Kapitel 4

Algebra

- Relationen
- Gruppen
- Ringe und Körper
- Anwendungen

Geordnete Paare

Bei Mengen kommt es auf die Reihenfolge der Elemente nicht an, so z.B.

$$\{x_1, x_2\} = \{x_2, x_1\}.$$

Dies ist ganz anders bei Folgen, wo ja die einzelnen Folgenglieder quasi durchnummeriert werden.

Ähnliche Gebilde wollen wir im Folgenden definieren:

Mit dem Symbol (x_1, x_2) bezeichnet man das *geordnete Paar* von x_1 und x_2; hier ist im Allgemeinen

$$(x_1, x_2) \neq (x_2, x_1)$$

(außer bei $x_1 = x_2$).

Produktmenge, n–Tupel

Definition

Unter der Produktmenge $A_1 \times A_2$ von A_1 und A_2 versteht man die Menge aller geordneten Paare (x_1, x_2) mit $x_1 \in A_1$, $x_2 \in A_2$:

$$A_1 \times A_2 := \{(x_1, x_2) \,|\, x_1 \in A_1, x_2 \in A_2\}.$$

Analog ist

$$A_1 \times A_2 \times ... \times A_n := \{(x_1, x_2, ..., x_n) \,| \; x_k \in A_k \text{ für } k = 1, 2, ..., n\}$$

die Menge aller geordneten n–Tupel $(x_1, x_2, \ldots, x_n)$ und heißt Produktmenge von $A_1, A_2, \ldots$ und A_n.
Gilt $A_1 = A_2 = \ldots = A_n = A$, so schreibt man kurz $A^n := A \times A \times \ldots \times A$.

Kartesisches Produkt

Man kann die Produktmenge auch *Kartesisches Produkt* nennen. Diese Begriffe sind schon aus der Analytischen Geometrie der Schule bekannt:

So ist etwa $(-3, 4) \in \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ ein Punkt der Ebene, während ein Punkt des Raums durch sein *Koordinaten–Tripel* („3–Tupel“) (x, y, z) repräsentiert wird. Man kann also

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) | \, x, y, z \in \mathbb{R}\}$$

mit den Punkten des dreidimensionalen Raums identifizieren.

Normalerweise interessiert uns jedoch nicht der gesamte Raum, sondern etwa eine Gerade, eine Ebene oder vielleicht ein Würfel. Die Punkte im Raum, die auf einer Ebene E liegen, stehen in einer ganz bestimmten *Relation* zueinander, etwa

$$E = \{(x, y, z) \in \mathbb{R}^3 \, | \, 2x + 3y - z = 5\} \subseteq \mathbb{R}^3.$$

Ganz abstrakt wollen wir eine beliebige Relation einfach als Teilmenge einer Produktmenge auffassen.

Definition

Unter einer (n–stelligen) Relation R versteht man eine Teilmenge der Produktmenge $A_1 \times A_2 \times \ldots \times A_n$:

$$R \subseteq A_1 \times A_2 \times \ldots \times A_n.$$

Gilt $A_1 = A_2 = \ldots = A_n = A$, so spricht man von einer n–stelligen Relation auf A.

Von besonderer Bedeutung sind 2–stellige Relationen.

Beispiel

$$A_1 = \{\textit{Armin, Rita, Karin, François}\}$$

sei eine Menge von Studierenden und

$$A_2 = \{\textit{Englisch, Französisch, Russisch}\}$$

eine Menge von Fremdsprachen. Die Produktmenge $A_1 \times A_2$ besteht dann aus $4 \cdot 3 = 12$ (daher der Name „Produktmenge“) Elementen der Form (Student, Fremdsprache).

Nehmen wir an, dass Armin Englisch spricht, Rita gar keine Fremdsprache beherrscht, Karin alle drei Fremdsprachen kann und François sich in Englisch und Französisch auskennt. Die Sprachkenntnisse der Studenten lassen sich dann als (zweistellige) Relation $R \subseteq A_1 \times A_2$ dokumentieren:

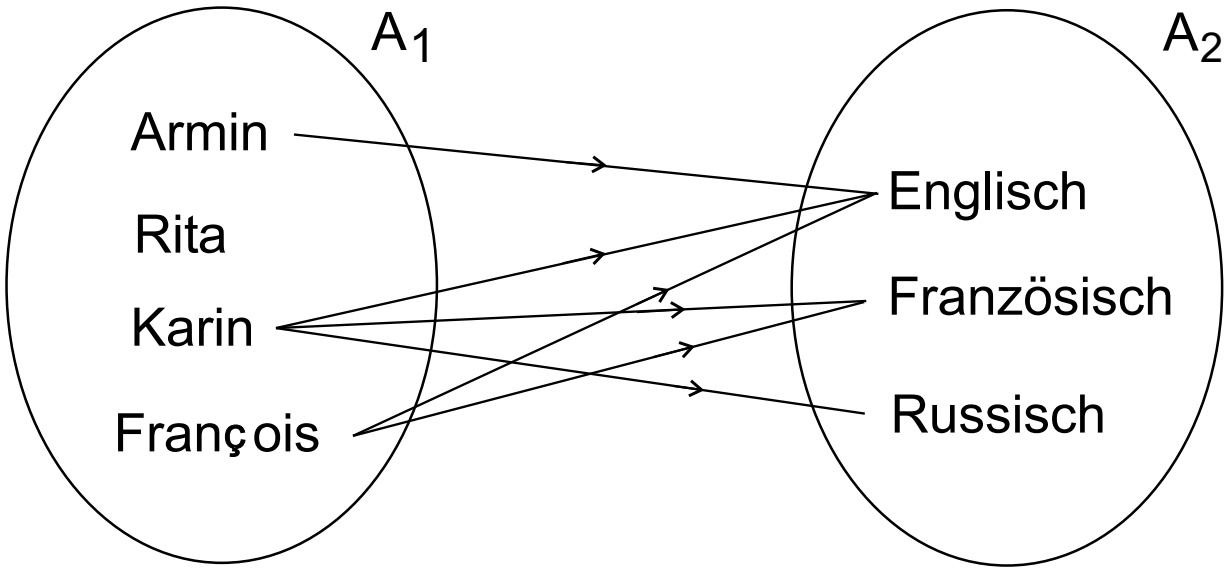
$$\begin{aligned} R = \{&(\textit{Armin,Englisch}), (\textit{Karin,Englisch}), (\textit{Karin,Französisch}), \\ &(\textit{Karin,Russisch}), (\textit{François,Englisch}), (\textit{François,Französisch})\}. \end{aligned}$$

Relationsgraph

Bei zweistelligen Relationen ist eine Veranschaulichung mit Hilfe von Pfeilen in einem Relationsgraphen möglich. Dabei können — anders als bei Funktionen — von einem Element mehrere Pfeile ausgehen (oder gar keine!).

