a + b) + c = a + (b + c) \qquad \text{und}$$
$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

  Diese Eigenschaft heißt **Assoziativität** der Addition bzw. der Multiplikation. Man sagt auch:
  - Es gilt das Assoziativgesetz für die Addition bzw. für die Multiplikation.
  - Die Addition ist assoziativ, die Multiplikation ist assoziativ.

- Für jede beliebige natürliche Zahl n gilt außerdem:

$$n + 0 = n = 0 + n \qquad \text{sowie}$$
$$n \cdot 1 = n = 1 \cdot n.$$

  Man sagt:
  0 ist das **Neutralelement bzgl. der Addition**,
  1 ist das **Neutralelement bzgl. der Multiplikation**.

Eigenschaften bekannter Rechenbereiche

- In $\mathbb{Z}$ gibt es zu jeder Zahl z eine „Gegenzahl“ $-z$ mit

$$z + (-z) = 0 = (-z) + z.$$

- Das hierzu Analoge gilt für die Multiplikation in $\mathbb{Z}$ **nicht**; für die ganze Zahl 2 etwa gibt es **keine** ganze Zahl a mit $2 \cdot a = 1$.

  Dagegen gibt es in $\mathbb{Q}$ eine solche **multiplikative Inverse** a **von** 2, nämlich

$$a = \frac{1}{2}.$$

- Für jede Zahl $x \in \mathbb{Q}$, außer der Null, gibt es einen sogenannten **Kehrbruch** x' mit

$$x \cdot x' = 1 = x' \cdot x.$$

  Wir schreiben anstelle von x' meistens $\frac{1}{x}$ oder x^{-1}.

Typen von Rechenbereichen

Gruppen

Wir nehmen die voranstehenden Beobachtungen zum Anlass für die nachstehenden Definitionen:

Definition:

Auf einer Menge G sei eine (binäre) Verknüpfung $*$ erklärt. Die Struktur $(G, *)$ heißt **Gruppe**, wenn Folgendes gilt:

1. $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$ (**Assoziativität**).
2. Es gibt ein **Neutralelement** $e \in G$ mit

$$a * e = a = e * a \text{ für alle } a \in G.$$

3. Zu jedem Element $a \in G$ existiert ein **inverses Element** a^{-1} mit

$$a * a^{-1} = e = a^{-1} * a.$$

Bemerkung:

Zur Bezeichnung einer Gruppe mit Verknüpfung $*$ und Neutralelement e sind die Bezeichnungen G oder $(G, *)$ oder $(G, *, e)$ möglich.

Beispiele:

Ist $(\mathbb{N}, +)$ eine Gruppe?	Nein, denn (3) ist nicht erfüllt.
Ist $(\mathbb{Z}, +)$ eine Gruppe?	Ja, denn $(1) - (3)$ sind erfüllt.
Ist $(\mathbb{Z}, \cdot)$ eine Gruppe?	Nein, denn (3) ist nicht erfüllt.
Ist $(\mathbb{Q}, \cdot)$ eine Gruppe?	Nein, denn 0 hat kein inverses Element.
Ist $(\mathbb{Q} \setminus \{0\}, \cdot)$ eine Gruppe?	Ja, denn $(1) - (3)$ sind erfüllt.

Typen von Rechenbereichen / algebraischen Strukturen

Noch mehr Definitionen ☺

Definition:

$(G, *)$ heißt **Halbgruppe**, wenn die Bedingung (1) aus Def. 6 (Assoziativität) erfüllt ist.

$(G, *)$ heißt **Monoid**, wenn die Bedingung (1) und (2) aus Def. 6 erfüllt ist (Assoziativität und Neutralelement).

Eine Gruppe $(G, *)$ heißt **kommutative Gruppe** (kGp), wenn $a * b = b * a$ für alle $a, b \in G$ gilt (Kommutativität).

Beispiele:

- $(\mathbb{N}, +, 0)$ ist ein Monoid.
- $(\mathbb{Z}, +, 0)$ ist eine kommutative Gruppe.

