Lineare Algebra für Informatiker · Wintersemester 2026/27

Tutoriumsblatt 4

Halbgruppen, Monoide, Gruppen, Körper

Ausführliche Erklärungen zu den Tutoriumsaufgaben

Mirkan Deniz Günkaya, Tutor

Wozu dieses Skript da ist

Dieses Skript habe ich für euch zum Selbststudium geschrieben. Es ist kein offizielles Material der Vorlesung und ersetzt nicht die Musterlösung von Herrn Dr. Gerkmann. Verbindlich ist das, was in der Vorlesung und in Moodle steht.

Ich erkläre hier die drei Tutoriumsaufgaben von Blatt 4 so ausführlich, dass ihr sie auch ohne das Tutorium nachvollziehen könnt: mit Bildern, Beispielen, Gegenbeispielen und den Fehlern, die ich am häufigsten sehe. Ihr dürft das Skript gern an Kommilitonen weitergeben. Wenn ihr einen Fehler findet, sagt mir bitte Bescheid.

Inhaltsverzeichnis

1 Werkzeugkasten **3**

1.1 Was ist eine Verknüpfung? . . . 3
1.2 Die Treppe: Halbgruppe, Monoid, Gruppe . . . 4
1.3 Beispiele für jede Stufe . . . 5
1.4 Verknüpfungstafeln lesen . . . 6
1.5 Drei Tatsachen, die wir ständig brauchen . . . 6
1.6 Körper . . . 7
1.7 Rezepte . . . 8

2 Aufgabe 1: Vereinigung und Durchschnitt **9**

2.1 Worum geht es? . . . 9
2.2 Ein Beispiel zum Anfassen: $M = \{1, 2\}$ . . . 9
2.3 Teil (a): Beide sind Monoide . . . 10
2.4 Teil (b): Der Fall $M = \varnothing$ . . . 11
2.5 Teil (c): Der Fall $M \neq \varnothing$ . . . 12
2.6 Etwas mehr: Welche Elemente sind überhaupt invertierbar? . . . 13

3 Aufgabe 2: Rechnen in einem beliebigen Monoid **14**

3.1 Worum geht es? . . . 14

3.2 Teil (a): Links- und Rechtsinverses . . . 14

3.3 Reicht nicht auch eine Seite? Ein Gegenbeispiel . . . 15

3.4 Teil (b): Wenn jedes Element sein eigenes Inverses ist . . . 16

3.4.1 Ein zweiter Weg ohne die Formel aus der Vorlesung . . . 17

4 Aufgabe 3: Der Körper mit drei Elementen **19**

4.1 Worum geht es? . . . 19

4.2 Die Additionstafel . . . 19

4.2.1 Dasselbe mit der Sudoku-Regel . . . 20

4.3 Die Multiplikationstafel . . . 21

4.4 Das Ergebnis . . . 22

4.5 Kontrolle: Rechnen modulo 3 . . . 22

4.6 Was haben wir bewiesen und was nicht? . . . 23

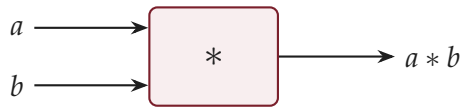
5 Überblick **24**

6 Selbsttest **24**

1 Werkzeugkasten

Bevor wir die Aufgaben lösen, klären wir die Begriffe. Blatt 4 hat viele neue Wörter, aber sie bauen alle aufeinander auf. Wer die Treppe in Abschnitt 1.2 verstanden hat, hat das halbe Blatt verstanden.

1.1 Was ist eine Verknüpfung?



zwei Elemente aus A wieder ein Element aus A

Eine Verknüpfung ist eine Maschine mit zwei Eingängen und einem Ausgang. Man steckt zwei Elemente einer Menge A hinein und bekommt ein Element derselben Menge heraus.

Verknüpfung

Eine Verknüpfung auf einer Menge A ist eine Abbildung

$$*\colon A \times A \to A, \qquad (a, b) \mapsto a * b.$$

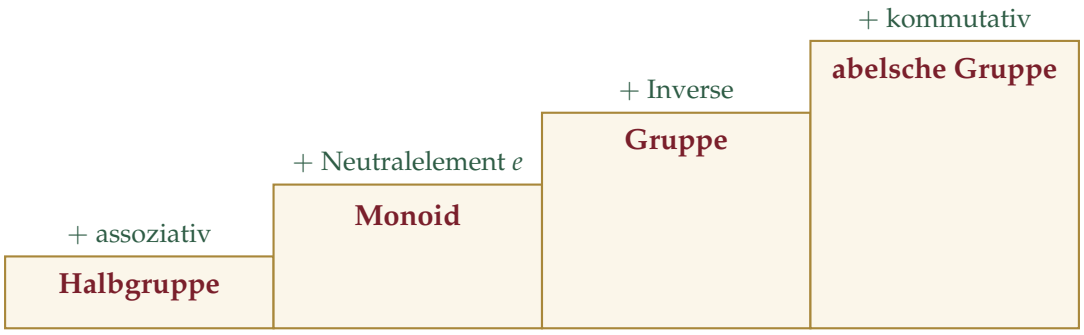
Der wichtige Teil der Definition ist das A ganz rechts. Das Ergebnis muss wieder in A liegen.

Menge	Rechenvorschrift	Verknüpfung?	Begründung
$\mathbb{N}$	$a + b$	ja	Summe natürlicher Zahlen ist natürlich
$\mathbb{N}$	$a - b$	nein	$3 - 5 = -2 \notin \mathbb{N}$
$\mathbb{Z}$	$a - b$	ja	Differenz ganzer Zahlen ist ganz
$\mathbb{Z}$	$a : b$	nein	$1 : 2 \notin \mathbb{Z}$, und $1 : 0$ gibt es gar nicht
$\mathcal{P}(M)$	$A \cup B$	ja	aus $A, B \subseteq M$ folgt $A \cup B \subseteq M$

Für Informatiker

In Java wäre eine Verknüpfung auf einem Typ `T` eine Methode mit der Signatur `T op(T a, T b)`. Zwei Werte vom Typ `T` gehen hinein, ein Wert vom Typ `T` kommt heraus. Die Division auf `int` passt nicht in dieses Schema, weil sie bei `b == 0` eine Ausnahme wirft und kein Ergebnis liefert.

1.2 Die Treppe: Halbgruppe, Monoid, Gruppe



Start: Menge A mit einer Verknüpfung $*\colon A \times A \to A$

Jede Stufe verlangt eine Eigenschaft mehr als die vorige. Wer auf einer höheren Stufe steht, erfüllt automatisch alles, was die unteren Stufen verlangen. Jede Gruppe ist also ein Monoid, und jedes Monoid ist eine Halbgruppe.

Halbgruppe, Monoid, Gruppe

Sei $*$ eine Verknüpfung auf einer Menge A.