Beispiel

Im vorherigen Beispiel erhalten wir den Relationsgraphen:



Umkehrrelation

Wenn man die Richtung der Pfeile im Relationsgraphen umkehrt, so erhält man übrigens die so genannte *Umkehrrelation*

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}.$$

Falls $R \subseteq A_1 \times A_2$, so ist $R^{-1} \subseteq A_2 \times A_1$.

Beispiel

Im obigen Beispiel erhalten wir nun

$R^{-1} = \{$*(Englisch, Armin), (Englisch, Karin), (Französisch, Karin), (Russisch, Karin), (Englisch, François), (Französisch, François)*$\}$.

Infix–Schreibweise: xRy

Mit (mathematischen) Relationen hat man übrigens schon in der Grundschule zu tun:

Ein Beispiel wäre die „Kleinerrelation“, mit der Zahlen verglichen werden.

Wenn Sie jedoch zwei Zahlen vergleichen, so schreiben Sie kurz „$-3 < 5$“ und nicht etwa in aufgeblähter Form „$(-3, 5) \in$ Kleinerrelation“.

Man nennt diese Schreibweise bei 2–stelligen Relationen Infix–Schreibweise:

Hier wird das Relationszeichen einfach zwischen die beiden Elemente gesetzt. Man sagt „zwischen x und y besteht die Relation R“ oder „x in Relation R zu y“ und schreibt

$$xRy$$

anstelle von $(x, y) \in R$.

Ordnungsrelation

Unter Verwendung dieser Infixschreibweise wollen wir nun einige besondere Typen 2–stelliger Relationen auf einer Menge A kennen lernen:

Definition

Eine Relation R heißt Ordnungsrelation auf einer Menge A, falls für beliebige $x, y, z \in A$ gilt:

Für alle $x \in A : x \, R \, x$. **(Reflexivität)**

Aus $x \, R \, y$ und $y \, R \, x$ folgt $x = y$. **(Antisymmetrie)**

Aus $x \, R \, y$ und $y \, R \, z$ folgt $x \, R \, z$. **(Transitivität)**

Man nennt A dann eine durch die Relation R geordnete Menge.

Beispiel

Die Relation „$\leq$“ ist eine Ordnungsrelation auf der Menge $\mathbb{R}$ der reellen Zahlen, denn es gilt:

- *Für alle $x \in \mathbb{R}$: $x \leq x$ (Reflexivität).*
- *Aus $x \leq y$ und $y \leq x$ folgt $x = y$ für alle $x, y \in \mathbb{R}$ (Antisymmetrie).*
- *Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$ für alle $x, y, z \in \mathbb{R}$ (Transitivität).*

Bei der Ordnungsrelation „$\leq$“ gilt übrigens noch zusätzlich, dass je zwei reelle Zahlen x, y stets “vergleichbar“ sind, d. h. es ist immer $x \leq y$ oder $y \leq x$.

Übung

Zeigen Sie:

Die Inklusionsrelation „$\subseteq$“ ist eine Ordnungsrelation auf der Potenzmenge (=Menge aller Teilmengen) einer Grundmenge G.

Sind je zwei Teilmengen „vergleichbar“?

Lösung

Es gilt für beliebige Teilmengen A, B und C einer Grundmenge G:

- $A \subseteq A$ *(Reflexivität).*
- *Aus $A \subseteq B$ und $B \subseteq A$ folgt $A = B$ (Antisymmetrie).*
- *Aus $A \subseteq B$ und $B \subseteq C$ folgt $A \subseteq C$ (Transitivität).*

Je zwei Teilmengen von G müssen nicht „vergleichbar“ sein, z.B. gilt für die Teilmengen $\{a, b\}$ und $\{b, c\}$ der Grundmenge $\{a, b, c\}$ weder