Gruppentafeln

Bauweise

Ein Werkzeug um Gruppen darzustellen sind Verknüpfungstafeln (bzw. Gruppentafeln). Die Bauweise einer Gruppentafel wird anhand einer Gruppe mit den Elementen e, a, b, c und Verknüpfung $*$ anhand des folgenden Schemas illustriert:

$*$	e	a	b	c
e				
a				$a * c$
b				
c		$c * a$		

Gruppentafeln
Bauweise

Die Verknüpfungstafeln von Gruppen sind nicht beliebig, sondern gehorchen dem (von uns so genannten)

Sudoku-Prinzip

In jeder Zeile und in jeder Spalte der Verknüpfungstafel einer Gruppe G steht jedes Element von G genau einmal.

Begründung: Im Folgenden wird diese Aussage in vier Teilaussagen zerlegt, die wir separat begründen.

Gruppentafeln

„Sudoku-Prinzip“

Teil 1: In jeder Zeile einer Gruppentafel steht jedes Element höchstens einmal.

Begründung:

$*$	$\ldots$	a	b	$\ldots$
$\ldots$				
x		$x * a$	$x * b$	
$\ldots$				

Würde in einer Zeile x in zwei voneinander verschiedenen Spalten a und b das gleiche Element stehen, so ergäbe sich daraus:

$$
\begin{aligned}
x * a &= x * b && \downarrow x^{-1} * \\
x^{-1} * (x * a) &= x^{-1} * (x * b) && \downarrow \text{Assoziativgesetz} \\
(x^{-1} * x) * a &= (x^{-1} * x) * b && \downarrow x^{-1} * x = e \\
e * a &= e * b \\
\rightsquigarrow \quad a &= b,
\end{aligned}
$$

im Widerspruch zur Annahme, dass a und b voneinander verschieden sind.

Gruppentafeln

„Sudoku-Prinzip“

Teil 2: In jeder Zeile einer Gruppentafel steht jedes Element mindestens einmal.

Es sei g ein beliebiges Gruppenelement

$*$	$\ldots$	a	$\ldots$
$\ldots$			
x		$x * a$	
$\ldots$			

Zu zeigen ist: Es gibt eine Spalte a, in der das beliebige Gruppenelement g steht. Wir lösen die Gleichung

$$x * a = g \qquad \downarrow x^{-1} *$$
$$x^{-1} * (x * a) = x^{-1} * g$$
$$a = x^{-1} * g \qquad \checkmark \text{ Es gibt eine Lösung!}$$

Wir stellen fest, dass das Element g in der Zeile x und der Spalte a steht, wobei $a = x^{-1} * g$ zu wählen ist.

Gruppentafeln

„Sudoku-Prinzip“

Teil 3: In jeder Spalte einer Gruppentafel steht jedes Element höchstens einmal.

Teil 4: In jeder Spalte einer Gruppentafel steht jedes Element mindestens einmal.

Begründung entsprechend der vorherigen Begründungen für Zeilen, durch Vertauschung von Zeilen und Spaltenbezeichnungen.

$\rightsquigarrow$ Wir haben gezeigt, dass jedes Gruppeneelement **mindestens einmal**, aber auch **höchstens einmal** in jeder Zeile und jeder Spalte der Gruppentafel vorkommt. Daraus folgt, dass jedes Gruppenelement wie beim Sudoku-Spiel **genau einmal** darin vorkommt.

Gruppentafeln

der kleinsten Gruppen

Wir untersuchen nun, wie die Verknüpfungstafeln für (einige kleine) endliche Gruppen aussehen (können). Im Folgenden bezeichnet n die sogenannte *Gruppenordnung*, d.h. die Anzahl der Elemente der Gruppe.

n=1

$*$	e
e	e

n=2

$*$	e	z
e		
z		

$\rightsquigarrow$

$*$	e	z
e	e	z
z	z	

$\rightsquigarrow$

$*$	e	z
e	e	z
z	z	e

Gruppentafeln
der kleinsten Gruppen

Beispiel einer Interpretation

Man kann sich die Gruppe mit zwei Elementen realisiert denken, indem man e mit der Menge der geraden Zahlen (g) und z mit der Menge der ungeraden Zahlen (u) identifiziert.