- $(A, *)$ heißt **Halbgruppe**, wenn $*$ assoziativ ist:

$$(a * b) * c = a * (b * c) \quad \text{für alle } a, b, c \in A.$$

- Eine Halbgruppe heißt **Monoid**, wenn es ein **Neutralelement** $e \in A$ gibt:

$$e * a = a \quad \text{und} \quad a * e = a \quad \text{für alle } a \in A.$$

- Ein Element a eines Monoids heißt **invertierbar**, wenn es ein $b \in A$ gibt mit

$$a * b = e \quad \text{und} \quad b * a = e.$$

  Dieses b heißt das Inverse von a und wird mit a^{-1} bezeichnet.
- Ein Monoid heißt **Gruppe**, wenn jedes Element invertierbar ist.
- Eine Halbgruppe, ein Monoid oder eine Gruppe heißt **kommutativ** (bei Gruppen auch **abelsch**), wenn $a * b = b * a$ für alle $a, b \in A$ gilt.

Was bedeuten die drei Eigenschaften anschaulich?

Assoziativ heißt: Bei drei Elementen in einer Reihe ist es egal, welche beiden man zuerst verknüpft. Deshalb darf man bei $a * b * c$ die Klammern weglassen. Die Reihenfolge der Elemente darf man dabei nicht ändern. Das wäre Kommutativität, und die ist eine andere Eigenschaft.

Neutralelement heißt: Es gibt ein Element, das beim Verknüpfen nichts verändert. Bei der Addition ist das die 0, bei der Multiplikation die 1.

Invertierbar heißt: Man kann die Wirkung von a rückgängig machen und landet wieder beim Neutralelement. Bei der Addition in $\mathbb{Z}$ macht $-a$ das a rückgängig.

Zwei Dinge, auf die ihr achten müsst

Beide Seiten. Beim Neutralelement und beim Inversen stehen jeweils zwei Gleichungen. Solange ihr nicht wisst, dass die Verknüpfung kommutativ ist, müsst ihr beide prüfen.

Die Reihenfolge der Quantoren. Das kennt ihr von Blatt 2. Beim Neutralelement gibt es *ein e*, das für *alle a* funktioniert. Beim Inversen bekommt *jedes a* sein *eigenes b*.

neutral: $\exists e\, \forall a\colon\ e * a = a = a * e$ Gruppe: $\forall a\, \exists b\colon\ a * b = e = b * a$

1.3 Beispiele für jede Stufe

	assoziativ	neutral	invertierbar sind	Stufe
$(\mathbb{Z}, -)$	nein			keine Halbgruppe
$(\mathbb{N}, +)$	ja	keins		Halbgruppe
$(\mathbb{N}_0, +)$	ja	0	nur 0	Monoid
$(\mathbb{Z}, +)$	ja	0	alle, $a^{-1} = -a$	abelsche Gruppe
$(\mathbb{Z}, \cdot)$	ja	1	nur 1 und -1	Monoid
$(\mathbb{Q}, \cdot)$	ja	1	alle außer 0	Monoid
$(\mathbb{Q} \setminus \{0\}, \cdot)$	ja	1	alle, $a^{-1} = \frac{1}{a}$	abelsche Gruppe

Zu drei Zeilen ein paar Worte.

$(\mathbb{Z}, -)$ ist nicht assoziativ: $(5 - 3) - 1 = 1$, aber $5 - (3 - 1) = 3$.

$(\mathbb{N}, +)$ hat kein Neutralelement, weil $\mathbb{N}$ bei uns mit 1 beginnt. Nimmt man die 0 dazu, wird aus der Halbgruppe ein Monoid. Eine Gruppe ist $(\mathbb{N}_0, +)$ trotzdem nicht: Es gibt kein $b \in \mathbb{N}_0$ mit $3 + b = 0$.

$(\mathbb{Q}, \cdot)$ scheitert nur an einem einzigen Element. Die 0 hat kein Inverses, weil $0 \cdot b = 0 \neq 1$ für jedes b gilt. Nimmt man die 0 heraus, erhält man eine Gruppe. Dieser Gedanke kommt beim Körper wieder.

Für Informatiker: zwei Beispiele aus dem Alltag

Strings mit Konkatenation. Die Menge aller Strings mit der Verknüpfung „hintereinanderhängen“ ist ein Monoid. Die Verknüpfung ist assoziativ, und der leere String ist das Neutralelement. Eine Gruppe ist es nicht: Einen nichtleeren String kann man durch Anhängen nie wieder leer machen. Kommutativ ist es auch nicht, denn `ab` und `ba` sind verschiedene Strings.

Bits mit XOR. Die Menge $\{0, 1\}$ mit XOR ist eine abelsche Gruppe. Das Neutralelement ist 0, und jedes Bit ist sein eigenes Inverses, denn $0 \oplus 0 = 0$ und $1 \oplus 1 = 0$. Dieses Beispiel begegnet uns in Aufgabe 2(b) wieder.

1.4 Verknüpfungstafeln lesen

Bei einer endlichen Menge kann man eine Verknüpfung vollständig in eine Tabelle schreiben. In der Zeile von x und der Spalte von y steht $x * y$. Hier sind die Tafeln für XOR und AND auf $\{0,1\}$:

$\oplus$	0	1
0	0	1
1	1	0

$\wedge$	0	1
0	0	0
1	0	1

An einer Tafel kann man viel ablesen:

So liest man eine Verknüpfungstafel

- **Neutralelement e:** Die Zeile von e und die Spalte von e wiederholen einfach die Kopfzeile.
- **Kommutativ:** Die Tafel ist symmetrisch zur Diagonalen von links oben nach rechts unten.
- **a ist invertierbar:** In der Zeile von a steht irgendwo e, etwa in der Spalte von b. Und in der Zeile von b steht e in der Spalte von a.
- **Assoziativität** sieht man einer Tafel leider nicht an. Die muss man nachrechnen oder wissen.

Für die beiden Tafeln oben heißt das: Bei XOR ist 0 neutral, die Tafel ist symmetrisch, und in jeder Zeile steht eine 0. Jedes Element ist invertierbar. Bei AND ist 1 neutral. In der Zeile von 0 steht aber keine 1. Die 0 ist nicht invertierbar, und $(\{0,1\}, \wedge)$ ist nur ein Monoid.

1.5 Drei Tatsachen, die wir ständig brauchen

Eindeutigkeit und Kürzungsregel

1. In einem Monoid gibt es **nur ein** Neutralelement.
2. Ein invertierbares Element hat **nur ein** Inverses.
3. In einer Gruppe gilt die **Kürzungsregel**: Aus $a * x = a * y$ folgt $x = y$. Ebenso folgt aus $x * a = y * a$, dass $x = y$ ist.

Die Beweise sind kurz, und es lohnt sich, sie einmal gesehen zu haben.

Zu 1. Sind e und e' beide neutral, dann ist $e = e * e' = e'$. Das erste Gleichheitszeichen gilt, weil e' neutral ist, das zweite, weil e neutral ist.

Zu 2. Sind b und c beide Inverse von a, dann ist

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

Merkt euch diese Rechnung. Aufgabe 2(a) benutzt denselben Trick.

Zu 3. Verknüpft man beide Seiten von $a * x = a * y$ von links mit a^{-1}, erhält man $a^{-1} * a * x = a^{-1} * a * y$, also $e * x = e * y$ und damit $x = y$.