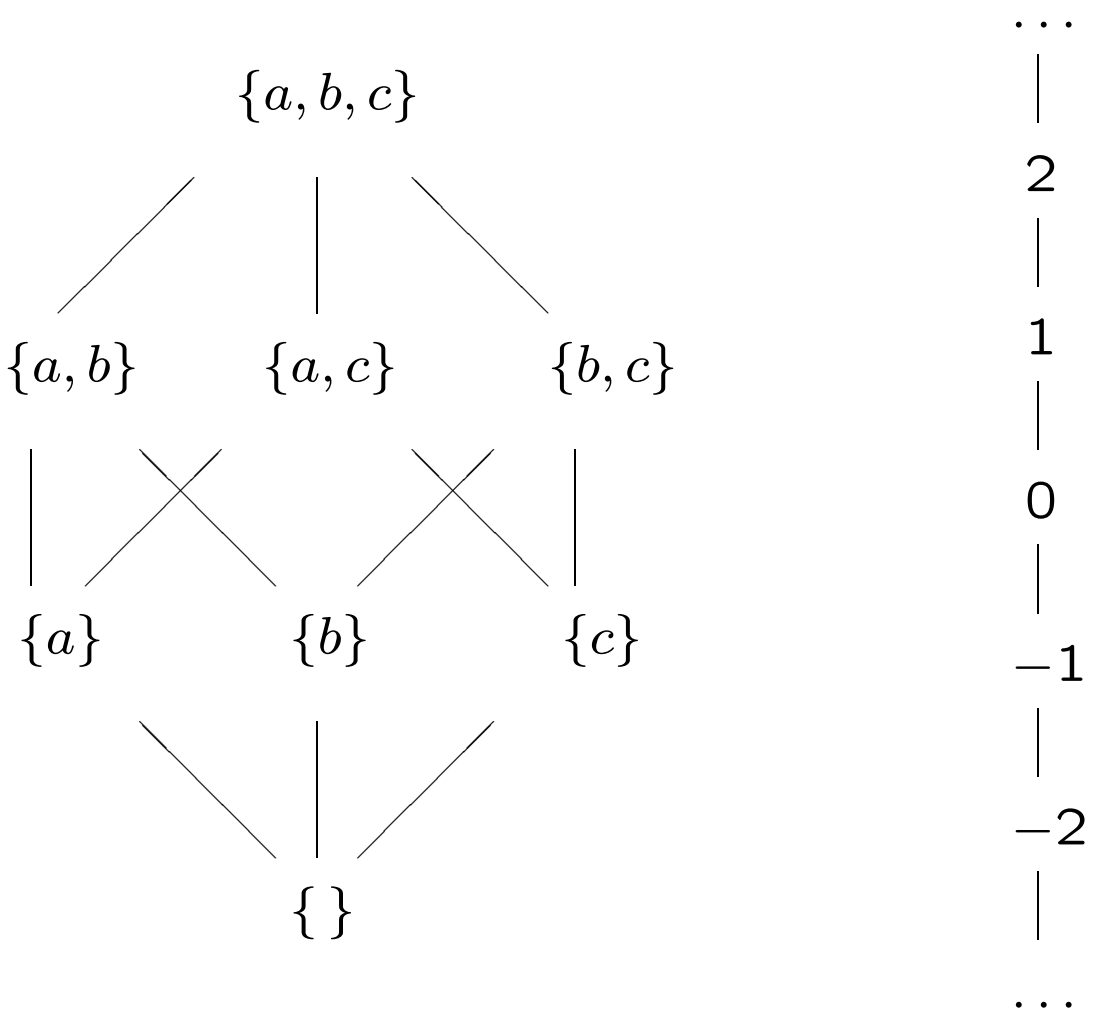
$$\{a, b\} \subseteq \{b, c\}$$

noch

$$\{b, c\} \subseteq \{a, b\}.$$

Unterschied zwischen „$\leq$“ und „$\subseteq$“

Den Unterschied der beiden Ordnungsrelationen „$\leq$“ und „$\subseteq$“ kann man der Abbildung entnehmen:



Lineare Ordnungsrelation

Man nennt eine Ordnungsrelation R *linear* oder *vollständig geordnet*, wenn für alle $x, y \in A$ stets gilt:

$$x\,R\,y \quad \text{oder} \quad y\,R\,x$$

(d.h. wenn je zwei $x, y \in A$ „vergleichbar“ sind).

Die Relation „$<$“ ist übrigens im Gegensatz zu „$\leq$“ keine Ordnungsrelation.

Aber auch für Relationen wie „$<$“ hat man einen Begriff geprägt, nämlich den der „strengen Ordnung“, auf den wir hier nicht näher eingehen wollen.

Äquivalenzrelation

Ein weiterer sehr wichtiger Typ einer 2–stelligen Relation auf einer Menge G ist die so genannte *Äquivalenzrelation*:

Definition

Eine Relation R heißt eine Äquivalenzrelation auf einer Menge A, falls für beliebige $x, y, z \in A$ gilt:

Für alle $x \in A : x \, R \, x$.	**(Reflexivität)**
Aus $x \, R \, y$ folgt $y \, R \, x$.	**(Symmetrie)**
Aus $x \, R \, y$ und $y \, R \, z$ folgt $x \, R \, z$.	**(Transitivität)**

Beispiel

Der Prototyp einer Äquivalenzrelation auf jeder (!) nicht-leeren Menge ist die Gleichheit, denn trivialerweise gilt:

- $x = x$ *für alle* x *(Reflexivität).*
- *Wenn* $x = y$*, dann auch* $y = x$ *(Symmetrie).*
- *Wenn* $x = y$ *und* $y = z$*, dann auch* $x = z$ *(Transitivität).*

Auch bei anderen Beispielen für Äquivalenzrelationen tritt der Begriff „gleich“ auf:

- *„*x *hat die gleiche Größe wie* y*“,*
- *„*x *ist gleichaltrig zu* y*“,*
- x *hat bei Division durch 5 den gleichen Rest wie* y*“ etc.*

Äquivalenzklassen, Repräsentanten

Für jede Äquivalenzrelation auf einer Menge $A \neq \emptyset$ gilt:
A ist die Vereinigung paarweise disjunkter nicht-leerer Äquivalenzklassen. (Man spricht auch von Zerlegung, Klasseneinteilung oder Partition der Menge A).
Jedes Element einer Äquivalenzklasse kann diese repräsentieren. Nimmt man aus jeder Äquivalenzklasse genau einen Repräsentanten, so erhält man ein vollständiges Repräsentanten–System.

Wir fassen also genau die Elemente $x \in A$ zusammen, die zu einem bestimmten $a \in A$ „äquivalent“ sind, nämlich in die Äquivalenzklasse

$$R_a = \{x \in A \mid xRa\}.$$

Das Element a ist dann der (oder besser: ein) Repräsentant von R_a.

Beispiel

In einer Menge von Studierenden

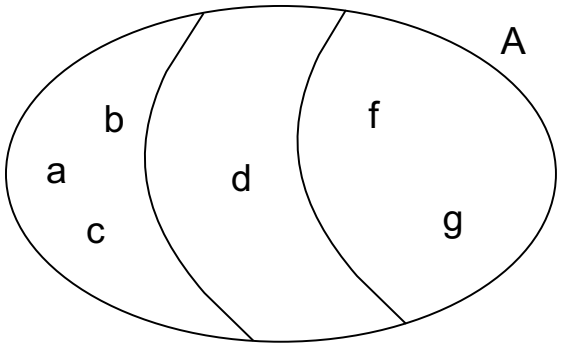
$$A = \{a, b, c, d, e, f\}$$

seien a*,* b *und* c *170 cm groß,* d *habe die Körpergröße 175 cm und* e *und* f *seien beide 180 cm groß. Mit der Äquivalenzrelation* R *(„*x *hat die gleiche Größe wie* y*“) gilt:*

$$R = \{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),$$

$$(c,b),(c,c),(d,d),(e,e),(e,f),(f,e),(f,f)\}.$$

Durch R *wird die Menge* A *in drei Äquivalenzklassen, nämlich* $\{a, b, c\}$*,* $\{d\}$ *und* $\{e, f\}$*, disjunkt zerlegt. Die Äquivalenzklasse* $\{a, b, c\}$ *hat beispielsweise den Repräsentanten* c*:* $R_c = \{a, b, c\}$*. Aber auch* b *wäre ein möglicher Repräsentant dieser Äquivalenzklasse:* $R_b = R_c = \{a, b, c\}$*. Ein vollständiges Repräsentantensystem wäre z.B.* $\{a, d, f\}$*.*



Operation, Verknüpfung

Wenn man zwei reelle Zahlen addiert, so erhält man wiederum eine reelle Zahl; wenn man zwei Teilmengen einer Grundmenge schneidet, so erhält man wiederum eine Teilmenge dieser Grundmenge: Man sagt, die jeweiligen *Operationen* führen nicht aus der Menge selbst heraus, sie sind „abgeschlossen“.