$*$	e	z
e	e	z
z	z	e

$$\begin{array}{c} e \to g \\ \longleftrightarrow \\ z \to u \\ * \to + \end{array}$$

$+$	g	u
g	g	u
u	u	g

Gruppentafeln

der Gruppen mit drei bzw. vier Elementen

Füllen Sie die Gruppentafel für $n = 3$ sowie $n = 4$ selbst aus.

n=3

$*$	e	x	y
e			
x			
y			

n=4

$*$	e	a	b	c
e				
a				
b				
c				

Gruppentafeln

der Gruppen mit drei Elementen

Im Falle $n = 3$ gibt es nach Festlegung der Reihenfolge e, x, y nur eine einzige Verknüpfungstafel:

n=3

$*$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Gruppentafeln

der Gruppen mit vier Elementen

Im Falle $n = 4$ gibt es vier unterschiedliche Gruppentafeln.

n=4

①

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

②

$*$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

③

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

④

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

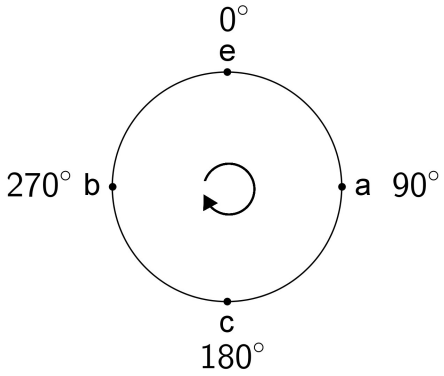
Gruppentafeln

der Gruppen mit vier Elementen

Wir werden im Folgenden sehen, dass die ersten drei Gruppentafeln im Grunde gleich sind, während die vierte Tafel andere Eigenschaften hat.

Zum Beispiel: ②

$*$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e



Jedem Element ist ein Winkel zugewiesen. Durch Addition der Winkel zweier Elemente erhält man das Ergebnis derer Verknüpfung.

z. B.: $e \mathrel{\widehat{=}} 0°, a \mathrel{\widehat{=}} 90°, e * a \to 0° + 90° = 90° \mathrel{\widehat{=}} a \quad \to a * e = a$

oder: $c \mathrel{\widehat{=}} 180°, c * c \to 180° + 180° = 360° \mathrel{\widehat{=}} 0° \mathrel{\widehat{=}} e \to c * c = e$

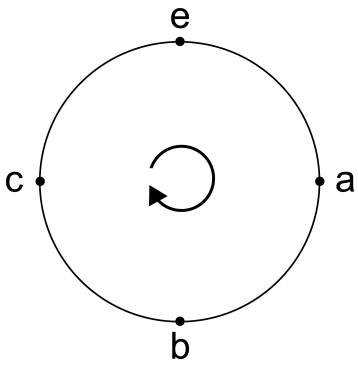
Gruppentafeln

der Gruppen mit vier Elementen

Eine solche Abbildung auf den Kreis ist für die ersten drei Gruppentafeln von $n = 4$ möglich.

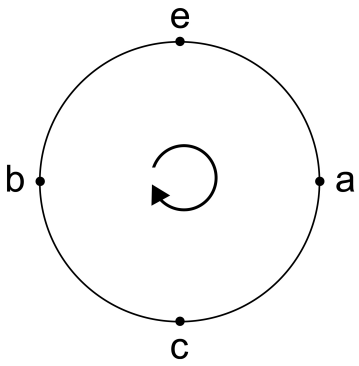
①

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b



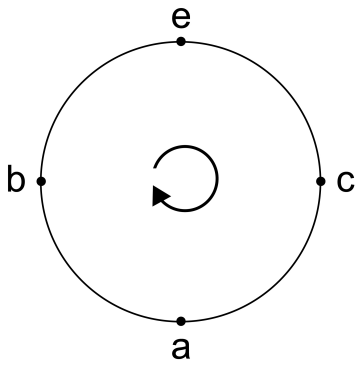
②

$*$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e



③

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a



Zyklische Gruppen und Erzeuger

Um das bisher Gesagte präzise zu machen, benötigen wir die folgende Definition:

Definition:

1. Es sei G eine Gruppe, $g \in G$. Die Menge

$$\langle g \rangle := \{e, g, g * g, g * g * g, \ldots\} \cup \{g^{-1}, g^{-1} * g^{-1}, \ldots\}$$

heißt (Gruppen-)**Erzeugnis** von g.

2. Falls das Erzeugnis eines Elementes g gleich der ganzen Gruppe G ist (falls also $\langle g \rangle = G$ gilt), so heißt g **Erzeuger von** G.
3. Falls G mindestens einen Erzeuger besitzt, so heißt G **zyklische Gruppe**.