Aus der Kürzungsregel folgt eine Eigenschaft, die man an jeder Gruppentafel sieht:

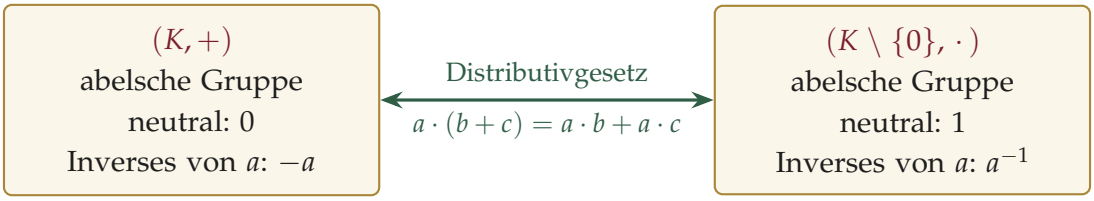
Sudoku-Regel

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

Warum? Stünde in der Zeile von a dasselbe Element in zwei verschiedenen Spalten x und y, dann wäre $a * x = a * y$ und nach der Kürzungsregel $x = y$. Das wären also gar keine verschiedenen Spalten. Und jedes Element b kommt in der Zeile von a auch wirklich vor, nämlich in der Spalte $x = a^{-1} * b$, denn $a * (a^{-1} * b) = b$.

Die XOR-Tafel erfüllt die Sudoku-Regel. Die AND-Tafel nicht: In der Zeile von 0 steht zweimal die 0. Daran erkennt man sofort, dass AND keine Gruppe liefert.

1.6 Körper



Ein Körper ist eine Menge mit *zwei* Verknüpfungen, in der man so rechnen kann, wie ihr es von den rationalen oder reellen Zahlen gewohnt seid: addieren, subtrahieren, multiplizieren und durch alles außer null dividieren.

Körper

Eine Menge K mit zwei Verknüpfungen $+$ und $\cdot$ heißt Körper, wenn gilt:

- $(K, +)$ ist eine abelsche Gruppe. Das Neutralelement heißt 0 (Nullelement), das Inverse von a heißt $-a$ (das Negative von a).
- Die Multiplikation ist assoziativ und kommutativ. Es gibt ein Neutralelement 1 (Einselement) mit $1 \neq 0$, und jedes $a \neq 0$ hat ein Inverses a^{-1}.
- Es gilt das Distributivgesetz: $a \cdot (b + c) = a \cdot b + a \cdot c$ für alle $a, b, c \in K$.

Die genaue Formulierung im Skript kann etwas anders aussehen. Inhaltlich ist es dasselbe. Haltet euch in der Klausur an die Formulierung aus der Vorlesung.

Das Bild oben zeigt die Struktur: zwei abelsche Gruppen auf derselben Menge. Die Null gehört zur multiplikativen Gruppe nicht dazu. Das Distributivgesetz ist die einzige Regel, in der beide Verknüpfungen gleichzeitig vorkommen. Wenn ihr eine Aussage beweisen wollt, die Plus und Mal verbindet, muss das Distributivgesetz im Beweis auftauchen.

Beispiele für Körper sind $\mathbb{Q}$ und $\mathbb{R}$. Kein Körper ist $\mathbb{Z}$, denn die 2 hat in $\mathbb{Z}$ kein multiplikatives Inverses.

Zwei Rechenregeln in jedem Körper

1. $c \cdot 0 = 0$ für jedes $c \in K$.
2. Sind $x \neq 0$ und $y \neq 0$, dann ist auch $x \cdot y \neq 0$.

Beide Regeln sind keine Axiome. Sie folgen aus den Axiomen. Die erste beweisen wir in Aufgabe 3. Die zweite geht so: Angenommen, $x \cdot y = 0$ und $x \neq 0$. Dann ist

$$y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0.$$

Ist ein Produkt null und ein Faktor nicht, dann muss also der andere Faktor null sein.

Für Informatiker: der kleinste Körper

Der kleinste Körper hat nur zwei Elemente, 0 und 1. Die Addition ist dort XOR, die Multiplikation ist AND. Das sind genau die beiden Tafeln aus Abschnitt 1.4. Jedes Bit eures Rechners ist ein Element dieses Körpers. In Aufgabe 3 bauen wir den nächstgrößeren Körper, den mit drei Elementen.

1.7 Rezepte

Wie zeigt man . . . ?

. . . dass $(A, *)$ ein Monoid ist?

1. Das Ergebnis $a * b$ liegt wieder in A.
2. $*$ ist assoziativ.
3. Ein Neutralelement e konkret angeben, prüfen, dass $e \in A$ liegt, und beide Gleichungen $e * a = a$ und $a * e = a$ nachrechnen.

. . . dass ein Monoid eine Gruppe ist? Für ein beliebiges a ein Inverses angeben und beide Gleichungen prüfen.

. . . dass ein Monoid keine Gruppe ist? *Ein* Element angeben, das nicht invertierbar ist. Dafür muss man begründen, dass *kein* Element als Inverses in Frage kommt.

Der letzte Punkt folgt aus der Verneinung von Quantoren. „Gruppe“ heißt $\forall a\ \exists b\colon a * b = e = b * a$. Die Verneinung ist $\exists a\ \forall b\colon \neg(a * b = e = b * a)$. Man braucht ein schlechtes a, muss dann aber alle b ausschließen.

2 Aufgabe 1: Vereinigung und Durchschnitt

Aufgabe 1

Sei M eine Menge. Wir betrachten auf $\mathcal{P}(M)$ die beiden Verknüpfungen $(A, B) \mapsto A \cup B$ und $(A, B) \mapsto A \cap B$. Als bekannt darf vorausgesetzt werden, dass diese beiden Verknüpfungen assoziativ sind.

(a) Zeigen Sie, dass $(\mathcal{P}(M), \cup)$ und $(\mathcal{P}(M), \cap)$ Monoide sind, und geben Sie für beide Monoide jeweils das Neutralelement an.

(b) Weisen Sie nach, dass die beiden Monoide im Fall $M = \varnothing$ jeweils Gruppen sind.

(c) Zeigen Sie, dass im Fall $M \neq \varnothing$ keines der beiden Monoide eine Gruppe ist.

2.1 Worum geht es?

Die Elemente, mit denen hier gerechnet wird, sind keine Zahlen. Es sind *Mengen*, genauer die Teilmengen einer festen Menge M. Die Potenzmenge $\mathcal{P}(M)$ ist die Menge aller Teilmengen von M. Zwei Teilmengen werden verknüpft, indem man sie vereinigt oder schneidet.

Bevor wir etwas beweisen, schauen wir uns ein Beispiel an. Das ist bei abstrakten Aufgaben fast immer der beste Anfang.