Definition

Unter einer (zweistelligen) Operation bzw. Verknüpfung $*$ auf M versteht man eine Abbildung

$$* : M \times M \to M,$$

die je zwei Elementen $a, b \in M$ eindeutig ein $a * b \in M$ zuordnet.

Wir haben die Operation hier bewusst mit dem Kürzel $*$ abgekürzt, denn $*$ kann vieles bedeuten.

Beispiel

a) Die Addition $+$ und die Multiplikation $\cdot$ sind Operationen auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$.

Dagegen ist die Subtraktion $-$ keine Operation auf $\mathbb{N}$ (etwa $5 - 7 = -2 \notin \mathbb{N}$), wohl aber auf $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$.

Ebenso ist die Division keine Operation auf $\mathbb{N}$ bzw. $\mathbb{Z}$, wohl aber auf $\mathbb{Q}\backslash\{0\}$ und $\mathbb{R}\backslash\{0\}$.
(Beachte: Durch „0“ darf man nicht teilen!)

b) Die aus der Mengenlehre bekannten Verknüpfungen

$$\cap,\ \cup \quad \textit{sowie} \quad \backslash$$

(Schnittmenge, Vereinigungsmenge und Differenzbildung) sind Operationen auf der Potenzmenge einer Grundmenge G.

Übung

Geben Sie die Verknüpfungstafel für die Operation

$$\cup$$

auf der Potenzmenge von $\{a, b\}$ *an!*

Lösung

$\cup$	$\{\ \}$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{\ \}$	$\{\ \}$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a,b\}$	$\{a,b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$

Kommutativ-, Assoziativgesetz und Neutrales Element

Definition

Eine Operation $*$ auf M heißt kommutativ, falls für alle $a, b \in M$ gilt:

$$a * b = b * a \quad \textbf{(Kommutativgesetz).}$$

Definition

Eine Operation $*$ auf M heißt assoziativ, falls für alle $a, b, c \in M$ gilt:

$$a * (b * c) = (a * b) * c \quad \textbf{(Assoziativgesetz).}$$

Definition

Ein $e \in M$ heißt neutrales Element der Operation $*$ auf M, wenn für alle $a \in M$ gilt:

$$a * e = e * a = a.$$

Beispiel

Für die Operation

$$+$$

auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$ ist das Element

$$0$$

neutrales Element.

Übung

Bestimmen Sie das neutrale Element für die Operationen

a) $\cdot$ *auf* $\mathbb{R}$*,*

b) $\cup$ *auf der Potenzmenge einer Grundmenge* G*,*

c) $\cap$ *auf der Potenzmenge einer Grundmenge* G*.*

Lösung

a) Neutrales Element für die Multiplikation auf $\mathbb{R}$ ist die 1*.*

b) Neutrales Element für die Operation $\cup$ auf der Potenzmenge einer Grundmenge G ist die Menge $\{\}$, denn

$$A \cup \{\} = \{\} \cup A = A.$$

c) Neutrales Element für die Operation $\cap$ auf der Potenzmenge einer Grundmenge G ist die Menge G, denn

$$A \cap G = G \cap A = A.$$

Eindeutigkeit des neutralen Elements

Auffällig ist, dass man (wenn überhaupt) nur ein einziges neutrales Element in einer Menge finden kann.

Nehmen wir einmal an, es gäbe zwei neutrale Elemente

$$e \quad \text{und} \quad \tilde{e}.$$

Dann gilt:

$$e = e * \tilde{e} = \tilde{e}.$$

Also müssen die beiden neutralen Elemente gleich sein!

Wir werden daher im Folgenden nur noch von *dem* neutralen Element reden.

Inverses Element

Bei der Addition reeller Zahlen stehen je zwei Elemente a und $-a$ in einer besonderen Beziehung zueinander, denn ihre Summe ergibt gerade das neutrale Element 0 der Addition:

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

Bei der Multiplikation hingegen gilt:

$$a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$$

für alle $a \neq 0$. Man nennt solche Elemente *inverse Elemente* und definiert allgemein:

Definition

In einer Menge M mit einer Operation $*$ und dem neutralen Element e verstehen wir unter dem inversen Element bzw. der Inversen a^{-1} eines Elements $a \in M$ ein Element mit

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

Selbst inverses Element

Wenn a^{-1} inverses Element zu a ist, dann ist natürlich auch a inverses Element zu a^{-1}. Speziell für das neutrale Element gilt:

$$e * e = e,$$

also ist es zu sich *selbst invers*.

Auch das inverse Element a^{-1} eines Elementes a ist eindeutig bestimmt (wie bereits das neutrale Element einer Menge eindeutig feststand).

Gebräuchlich sind die Abkürzungen

$$\begin{aligned} \underbrace{a * a * \ldots * a}_{n-\text{mal}} &= a^n, \\ \underbrace{a^{-1} * a^{-1} * \ldots * a^{-1}}_{n-\text{mal}} &= a^{-n}, \\ a^0 &= e. \end{aligned}$$

Beispiel

a) Für die Operation $+$ auf $\mathbb{Z}$, $\mathbb{Q}$oder $\mathbb{R}$ ist $-a$ das zu a inverse Element.

b) Für die Operation $\cdot$ auf $\mathbb{Q}\backslash\{0\}$ oder $\mathbb{R}\backslash\{0\}$ ist $1/a$ das zu a inverse Element.
(Beachte: Wir müssen hier die „0“ aus der Menge jeweils ausnehmen, denn „$0 \cdot\ ? = 1$“ hat keine Lösung.)

c) Für die Operation $\cdot$ auf $\mathbb{N}$ gibt es nur zu 1 ein inverses Element, nämlich 1 selbst.
Aber „$2 \cdot\ ? = 1$?“
(Beachte: $1/2 \notin \mathbb{N}$.)