Beispiel:

$(\mathbb{Z}, +)$ ist eine zyklische Gruppe mit Erzeugern 1 und -1.

Zyklische Gruppen und Erzeuger

Satz:

Falls eine Gruppe G endlich viele Elemente hat, so gilt für das Erzeugnis eines jeden Elements $g \in G$:

$$\langle g \rangle = \{e, g, g * g, g * g * g, \ldots\}$$

Beispiel:

Jede der auf Folie 20 angegebenen Gruppen der Ordnung $n = 4$ ist zyklisch. So hat z.B. die unter ① gegebene Gruppe den Erzeuger a. Dagegen ist die auf Folie 18 zuletzt angegebene Gruppe der Ordnung $n = 4$ *nicht* zyklisch, denn:

$$\langle e \rangle = \{e\},\ \langle a \rangle = \{e, a\},\ \langle b \rangle = \{e, b\},\ \langle c \rangle = \{e, c\}$$

Weitere algebraische Strukturen

Ringe

Definition:

Auf einer Menge R seien zwei Verknüpfungen $+$ und $\cdot$ erklärt, und es sei $0 \in R, 1 \in R, 0 \neq 1$.

Es gelte:

1. $\left(R, +, 0\right)$ ist eine kommutative Gruppe.
2. $\left(R, \cdot, 1\right)$ ist ein Monoid.
3. Für alle $a, b, c \in R$ gilt:

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

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

Dann heißt $\left(R, +, 0, \cdot, 1\right)$ ein **Ring** (mit 1).

Weitere algebraische Strukturen

Ringe

Bemerkungen:

1. In Punkt (3) der vorstehenden Definition wird die sogenannte Distributivität gefordert.
2. Da wir nicht (generell) davon ausgehen können, dass die Multiplikation in einem gegebenen Ring kommutativ ist, benötigen wir tatsächlich beide Distributivgesetze.

Beispiele für Ringe:

- Die Menge der ganzen Zahlen $\big(\mathbb{Z},\, +,\, 0,\, \cdot,\, 1\big)$.
- Die Menge der Restklassen modulo n (vgl. die Übungen).
- Die Menge der $n \times n$-Matrizen (siehe Kapitel 6).

Weitere algebraische Strukturen

Körper

Definition:

1. Ein Ring $(R, +, 0, \cdot, 1)$ heißt **Körper** (engl. *field*), wenn $(R \setminus \{0\}, \cdot, 1)$ eine Gruppe ist.
2. Ein Körper heißt **kommutativer** Körper, wenn die multiplikative Struktur (Gruppe) *kommutativ* ist.

Beispiel:

$\mathbb{Q}$ und $\mathbb{R}$ sind kommutative Körper

Bemerkungen:

- Alle endlichen Körper sind kommutativ.
- Es gibt auch nicht kommutative Körper, z. B. der Hamiltonsche Quaternionenkörper ($\rightsquigarrow$ interessant für die Darstellung von Drehungen in der Computergrafik / bei Computerspielen).

Der Körper $\mathbb{F}_2$

Additive Struktur

Der Körper $\mathbb{F}_2$ enthält die Elemente 0 und 1. Seine additive Struktur ist eine Gruppe mit 2 Elementen (vgl. Folie 15):

$*$	e	z
e	e	z
z	z	e

$$\begin{array}{c} e \to 0 \\ \longleftrightarrow \\ z \to 1 \\ * \to + \end{array}$$

$+$	0	1
0	0	1
1	1	0

Der Körper $\mathbb{F}_2$

Additive Struktur von $\mathbb{F}_2$:

$+$	0	1
0	0	1
1	1	0

Die multiplikative Struktur ist wie folgt:

$\cdot$	0	1
0	0	0
1	0	1

$\mathbb{F}_2 = \{\{0, 1\}, +, 0, \cdot, 1\}$

Der Körper $\mathbb{F}_2$

Bemerkungen:

- Addition und Multiplikation in $\mathbb{F}_2$ verhalten sich wie die entsprechenden Operationen auf den Klassen der geraden bzw. ungeraden ganzen Zahlen.
- Die Multiplikationstafel

$\cdot$	0	1
0	0	0
1	0	1

bildet **kein** Sudoku.

- Für **jeden** Körper K bildet **nicht** $(K, \cdot)$, sondern

$$K^* := (K \setminus \{0\}, \cdot)$$

eine Gruppe.