2.2 Ein Beispiel zum Anfassen: $M = \{1, 2\}$

Für $M = \{1, 2\}$ ist $\mathcal{P}(M) = \{\varnothing, \{1\}, \{2\}, M\}$. Das sind vier Elemente, also können wir beide Verknüpfungstafeln vollständig aufschreiben:

$\cup$	$\varnothing$	$\{1\}$	$\{2\}$	M
$\varnothing$	$\varnothing$	$\{1\}$	$\{2\}$	M
$\{1\}$	$\{1\}$	$\{1\}$	M	M
$\{2\}$	$\{2\}$	M	$\{2\}$	M
M	M	M	M	M

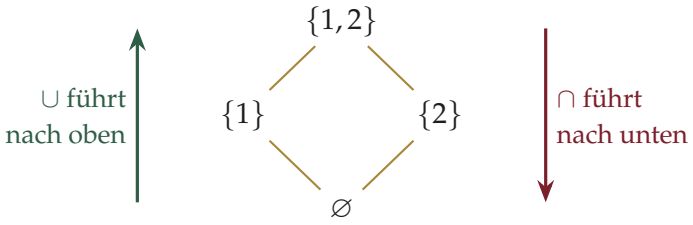
$\cap$	$\varnothing$	$\{1\}$	$\{2\}$	M
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
$\{1\}$	$\varnothing$	$\{1\}$	$\varnothing$	$\{1\}$
$\{2\}$	$\varnothing$	$\varnothing$	$\{2\}$	$\{2\}$
M	$\varnothing$	$\{1\}$	$\{2\}$	M

Lest die Tafeln mit den Regeln aus Abschnitt 1.4.

Links, Vereinigung. Die Zeile und die Spalte von $\varnothing$ (golden hinterlegt) wiederholen die Kopfzeile. Also ist $\varnothing$ das Neutralelement. Sucht jetzt, wo $\varnothing$ als Ergebnis vorkommt: nur ein einziges Mal, oben links. In den Zeilen von $\{1\}$, $\{2\}$ und M steht nirgends $\varnothing$. Diese drei Elemente haben kein Inverses.

Rechts, Durchschnitt. Hier wiederholen die Zeile und die Spalte von M die Kopfzeile. Das Neutralelement ist M. Als Ergebnis kommt M nur unten rechts vor. Die Elemente $\varnothing$, $\{1\}$ und $\{2\}$ haben kein Inverses.

Damit kennen wir die Antworten auf alle drei Teilaufgaben schon, zumindest für $M = \{1, 2\}$. Es bleibt zu verstehen, warum das so ist.



Das Bild zeigt die vier Teilmengen nach Größe geordnet. Vereinigen macht eine Menge größer oder lässt sie gleich, man bewegt sich im Bild nach oben. Schneiden macht kleiner, man bewegt sich nach unten. Beides sind Einbahnstraßen. Das Neutralelement der Vereinigung liegt ganz unten. Wer es einmal verlassen hat, kommt mit $\cup$ nicht mehr dorthin zurück. Beim Durchschnitt liegt das Neutralelement ganz oben, und $\cap$ führt nur nach unten.

Für Informatiker: Bitmasken

Nummeriert man die Elemente von $M = \{1, \ldots, n\}$ durch, dann entspricht jede Teilmenge einer Bitmaske der Länge n. Bit i ist gesetzt, wenn i in der Teilmenge liegt. Für $n = 2$:

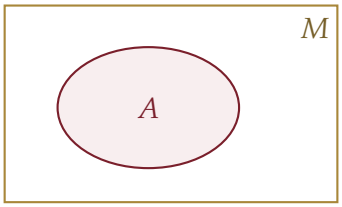
$$\varnothing \leftrightarrow 00, \qquad \{1\} \leftrightarrow 01, \qquad \{2\} \leftrightarrow 10, \qquad M \leftrightarrow 11.$$

Die Vereinigung ist dann das bitweise OR, der Durchschnitt das bitweise AND. Das Neutralelement von OR ist die Maske aus lauter Nullen, das von AND die Maske aus lauter Einsen. OR kann Bits nur setzen und nie löschen. Deshalb gibt es von einer Maske mit einem gesetzten Bit keinen Weg zurück zu 00.

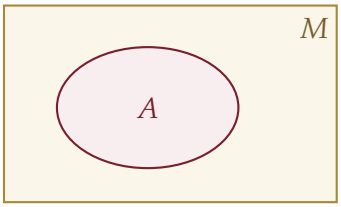
2.3 Teil (a): Beide sind Monoide

Idee

Wir arbeiten das Rezept für Monoide ab. Die Assoziativität ist geschenkt. Wir müssen also nur prüfen, dass die Ergebnisse wieder in $\mathcal{P}(M)$ liegen, und jeweils ein Neutralelement finden. Das Beispiel hat uns schon gezeigt, welche es sind: $\varnothing$ für $\cup$ und M für $\cap$.



$A \cup \varnothing = A$: nichts kommt dazu



$A \cap M = A$: nichts fällt weg, weil $A \subseteq M$

Verknüpfung. Seien $A, B \in \mathcal{P}(M)$, also $A \subseteq M$ und $B \subseteq M$. Dann sind auch $A \cup B \subseteq M$ und $A \cap B \subseteq M$. Die Ergebnisse liegen wieder in $\mathcal{P}(M)$.

Halbgruppe. Die Verknüpfungen $\cup$ und $\cap$ sind nach Voraussetzung assoziativ. Also sind $(\mathcal{P}(M), \cup)$ und $(\mathcal{P}(M), \cap)$ Halbgruppen.

Neutralelement für $\cup$. Die leere Menge ist Teilmenge von M, also $\varnothing \in \mathcal{P}(M)$. Für jedes

$A \in \mathcal{P}(M)$ gilt

$$\varnothing \cup A = A \quad \text{und} \quad A \cup \varnothing = A.$$

Also ist $\varnothing$ ein Neutralelement, und $(\mathcal{P}(M), \cup)$ ist ein Monoid.

Neutralelement für $\cap$. Es gilt $M \subseteq M$, also $M \in \mathcal{P}(M)$. Für jedes $A \in \mathcal{P}(M)$ gilt $A \subseteq M$ und deshalb

$$M \cap A = A \quad \text{und} \quad A \cap M = A.$$

Also ist M ein Neutralelement, und $(\mathcal{P}(M), \cap)$ ist ein Monoid.

Warum gilt $A \cap M = A$? Im Durchschnitt liegen genau die Elemente, die in A *und* in M liegen. Weil $A \subseteq M$ ist, liegt jedes Element von A ohnehin in M. Die zweite Bedingung ist also immer erfüllt, und übrig bleibt genau A. An dieser Stelle wird $A \subseteq M$ wirklich gebraucht.

Häufiger Fehler

„Das Neutralelement von $\cap$ ist $\varnothing$." Das wird oft geschrieben, weil es bei $\cup$ so war. Eine Probe genügt: $\{1\} \cap \varnothing = \varnothing$, und das ist nicht $\{1\}$. Beim Schneiden mit $\varnothing$ bleibt von jeder Menge nichts übrig.

Das Neutralelement gehört zur Verknüpfung. Dieselbe Menge $\mathcal{P}(M)$ hat mit $\cup$ ein anderes Neutralelement als mit $\cap$. Es gibt nicht „das Neutralelement von $\mathcal{P}(M)$".

2.4 Teil (b): Der Fall $M = \varnothing$

Idee

Wir schreiben auf, wie $\mathcal{P}(\varnothing)$ aussieht. Danach ist die Aufgabe fast erledigt.