Beispiel — Fortsetzung

d) In der Potenzmenge einer Grundmenge G gibt es bei der Operation $\cap$ zu einer echten Teilmenge von G kein inverses Element:

So ist etwa für $G = \{a, b, c\}$ die Gleichung

$$„\{a, b\} \cap \ ? = G“$$

nicht lösbar.
(Beachte: G ist das neutrale Element der Operation $\cap$ auf G.)

e) Bei der Operation $\cup$ gibt es zu keiner nicht–leeren Menge ein inverses Element:

So ist etwa für $G = \{a, b, c\}$ die Gleichung

$$„\{a, b\} \cup \ ? = \emptyset“$$

nicht lösbar.
(Beachte: $\emptyset$ ist das neutrale Element der Operation $\cup$ auf G.)

Übung

Gegeben sei die Verknüpfungstafel

$*$	a	b	c	d
a	c	a	d	b
b	a	b	c	d
c	d	c	b	a
d	b	d	a	c

Gibt es ein neutrales Element?
Gibt es jeweils zueinander inverse Elemente?
Sind Elemente zu sich selbst invers?

Lösung

Das Element b ist neutrales Element.

Die Elemente a und d sind wegen

$$a * d = d * a = b$$

zueinander invers .

Das Element c ist wegen

$$c * c = b$$

zu sich selbst invers .

Ebenso ist das neutrale Element b wegen

$$b * b = b$$

zu sich selbst invers .

Gruppe, Kommutative oder abelsche Gruppe

Definition

Eine Menge G mit einer Verknüpfung $*$, geschrieben $(G, *)$, heißt eine Gruppe, falls die folgenden Eigenschaften erfüllt sind:

- **Abgeschlossenheit der Verknüpfung,**
- **Gültigkeit des Assoziativgesetzes,**
- **Existenz eines neutralen Elements,**
- **Existenz eines inversen Elements zu jedem Element der Menge.**

Die Operation $*$ in einer Gruppe G muss nicht kommutativ sein.

Gilt aber zusätzlich noch das *Kommutativgesetz*, so nennt man die Gruppe *kommutativ* oder (nach dem berühmten Mathematiker Abel) *abelsch*.

Beispiel

a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ *und* $(\mathbb{R}, +)$ *sind kommutative Gruppen mit dem neutralen Element 0 und den zu* a *Inversen* $-a$.

b) $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$ *sind kommutative Gruppen mit dem neutralen Element 1 und den zu* a *Inversen* $1/a$.

Wichtige Gruppeneigenschaften

- Es gibt genau ein neutrales Element.
- Zu jedem Element gibt es genau ein inverses.
- Gleichungen der Form

  $$a * x = b \quad \text{und} \quad y * a = b$$

  (a und b gegeben, x und y unbekannt) sind immer eindeutig lösbar (mit $x = a^{-1} * b$ bzw. $y = b * a^{-1}$).
- Aus $a * b = a * c$ folgt $b = c$, aus $b * a = c * a$ analog $b = c$.
- Man erhält sämtliche Elemente einer endlichen Gruppe genau einmal, wenn man alle mit einem festen Gruppenelement a von links bzw. von rechts multipliziert.

  Daraus folgt, dass in jeder Zeile bzw. jeder Spalte der Verknüpfungstafel einer Gruppe jedes Element genau einmal auftritt.

Beispiel

Gegeben seien die beiden Verknüpfungstafeln

$*$	a	b	c	d
a	c	a	d	b
b	a	b	c	d
c	d	c	b	a
d	b	d	a	c

und

$*$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

Die erste Verknüpfungstafel zeigt eine Gruppe mit b *als neutralem Element,* a *und* d *zueinander inversen Elementen sowie zu sich selbst inversem* c*.*

Auch in der zweiten Tafel wird eine Gruppe beschrieben, die so genannte zyklische Gruppe der Ordnung 4 (d.h. mit vier Elementen der Form a*,* $a^2 = a * a$*,* a^3 *und* $a^4 = e$*). Hier ist* $e = a^4$ *das neutrale Element,* a *und* a^3 *sind zueinander invers,* a^2 *ist zu sich selbst invers. Beide Gruppen sind abelsch.*

In der mathematischen Fachsprache nennt man sie isomorph*. Bis auf Umbenennung sind sie identisch:*

$$a \simeq a,\ b \simeq e,\ c \simeq a^2 \quad \textit{und} \quad d \simeq a^3.$$

Übung

Gegeben sei die Verknüpfungstafel

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

Liegt eine Gruppe vor?

Ist diese Gruppe isomorph (gleich bis auf Umbenennung) zu den beiden Gruppen

$*$	a	b	c	d
a	c	a	d	b
b	a	b	c	d
c	d	c	b	a
d	b	d	a	c

und

$*$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

Lösung

Es liegt eine Gruppe vor mit e als neutralem Element.

Alle Elemente sind zu sich selbst invers, und das Assoziativgesetz prüft man leicht — allerdings mit einigem Aufwand — nach.

Die Gruppe ist sogar kommutativ, was man der Symmetrie zur Diagonalen in der Verknüpfungstafel entnehmen kann.

Da die (isomorphen) Vergleichs-Gruppen im Gegensatz zur hier vorliegenden Gruppe nur zwei Selbstinverse aufweisen (nämlich b und c bzw. $e = a^4$ und a^2), können sie nicht isomorph zur hier untersuchten Gruppe sein.

Die Isomorphie („gleich bis auf Umbenennung“) ist im übrigen eine Äquivalenzrelation auf der Menge aller Gruppen.

Körper

Wir haben immer wieder die uns vertrauten Zahlen $\mathbb{R}$ bzw. $\mathbb{R}\backslash\{0\}$ mit den Operationen $+$ bzw. $\cdot$ als Beispiele für die Begriffe „Operation“, „Assoziativgesetz“, „Gruppe“ etc. verwendet.

Die Grundrechenarten $-$ und $/$ beschreiben dann die inversen Operationen.

Die Operationen $+$ und $\cdot$ stehen jedoch nicht beziehungslos nebeneinander, sondern es gelten die vertrauten *Distributivgesetze*.

In der Mathematik sind nun an vielen Stellen Mengen mit zwei Verknüpfungen $+$ und $\cdot$, die unsere vom Rechnen mit Zahlen gewohnten Rechengesetze erfüllen, von besonderer Bedeutung.

Man hat solchen Gebilden allgemein die Bezeichnung *„Körper“* gegeben.