Welche Teilmengen hat die leere Menge? Genau eine, nämlich sich selbst. Also ist

$$\mathcal{P}(\varnothing) = \{\varnothing\}.$$

Das ist eine Menge mit einem Element.

Häufiger Fehler

$\varnothing$ und $\{\varnothing\}$ sind nicht dasselbe. Die Menge $\varnothing$ hat kein Element. Die Menge $\{\varnothing\}$ hat ein Element, und dieses Element ist die leere Menge. Stellt euch eine leere Schachtel vor und daneben eine Schachtel, in der eine leere Schachtel liegt. Die zweite Schachtel ist nicht leer.

Sei $M = \varnothing$. Dann besteht $\mathcal{P}(M) = \{\varnothing\}$ aus genau einem Element. Dieses Element ist in beiden Monoiden das Neutralelement: In $(\mathcal{P}(M), \cup)$ ist es $\varnothing$, und in $(\mathcal{P}(M), \cap)$ ist es $M = \varnothing$.

Aus der Vorlesung ist bekannt, dass das Neutralelement eines Monoids immer invertierbar und sein eigenes Inverses ist, denn $e * e = e$. Also ist jedes Element von $(\mathcal{P}(\varnothing), \cup)$ und von $(\mathcal{P}(\varnothing), \cap)$ invertierbar, und beide Monoide sind Gruppen.

Die Verknüpfungstafeln sind in diesem Fall winzig:

$\cup$	$\varnothing$
$\varnothing$	$\varnothing$

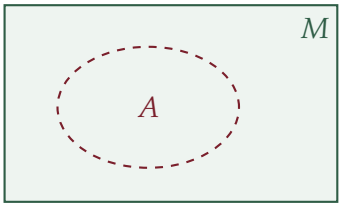
$\cap$	$\varnothing$
$\varnothing$	$\varnothing$

Eine Gruppe mit nur einem Element nennt man die triviale Gruppe. Sie besteht nur aus dem Neutralelement. Dass für $M = \varnothing$ beide Verknüpfungen dasselbe Neutralelement haben, ist kein Widerspruch zu Teil (a): Dort war es $\varnothing$ für $\cup$ und M für $\cap$, und hier ist eben $M = \varnothing$.

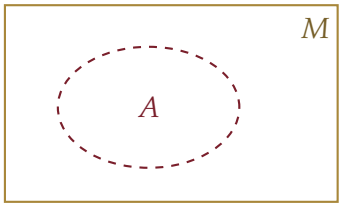
2.5 Teil (c): Der Fall $M \neq \varnothing$

Idee

Um zu zeigen, dass ein Monoid keine Gruppe ist, brauchen wir ein einziges Element ohne Inverses. Das Bild mit den Einbahnstraßen sagt uns, wo wir suchen müssen: möglichst weit weg vom Neutralelement. Bei $\cup$ ist das Neutralelement $\varnothing$ ganz unten, also nehmen wir das oberste Element M. Bei $\cap$ ist das Neutralelement M ganz oben, also nehmen wir das unterste Element $\varnothing$.



$A \cup M = M$ für jedes A:
das Ergebnis ist nie $\varnothing$



$A \cap \varnothing = \varnothing$ für jedes A:
das Ergebnis ist nie M

Sei $M \neq \varnothing$.

Vereinigung. Das Neutralelement von $(\mathcal{P}(M), \cup)$ ist $\varnothing$. Wir zeigen, dass das Element $M \in \mathcal{P}(M)$ nicht invertierbar ist. Für jedes $A \in \mathcal{P}(M)$ gilt $A \subseteq M$ und deshalb $A \cup M = M$. Wegen $M \neq \varnothing$ ist also $A \cup M \neq \varnothing$ für jedes A. Es gibt kein $A \in \mathcal{P}(M)$ mit $A \cup M = \varnothing$. Damit ist M nicht invertierbar, und $(\mathcal{P}(M), \cup)$ ist keine Gruppe.

Durchschnitt. Das Neutralelement von $(\mathcal{P}(M), \cap)$ ist M. Wir zeigen, dass das Element $\varnothing \in \mathcal{P}(M)$ nicht invertierbar ist. Für jedes $A \in \mathcal{P}(M)$ gilt $A \cap \varnothing = \varnothing$. Wegen $\varnothing \neq M$ ist also $A \cap \varnothing \neq M$ für jedes A. Es gibt kein $A \in \mathcal{P}(M)$ mit $A \cap \varnothing = M$. Damit ist $\varnothing$ nicht invertierbar, und $(\mathcal{P}(M), \cap)$ ist keine Gruppe.

Wo wurde $M \neq \varnothing$ benutzt? In beiden Teilen an genau einer Stelle: beim Schluss „$M \neq \varnothing$, also ist das Ergebnis nicht das Neutralelement“. Für $M = \varnothing$ funktioniert dieser Schluss nicht. Das muss auch so sein, denn nach Teil (b) liegen dann Gruppen vor. Es ist eine gute Gewohnheit, nach jedem Beweis zu prüfen, ob jede Voraussetzung wirklich verwendet wurde.

Häufiger Fehler

„Das Inverse von A ist das Komplement $M \setminus A$." Das ist die häufigste falsche Idee zu dieser Aufgabe. Rechnen wir nach:

$$A \cup (M \setminus A) = M, \qquad A \cap (M \setminus A) = \varnothing.$$

Bei $\cup$ müsste aber $\varnothing$ herauskommen, und bei $\cap$ müsste M herauskommen. Das Komplement liefert in beiden Fällen genau das falsche Ergebnis.

Nur ein Beispiel für A ausprobieren. Wer schreibt „$\{1\} \cup M \neq \varnothing$, also hat M kein Inverses", hat einen einzigen Kandidaten ausgeschlossen. Man muss *alle* A ausschließen.

2.6 Etwas mehr: Welche Elemente sind überhaupt invertierbar?

Verlangt war nur ein Element ohne Inverses. Man kann aber genau sagen, was los ist: In beiden Monoiden ist ausschließlich das Neutralelement invertierbar.

Für $\cup$. Angenommen, A ist invertierbar. Dann gibt es ein B mit $A \cup B = \varnothing$. Wegen $A \subseteq A \cup B = \varnothing$ folgt $A = \varnothing$.

Für $\cap$. Angenommen, A ist invertierbar. Dann gibt es ein B mit $A \cap B = M$. Wegen $M = A \cap B \subseteq A \subseteq M$ folgt $A = M$.

Das passt zu den Tafeln aus Abschnitt 2.2, wo das Neutralelement jeweils nur in einer einzigen Zelle stand.

Ausblick: Mit XOR klappt es

Auf Bitmasken gibt es neben OR und AND noch XOR. Die Mengenoperation dazu heißt symmetrische Differenz: $A \triangle B$ enthält die Elemente, die in genau einer der beiden Mengen liegen. Mit dieser Verknüpfung ist $\mathcal{P}(M)$ tatsächlich eine Gruppe. Das Neutralelement ist $\varnothing$, und jede Menge ist ihr eigenes Inverses, denn $A \triangle A = \varnothing$. Das gehört nicht zur Aufgabe, zeigt aber: Ob eine Menge eine Gruppe ist, hängt an der Verknüpfung und nicht an der Menge.

3 Aufgabe 2: Rechnen in einem beliebigen Monoid

Aufgabe 2

Sei $(M, *)$ ein Monoid mit Neutralelement e.

(a) Sei $a \in M$ ein Element, für das Elemente $b, c \in M$ mit $a * b = e$ und $c * a = e$ existieren. Zeigen Sie, dass a dann ein invertierbares Element in $(M, *)$ ist.

(b) Zeigen Sie: Gilt $a * a = e$ für jedes $a \in M$, dann ist $(M, *)$ eine kommutative Gruppe.

3.1 Worum geht es?

In Aufgabe 1 hatten wir ein konkretes Monoid vor uns. Hier ist $(M, *)$ irgendein Monoid. Das M hat mit der Menge M aus Aufgabe 1 nichts zu tun. Wir wissen über M nur drei Dinge:

- $*$ ist assoziativ,
- $e * x = x$ und $x * e = x$ für alle $x \in M$,
- die jeweilige Voraussetzung der Teilaufgabe.

Mehr dürfen wir nicht benutzen. Insbesondere wissen wir nicht, ob $*$ kommutativ ist. Was wir beweisen, gilt dafür in jedem Monoid: für Zahlen, Mengen, Abbildungen, Strings und Matrizen.

3.2 Teil (a): Links- und Rechtsinverses

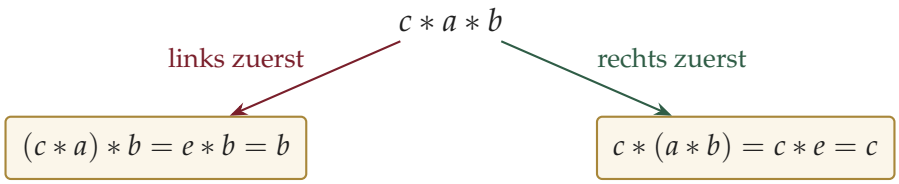
Sortieren wir, was gegeben ist und was fehlt.

Gegeben	$a * b = e$	(b steht *rechts* von a: ein Rechtsinverses)
	$c * a = e$	(c steht *links* von a: ein Linksinverses)
Gesucht	*ein* Element d mit $a * d = e$ *und* $d * a = e$	

Das Problem: b passt auf der einen Seite, c auf der anderen. Niemand hat uns gesagt, dass b und c dasselbe Element sind.

Idee

Wir zeigen $b = c$. Dann erfüllt b beide Gleichungen, und wir sind fertig. Dafür schreiben wir den Ausdruck $c * a * b$ hin und rechnen ihn auf zwei Arten aus.



Assoziativität: Beide Wege liefern dasselbe Element. Also ist $b = c$.

Das a liegt wie der Belag eines Sandwichs zwischen c und b. Klammert man links, hebt c das a auf, und es bleibt b übrig. Klammert man rechts, hebt b das a auf, und es bleibt c übrig. Die Assoziativität sagt, dass beide Rechnungen dasselbe Ergebnis haben.

Es gilt

$$\begin{aligned} b &= e * b && (e \text{ ist neutral}) \\ &= (c * a) * b && (\text{Voraussetzung } c * a = e) \\ &= c * (a * b) && (\text{Assoziativität}) \\ &= c * e && (\text{Voraussetzung } a * b = e) \\ &= c && (e \text{ ist neutral}) \end{aligned}$$

Also ist $b = c$. Das Element b erfüllt damit $a * b = e$ und $b * a = c * a = e$. Nach Definition ist a invertierbar, und es gilt $a^{-1} = b$.

Schaut euch die Begründungen in der rechten Spalte an: neutral, Voraussetzung, assoziativ, Voraussetzung, neutral. Jede Eigenschaft des Monoids und jede Voraussetzung kommt vor. So sieht ein Beweis aus, in dem man nur die Axiome zur Verfügung hat.

Vergleicht die Rechnung außerdem mit dem Beweis aus Abschnitt 1.5, dass das Inverse eindeutig ist. Es ist dieselbe Rechnung.

Häufiger Fehler

Kommutativität benutzen. Wer schreibt „aus $a * b = e$ folgt $b * a = e$“, hat stillschweigend $a * b = b * a$ verwendet. Das ist nicht gegeben.

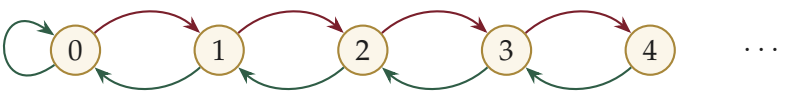
a^{-1} **zu früh hinschreiben.** Das Symbol a^{-1} ist erst erlaubt, wenn feststeht, dass a invertierbar ist. Genau das soll hier bewiesen werden. Wer in der ersten Zeile „multipliziere mit a^{-1}“ schreibt, setzt die Behauptung voraus.

3.3 Reicht nicht auch eine Seite? Ein Gegenbeispiel

Man könnte denken, die Aufgabe verlange zu viel und ein Linksinverses allein sei schon genug. Das stimmt nicht. Dazu ein Beispiel, das an Blatt 3 anknüpft.

Wir nehmen als Monoid die Menge aller Abbildungen $\mathbb{N}_0 \to \mathbb{N}_0$ mit der Hintereinanderausführung $\circ$. Die Hintereinanderausführung ist assoziativ, und die Identität id ist das Neutralelement. Darin betrachten wir zwei Abbildungen:

$$f(n) = n + 1$$



$$g(n) = n - 1 \text{ für } n \geq 1, \quad g(0) = 0$$

Die Abbildung f schiebt jede Zahl um eins nach rechts. Die Abbildung g schiebt jede Zahl um eins nach links, nur die 0 bleibt, wo sie ist.

- Erst f, dann g: $g(f(n)) = g(n+1) = n$. Also ist $g \circ f = \mathrm{id}$.
- Erst g, dann f: $f(g(0)) = f(0) = 1 \neq 0$. Also ist $f \circ g \neq \mathrm{id}$.

Die Abbildung f hat mit g ein Linksinverses. Ein Rechtsinverses kann f nicht haben. Sonst wäre f nach Teil (a) invertierbar und damit bijektiv. f ist aber nicht surjektiv, weil die 0 nie getroffen wird.

Merke

Ein einseitiges Inverses allein macht ein Element noch nicht invertierbar. Hat ein Element aber auf *beiden* Seiten eines, dann sind die beiden gleich, und das Element ist invertierbar.

3.4 Teil (b): Wenn jedes Element sein eigenes Inverses ist

Die Voraussetzung lautet $a * a = e$ für jedes $a \in M$. Anschaulich: Zweimal dasselbe tun bringt einen zurück zum Ausgangspunkt. Das kennt ihr vom Lichtschalter. Zweimal drücken, und das Licht ist im selben Zustand wie vorher.