Körper

Definition

Eine Menge K mit den zwei Operationen $+$ und $\cdot$, geschrieben $(K, +, \cdot)$, heißt Körper, falls gilt:

a) $(K, +)$ **ist eine kommutative Gruppe, die so genannte additive Gruppe, mit dem neutralen Element „0“, genannt Nullelement.**

b) $(K \backslash \{0\}, \cdot)$ **ist ebenfalls eine kommutative Gruppe, die so genannte multiplikative Gruppe, mit dem neutralen Element „1“, genannt Einselement.**

c) Für beliebige $a, b, c \in K$ gelten die Distributivgesetze

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c), \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c). \end{aligned}$$

Beispiel

$$(\mathbb{Q}, +, \cdot) \quad \textit{und} \quad (\mathbb{R}, +, \cdot),$$

d.h. die rationalen bzw. die reellen Zahlen mit den Operationen Addition „+“ und Multiplikation „·“, sind Körper.

Ringe

Im Gegensatz dazu ist etwa $(\mathbb{Z}, +, \cdot)$ kein Körper, denn hier lassen sich keine Inversen bzgl. der Multiplikation bilden. Da auch solche „abgespeckten Körper“ häufiger als Struktur in der Mathematik vorkommen, hat man auch ihnen einen eigenen Namen, nämlich die Bezeichnung *„Ring“*, gegeben:

Definition

Eine Menge R mit den zwei Operationen $+$ und $\cdot$, geschrieben $(R, +, \cdot)$, heißt Ring, falls gilt:

a) $(R, +)$ **ist eine kommutative Gruppe.**

b) Für die Operation $\cdot$ gilt das Assoziativgesetz.

c) Für beliebige $a, b, c \in R$ gelten die Distributivgesetze:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c), \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c). \end{aligned}$$

Beispiel

a) $(\mathbb{Z}, +, \cdot)$ *ist ein kommutativer Ring mit Einselement 1. Von den Körpereigenschaften „fehlen“ letztlich nur die Inversen bzgl. der Multiplikation.*

b) Eine besondere Rolle spielt in der Informatik der Körper mit nur zwei Elementen, nämlich der „0“ und der „1“. Mit ihm kann man binär rechnen*. Die Verknüpfungstafeln lauten:*

$+$	0	1
0	0	1
1	1	0

und

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

Man kann das Rechnen mit „0“ und „1“ auch als Rechnen mit „Resten“ auffassen, nämlich als Rechnen mit den Resten bzgl. der Division durch 2*. Solches Rechnen wird auch „Rechnen modulo 2“ oder „Rechnen mit Restklassen bzgl. 2“ genannt.*

Küchenkräuter in Männermagazinen

Äquivalenzrelationen und andere Relationen kommen durchaus häufig im Alltag vor.

Als Beispiel wollen wir folgenden Artikel „Wer geht mit wem?“ aus Men’s Health betrachten:

Die Relation R, von der in dem Artikel die Rede ist, lautet ganz einfach:

„x kann mit y im gleichen Blumentopf auf der Fensterbank gezüchtet werden“.

Diese Relation ist auf einer Menge von Küchenkräutern K erklärt.

„Kräuterharmonie“ als Relation

$$K = \{Basilikum, Dill, Estragon, Majoran, Minze, Petersilie, Rosmarin, Salbei, Schnittlauch, Thymian\}.$$

Wir können nun die Tabelle aus Men’s Health auch als Relation wie folgt schreiben:

$$R = \{(Basilikum,\ Basilikum), (Basilikum,\ Dill), (Basilikum,\ Majoran),\ \ldots, (Thymian,\ Schnittlauch), (Thymian,\ Thymian)\}.$$

Dabei bedeutet (Basilikum, Basilikum), dass Basilikum und Basilikum im gleichen Topf wachsen, ebenso Basilikum und Dill — ausgedrückt durch das geordnete Paar (Basilikum, Dill).

Da etwa Basilikum und Estragon (laut Tabelle) nicht im Blumentopf harmonieren, gehört (Basilikum, Estragon) nicht zur Relation R.

Relationseigenschaften

Mit den Eigenschaften „Reflexivität“, „Symmetrie“ und „Transitivität“ ist es auch ganz einfach:

- Jedes Küchenkraut gedeiht mit einem Pflänzchen der gleichen Art im Topf („Reflexivität“).
- Wenn Pflänzchen x mit Pflänzchen y im gleichen Topf harmoniert, dann auch y mit x („Symmetrie“).
- Und wenn x mit y wächst und y mit z gedeiht, dann können wir auch beruhigt x und z zusammenpflanzen („Transitivität“).

Und automatisch kommt man auf den Begriff der Äquivalenzklasse: Das sind diejenigen Küchenkräuter zusammengefasst, die miteinander können.

Äquivalenzklassen

In unserem Beispiel gibt es zwei Äquivalenzklassen, nämlich

$$\{Basilikum, Dill, Majoran, Petersilie, \\ Schnittlauch, Thymian\}$$

und

$$\{Estragon, Minze, Rosmarin, Salbei\}.$$

Interessanter ist es vielleicht, eine (2-stellige) Relation R „x kann mit y“ auf der Menge aller Menschen zu betrachten. Bei den Menschen geht es nicht so gesittet zu wie bei den Küchenkräutern:

- Diese Relation ist nämlich keineswegs reflexiv — und davon lebt der Großteil aller im „Psychogewerbe“ Tätigen.
- Die Relation ist auch nicht symmetrisch, aber das wissen diejenigen, die schon einmal unglücklich verliebt waren, ganz genau.
- Transitiv ist die Relation auch nicht — denken Sie an die klassische Schwiegermutter-Konstellation Ehemann, Ehefrau und deren Mutter.

Warum gilt „Minus mal Minus ergibt Plus“?

Warum ergibt Minus mal Minus urplötzlich Plus?

$$(-3) \cdot (-4) = 12$$

Warum ergibt -4 mal -3 etwas Positives, nämlich $+12$? Anschaulich ist das Ganze auf keinen Fall!

In der Schule hatte man nach den natürlichen Zahlen $\mathbb{N}$ die ganzen Zahlen $\mathbb{Z}$ kennengelernt, wobei unter -4 ja so etwas wie Schulden auf der Bank vorstellbar waren, aber die Multiplikationsregeln wie

Minus	mal	Plus	ergibt	Minus
Plus	mal	Minus	ergibt	Minus
Minus	mal	Minus	ergibt	Plus

wirkten irgendwie erfunden. Vielleicht könnte etwas ganz anderes gelten?

Dass dies *nicht* der Fall sein kann, lehrt uns die Algebra. $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Einselement:

0 ist das neutrale Element der Addition, $(-a)$ ist das zu a inverse Element der Addition, 1 ist das neutrale Element bzgl. Multiplikation usw.

Rechengesetze in Ringen

Man kann nun in Ringen einige Rechengesetze zeigen, die immer gelten müssen, beispielsweise

$$0 \cdot a = 0.$$

Dies erscheint uns trivial, da wir an das Rechnen mit reellen Zahlen gewohnt sind. Dahinter steckt aber etwas viel Allgemeineres:

In jedem Ring ergibt die Multiplikation des neutralen Elements bzgl. Addition mit einem beliebigen Element aus dem Ring wiederum das neutrale Element bzgl. Addition. Man kann dies ganz allgemein (d.h. nur unter Kenntnis der Rechengesetze in Ringen, ohne zu wissen, in welchem speziellen Ring man rechnet) nachweisen.

Wir wollen hier zunächst beweisen, dass Minus mal Plus Minus ergibt. In der Terminologie von Ringen ausgedrückt:

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

Dazu ist zu zeigen, dass $(-a) \cdot b$ *das inverse Element bzgl. Addition zu* $(a \cdot b)$ ist.

„Minus mal Minus ergibt Plus“!

Wir formen also $(-a) \cdot b + (a \cdot b)$ um, bis wir 0 als Ergebnis erhalten:

$$\begin{aligned} (-a) \cdot b + a \cdot b &= [(-a) + a] \cdot b \\ &= 0 \cdot b \\ &= 0. \end{aligned}$$

Hinter der Umformung der ersten Zeile steckt das Distributivgesetz, in der zweiten Zeile wurde ausgenutzt, dass a und $(-a)$ invers zueinander bzgl. Addition sind, und zur dritten Zeile wurde $0 \cdot b = 0$ verwendet.

Jetzt kann man analog „Minus mal Minus ergibt Plus“ zeigen. Wie oben erhalten wir:

$$\begin{aligned} (-a) \cdot b + (-a) \cdot (-b) &= (-a) \cdot [b + (-b)] \\ &= (-a) \cdot 0 \\ &= 0. \end{aligned}$$

Also ist $(-a) \cdot (-b)$ invers zu $(-a) \cdot b$, Letzteres war invers zu $(a \cdot b)$.

Da Inverse eindeutig sind, muss $(-a) \cdot (-b)$ gleich $(a \cdot b)$ sein. Also: „Minus mal Minus ergibt Plus“!

Restklassen modulo 5

Wir wollen im Folgenden mit Resten rechnen, so wie sie beim Dividieren von natürlichen Zahlen durch andere natürliche Zahlen entstehen:

Beispielsweise fallen bei der Division durch 5 die möglichen Reste 0, 1, 2, 3 und 4 an. Wir können sogar eine Äquivalenzrelation erklären

„x hat bei Division durch 5 denselben Rest wie y“

und erreichen damit eine Einteilung aller natürlichen Zahlen in Äquivalenzklassen, nämlich die Zahlen, die bei Division durch 5 den Rest 0 haben, die Zahlen, die bei Division durch 5 den Rest 1 haben, etc.

Wir wollen diese so genannten Restklassen modulo 5 mit $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ und $\overline{4}$ bezeichnen und erhalten:

$$\begin{aligned}
\overline{0} &= \{0, 5, 10, 15, 20, ...\},\\
\overline{1} &= \{1, 6, 11, 16, 21, ...\},\\
\overline{2} &= \{2, 7, 12, 17, 22, ...\},\\
\overline{3} &= \{3, 8, 13, 18, 23, ...\},\\
\overline{4} &= \{4, 9, 14, 19, 24, ...\}.
\end{aligned}$$

Restklassen

Die Zahlen 0, 1, 2, 3 und 4 sind ein vollständiges Repräsentanten-System dieser Restklassen — daher auch die Bezeichnungen $\overline{0}$, $\overline{1}$ etc. für die Restklassen.

Man könnte aber natürlich auch genauso gut in diesem Zusammenhang 10, 21, 2, 18 und 109 wählen:

$\overline{10} = \overline{0}$, $\overline{21} = \overline{1}$, denn etwa 10 und 0 sowie 21 und 1 sind in derselben Restklasse.

Man kann nun nicht nur alle natürlichen Zahlen $\mathbb{N}$, sondern sogar alle ganzen Zahlen $\mathbb{Z}$ in derartige Restklassen einteilen.

Es ist leicht ersichtlich, dass z.B. alle Zahlen in der Restklasse $\overline{2}$ ausgehend von 2 selbst durch Addition von Vielfachen von 5 entstehen:

$$2 + 5 = 7,\ 2 + 10 = 12,\ 2 + 15 = 17 \text{ etc.}$$

Restklassen modulo 5 von $\mathbb{Z}$

Man könnte natürlich auch solche Vielfache von 5 subtrahieren ($2-5=-3$, $2-10=-8$ etc.) und würde damit alle ganzen Zahlen $\mathbb{Z}$ in Restklassen modulo 5 einteilen:

$$\begin{aligned}
\overline{0} &= \{...,-15,-10,-5,\ 0,5,10,15,20,...\},\\
\overline{1} &= \{...,-14,-9,-4,\ 1,6,11,16,21,...\},\\
\overline{2} &= \{...,-13,-8,-3,\ 2,7,12,17,22,...\},\\
\overline{3} &= \{...,-12,-7,-2,\ 3,8,13,18,23,...\},\\
\overline{4} &= \{...,-11,-6,-1,\ 4,9,14,19,24,...\}.
\end{aligned}$$

Man verwendet in der Mathematik häufig für die Relation

„x hat bei Division durch 5 denselben Rest wie y“

oder

„$x-y$ ist durch 5 teilbar“

eine andere Sprechweise und sagt:

„x und y sind kongruent modulo 5“.

Die Menge aller Restklassen modulo 5 bezeichnet man mit $\mathbb{Z}/[5] := \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$.