Ein Beispiel ist XOR auf Bitfolgen der Länge zwei:

$\oplus$	00	01	10	11
00	**00**	01	10	11
01	01	**00**	11	10
10	10	11	**00**	01
11	11	10	01	**00**

Das Neutralelement ist 00. Auf der Diagonalen steht überall 00. Das ist die Bedingung $a * a = e$. Außerdem ist die Tafel symmetrisch zur Diagonalen, die Verknüpfung ist also kommutativ. Die Aufgabe behauptet, dass das kein Zufall ist: Aus der Diagonale folgt die Symmetrie, und zwar in jedem Monoid.

Zu zeigen sind zwei Dinge. Erstens ist $(M, *)$ eine Gruppe. Zweitens ist diese Gruppe kommutativ.

Idee für Schritt 1

Wir brauchen für jedes a ein Inverses. Die Voraussetzung liefert es direkt: a selbst.

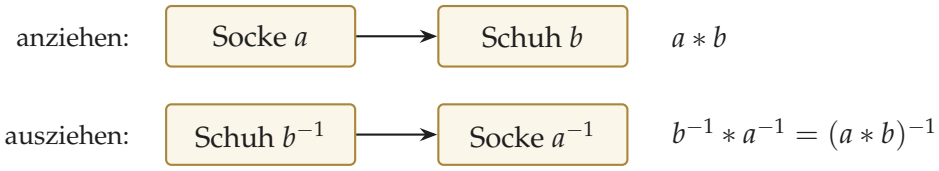
Schritt 1: $(M, *)$ ist eine Gruppe. Sei $a \in M$. Wir setzen $b = a$. Dann ist $a * b = a * a = e$ und $b * a = a * a = e$. Also ist a invertierbar, und es gilt $a^{-1} = a$. Weil jedes Element des Monoids invertierbar ist, ist $(M, *)$ eine Gruppe.

Idee für Schritt 2

Wir müssen $a * b = b * a$ zeigen. Die Voraussetzung spricht aber immer nur über ein einzelnes Element. Wie bekommt man a und b in eine gemeinsame Gleichung? Indem man die Voraussetzung auf das Element $a * b$ anwendet. Auch $a * b$ ist ein Element von M, also gilt auch dafür: Es ist sein eigenes Inverses.

Dazu brauchen wir eine Regel aus der Vorlesung: Das Inverse eines Produkts ist das Produkt der Inversen in *umgekehrter* Reihenfolge.

$$(a * b)^{-1} = b^{-1} * a^{-1}$$



Morgens zieht ihr erst die Socke an und dann den Schuh. Abends müsst ihr erst den Schuh ausziehen und dann die Socke. Wer etwas rückgängig macht, fängt mit dem letzten Schritt an. Die Probe bestätigt die Formel:

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e.$$

Schritt 2: Die Gruppe ist kommutativ. Seien $a, b \in M$. Nach Schritt 1 gilt $c^{-1} = c$ für jedes $c \in M$. Wir wenden das auf $c = a * b$, auf $c = b$ und auf $c = a$ an:

$$\begin{aligned} a * b &= (a * b)^{-1} && (c^{-1} = c \text{ für } c = a * b) \\ &= b^{-1} * a^{-1} && \text{(Vorlesung)} \\ &= b * a && (b^{-1} = b \text{ und } a^{-1} = a) \end{aligned}$$

Also gilt $a * b = b * a$ für alle $a, b \in M$.

Ein zweiter Weg ohne die Formel aus der Vorlesung

Man kann die Kommutativität auch direkt nachrechnen. Wegen $a * b \in M$ gilt $(a * b) * (a * b) = e$. Diesen Ausdruck schieben wir zwischen a und b:

$$\begin{aligned} a * b &= a * e * b && (e \text{ ist neutral}) \\ &= a * (a * b * a * b) * b && ((a * b) * (a * b) = e) \\ &= (a * a) * (b * a) * (b * b) && \text{(Assoziativität: nur umklammert)} \\ &= e * (b * a) * e && (a * a = e \text{ und } b * b = e) \\ &= b * a && (e \text{ ist neutral}) \end{aligned}$$

In der dritten Zeile wurde kein Element verschoben. Die Reihenfolge a, a, b, a, b, b ist dieselbe wie in der Zeile davor. Es wurden nur die Klammern anders gesetzt, und das erlaubt die Assoziativität.

Häufiger Fehler

Schritt 1 vergessen. Viele beweisen nur die Kommutativität. Verlangt ist „kommutative Gruppe“, also muss auch begründet werden, warum überhaupt eine Gruppe vorliegt.

Die Umkehrung glauben. Die Aufgabe sagt: Aus $a * a = e$ für alle a folgt kommutativ. Die Umkehrung ist falsch. $(\mathbb{Z}, +)$ ist eine kommutative Gruppe, aber $1 + 1 = 2 \neq 0$.

$(a * b)^{-1} = a^{-1} * b^{-1}$ **schreiben.** Die Reihenfolge dreht sich um. Dass es in dieser Aufgabe am Ende keinen Unterschied macht, ist erst das Ergebnis des Beweises und darf nicht vorher benutzt werden.

Merke

Wenn eine Voraussetzung „für jedes Element“ gilt, dürft ihr sie auf jedes Element anwenden, das ihr selbst baut, zum Beispiel auf $a * b$. Das ist oft der entscheidende Schritt.

4 Aufgabe 3: Der Körper mit drei Elementen

Aufgabe 3

Sei $(K, +, \cdot)$ ein Körper bestehend aus drei Elementen, $K = \{0, 1, a\}$, wobei 0 das Null- und 1 das Einselement von K bezeichnet. Zeigen Sie, dass die Verknüpfungen $+$ und $\cdot$ durch diese Angaben bereits eindeutig festgelegt sind, d. h. füllen Sie die beiden Verknüpfungstabellen aus und begründen Sie die einzelnen Einträge.

$+$	0	1	a
0			
1			
a			

$\cdot$	0	1	a
0			
1			
a			

4.1 Worum geht es?

Wir wissen über K sehr wenig:

- K ist ein Körper, es gelten also alle Axiome aus Abschnitt 1.6.
- K hat genau drei Elemente. Insbesondere sind 0, 1 und a paarweise verschieden: $0 \neq 1$, $0 \neq a$, $1 \neq a$.
- 0 ist das Neutralelement der Addition, 1 das der Multiplikation.

Was a für ein Ding ist, wissen wir nicht. Trotzdem behauptet die Aufgabe, dass alle 18 Einträge der beiden Tafeln feststehen. Die Axiome lassen keine Wahl.

Die Methode: Ausschließen

In jeder Zelle kann nur 0, 1 oder a stehen. Für jede offene Zelle zeigen wir, dass zwei der drei Möglichkeiten zu einem Widerspruch führen. Dann bleibt die dritte. Ein Widerspruch ist hier immer eine Gleichung wie $1 = 0$ oder $a = 1$, die der Verschiedenheit der drei Elemente widerspricht.

Das Werkzeug ist die Kürzungsregel in der Gruppe $(K, +)$: Aus $x + y = x + z$ folgt $y = z$. Man addiert auf beiden Seiten $-x$.