Restklassen-Arithmetik

Natürlich ist die Zahl 5 in keiner Weise etwas Besonderes: Ebenso könnte man irgendeine natürliche Zahl $n > 1$ nehmen, die Äquivalenzrelation

„x und y sind kongruent modulo n“

betrachten und erhielte dann insgesamt n Restklassen

$$\mathbb{Z}/[n] = \{\overline{0},\ \overline{1},\ \overline{2},\ \ldots,\ \overline{n-2},\ \overline{n-1}\}.$$

Interessant ist nun insbesondere, dass man mit derartigen Restklassen sogar rechnen kann! Dazu definieren wir:

$$\overline{a} \oplus \overline{b} = \overline{a+b}.$$

Was ist damit gemeint? Ganz einfach:

Man addiert zwei Restklassen, indem man die Repräsentanten ganz gewöhnlich (wie Zahlen) addiert und dann (durch Modulo-Rechnen) die zugehörige Restklasse ermittelt.

Im Beispiel modulo 5:

$$\overline{4} \oplus \overline{3} = \overline{4+3} = \overline{7} = \overline{2}.$$

Restklassen-Arithmetik

Das Ganze funktioniert, da man anstelle von 4 und 3 auch beliebige andere Repräsentanten der jeweiligen Restklassen nehmen könnte:

Beispielsweise 24 anstelle von 4 (wegen $\overline{4} = \overline{24}$) und -7 anstelle von 3 (wegen $\overline{3} = \overline{-7}$).

Es ergibt sich damit:

$$\overline{24} \oplus \overline{-7} = \overline{24 - 7} = \overline{17} = \overline{2}.$$

Man kann dies allgemein zeigen:

Die Definition

$$\overline{a} \oplus \overline{b} = \overline{a + b}.$$

ist unabhängig davon, welche Zahl man als Repräsentanten einer Äquivalenzklasse nimmt.

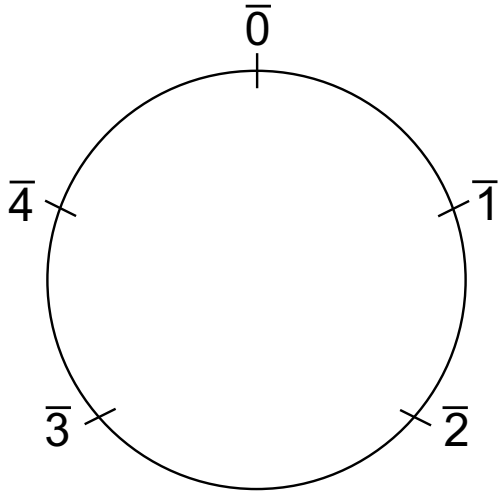
Modulo-Arithmetik mittels Uhr

Die Restklassen-Addition kann man sich auch an einer Uhr veranschaulichen — allerdings an einer ungewöhnlichen Uhr mit genau 5 Einteilungen.

Wenn man z.B. $\overline{4}$ und $\overline{3}$ addiert, so würde man zunächst auf die Einteilung $\overline{4}$ der Uhr gehen und dann im Uhrzeigersinn 3 Einheiten weiterrücken.

Man könnte aber auch, startend bei $\overline{0}$ (neutrales Element!), 24 Einheiten im Uhrzeigersinn und 7 im Gegenuhrzeigersinn rücken — wieder käme man bei $\overline{24} \oplus \overline{-7} = \overline{2}$ an.

Dies liegt, wie bereits bemerkt, daran, dass die Definition der Restklassenaddition unabhängig von den Repräsentanten der Restklassen ist.



Modulo-Arithmetik

Die Verknüpfungstafel für die (Restklassen-) Addition für die Restklassen $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ und $\overline{4}$ hat insgesamt die folgende Gestalt:

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Hier liegt eine (zyklische) Gruppe vor: $\overline{0}$ ist das neutrale Element, jeweils $\overline{1}$ und $\overline{4}$ sowie $\overline{2}$ und $\overline{3}$ sind zueinander invers.

Man erhält beispielsweise alle Restklassen, indem man sukzessive $\overline{1}$ auf ein beliebiges Element, etwa $\overline{1}$, addiert:

$$\overline{1} \oplus \overline{1} = \overline{2},\ \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{3},\ \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{4}$$

und schließlich

$$\overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{0}.$$

Restklassen-Multiplikation

Analog zur Restklassen-Addition lässt sich eine Restklassen-Multiplikation definieren:

$$\overline{a} \otimes \overline{b} = \overline{a \cdot b}.$$

Im Beispiel modulo 5 etwa: $\overline{2} \otimes \overline{3} = \overline{2 \cdot 3} = \overline{6} = \overline{1}$. Die gesamte Verknüpfungstafel hat dann die Gestalt:

$\otimes$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Gemäß Verknüpfungstafel gilt: $\overline{1}$ ist neutrales Element: $\overline{1} \otimes \overline{a} = \overline{1 \cdot a} = \overline{a}$. Wegen $\overline{2} \otimes \overline{3} = \overline{1}$ sind $\overline{2}$ und $\overline{3}$ zueinander inverse Elemente.

Insgesamt liegt auch eine multiplikative Gruppe vor und — da die Distributivgesetze gelten — ist

$$(\mathbb{Z}/[5], \oplus, \otimes)$$

ein Körper.

Restklassen modulo 6

Wir wollen uns im Folgenden auch einmal die Verknüpfungstafeln für Restklassen bzgl. eines anderen n (etwa für $n = 6$) ansehen:

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\otimes$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Wenn man diese Verknüpfungstafeln studiert, so fällt zunächst bei der Restklassen-Addition $\oplus$ nichts auf. Wieder liegt eine zyklische Gruppe vor.

Interessant wird es erst bei der Restklassen-Multiplikation! Das neutrale Element der Multiplikation ist $\overline{1}$, aber gewisse inverse Elemente fehlen.

Restklassen modulo 6

Wenn man sich die Zeile (oder Spalte) von $\overline{2}$ ansieht, so ist in dieser Zeile (oder Spalte) kein $\overline{1}$ zu entdecken — mit anderen Worten:

Die Gleichung „$\overline{2} \otimes \overline{?} = \overline{1}$“ hat keine Lösung. Also gibt es kein inverses Element zu $\overline{2}$. Man hat in diesem Fall keinen Körper, sondern nur einen kommutativen Ring mit Einselement vorliegen.

In der Tabelle bzgl. der Restklassen-Multiplikation modulo 6 findet man ein weiteres ungewohntes Phänomen:

$$\overline{2} \otimes \overline{3} = \overline{0}.$$

Man sagt auch, dass $\overline{2}$ und $\overline{3}$ *Nullteiler* sind. Von den reellen Zahlen her ist uns derartiges nicht geläufig.

Derartige Nullteiler können nicht in Körpern, wohl aber in Ringen vorkommen.