Vorsicht vor Schulwissen

Schreibt nicht $1 + 1 = 2$. In K gibt es keine 2. Es gibt nur 0, 1 und a, und $1 + 1$ muss eines dieser drei Elemente sein. Alles, was ihr über Zahlen wisst, zählt hier nur, wenn es aus den Körperaxiomen folgt.

4.2 Die Additionstafel

So füllt sich die Tafel in vier Schritten. Neue Einträge sind hervorgehoben.

$+$	0	1	a
0	**0**	**1**	**a**
1	**1**		
a	**a**		

Schritt 1
0 ist neutral

$+$	0	1	a
0	0	1	a
1	1		**0**
a	a	**0**	

Schritt 2
$1+a=0$

$+$	0	1	a
0	0	1	a
1	1	**a**	0
a	a	0	

Schritt 3
$1+1=a$

$+$	0	1	a
0	0	1	a
1	1	a	0
a	a	0	**1**

Schritt 4
$a+a=1$

Schritt 1: Zeile und Spalte der 0**.** Weil 0 das Nullelement ist, gilt $0+x=x$ und $x+0=x$ für jedes $x \in K$. Das liefert $0+0=0$, $0+1=1$, $0+a=a$, $1+0=1$ und $a+0=a$. Fünf Einträge stehen fest.

Schritt 2: $1+a$**.**

- Angenommen, $1+a=1$. Dann ist $1+a=1+0$, und Addition von -1 auf beiden Seiten liefert $a=0$. Widerspruch zu $a \neq 0$.
- Angenommen, $1+a=a$. Dann ist $1+a=0+a$, und Addition von $-a$ auf beiden Seiten liefert $1=0$. Widerspruch zu $1 \neq 0$.

Es bleibt nur $1+a=0$. Weil die Addition kommutativ ist, gilt auch $a+1=0$.

Schritt 3: $1+1$**.**

- Angenommen, $1+1=1$. Dann ist $1+1=1+0$, also $1=0$. Widerspruch.
- Angenommen, $1+1=0$. Nach Schritt 2 ist auch $1+a=0$. Also wäre $1+1=1+a$, und Addition von -1 liefert $1=a$. Widerspruch zu $1 \neq a$.

Es bleibt nur $1+1=a$.

Schritt 4: $a+a$**.**

- Angenommen, $a+a=a$. Dann ist $a+a=a+0$, also $a=0$. Widerspruch.
- Angenommen, $a+a=0$. Nach Schritt 2 ist auch $a+1=0$. Also wäre $a+a=a+1$, und Addition von $-a$ liefert $a=1$. Widerspruch.

Es bleibt nur $a+a=1$.

Was bedeutet Schritt 2? Die Gleichung $1+a=0$ sagt, dass a das Negative von 1 ist: $a=-1$. Ebenso ist 1 das Negative von a. In den Schritten 3 und 4 kann man deshalb auch so argumentieren: Wäre $1+1=0$, dann wäre 1 sein eigenes Negatives. Das Negative von 1 ist aber a, und das Negative ist eindeutig. Das ist dasselbe Argument in anderen Worten.

Warum diese Reihenfolge? Für den Ausschluss von $1+1=0$ haben wir das Ergebnis $1+a=0$ aus Schritt 2 gebraucht. Mit $1+1$ anzufangen wäre deshalb schwieriger gewesen. Bei solchen Aufgaben lohnt es sich, zuerst die Zelle zu suchen, in der schon am meisten feststeht.

Dasselbe mit der Sudoku-Regel

Weil $(K,+)$ eine Gruppe ist, steht in jeder Zeile und jeder Spalte der Additionstafel jedes Element genau einmal (Abschnitt 1.5). Damit kann man die Tafel nach Schritt 1 ganz ohne Rechnen

vervollständigen:

- *Zeile von* 1*:* Dort steht schon eine 1. In den beiden freien Zellen müssen also 0 und a stehen.
- *Spalte von a:* Dort steht oben schon ein a. In der Zelle $1 + a$ kann also kein a stehen. Also ist $1 + a = 0$, und für $1 + 1$ bleibt a.
- *Zeile von a:* Dort stehen jetzt a und 0. Für $a + a$ bleibt nur 1.

Die Sudoku-Regel ist eine Abkürzung für die Rechnungen oben. Jeder Ausschluss „das Element steht in dieser Zeile schon“ ist eine Anwendung der Kürzungsregel. In einer Abgabe solltet ihr die Regel entweder beweisen oder die Rechnungen wie in der Lösung oben ausschreiben.

4.3 Die Multiplikationstafel

·	0	1	a
0	**0**	**0**	**0**
1	**0**		
a	**0**		

Schritt 5
$c \cdot 0 = 0$

·	0	1	a
0	0	0	0
1	0	**1**	***a***
a	0	***a***	

Schritt 6
1 ist neutral

·	0	1	a
0	0	0	0
1	0	1	a
a	0	a	**1**

Schritt 7
$a \cdot a = 1$

Idee

Bei der Multiplikation ist die Null ein Sonderfall, weil sie nicht zur multiplikativen Gruppe gehört. Dass $c \cdot 0 = 0$ ist, steht in keinem Axiom. Wir müssen es beweisen. Weil in der Aussage die Null (aus der Addition) und das Malzeichen gleichzeitig vorkommen, wird das Distributivgesetz im Beweis gebraucht.

Schritt 5: Zeile und Spalte der 0**.** Sei $c \in K$ beliebig. Dann gilt

$$\begin{aligned} c \cdot 0 &= c \cdot (0 + 0) && (0 + 0 = 0) \\ &= c \cdot 0 + c \cdot 0 && \text{(Distributivgesetz)} \end{aligned}$$

Wir addieren auf beiden Seiten $-(c \cdot 0)$:

$$\underbrace{-(c \cdot 0) + c \cdot 0}_{=0} = \underbrace{-(c \cdot 0) + c \cdot 0}_{=0} + c \cdot 0,$$

also $0 = c \cdot 0$. Damit ist $0 \cdot 0 = 0$, $1 \cdot 0 = 0$ und $a \cdot 0 = 0$. Weil die Multiplikation kommutativ ist, gilt auch $0 \cdot 1 = 0$ und $0 \cdot a = 0$.

Schritt 6: Zeile und Spalte der 1**.** Weil 1 das Einselement ist, gilt $1 \cdot 1 = 1$, $1 \cdot a = a$ und $a \cdot 1 = a$.

Schritt 7: $a \cdot a$**.**

- Der Fall $a \cdot a = 0$ kann nicht eintreten. Es ist $a \neq 0$, und in einem Körper ist das Produkt von zwei Elementen ungleich null wieder ungleich null.

- Angenommen, $a \cdot a = a$. Wegen $a \neq 0$ besitzt a ein Inverses a^{-1}. Multiplikation beider Seiten mit a^{-1} liefert $a^{-1} \cdot a \cdot a = a^{-1} \cdot a$, also $1 \cdot a = 1$ und damit $a = 1$. Widerspruch zu $a \neq 1$.

Es bleibt nur $a \cdot a = 1$.

Der Trick in Schritt 5 ist, die Null künstlich als $0 + 0$ zu schreiben. Dadurch entsteht eine Summe, auf die man das Distributivgesetz anwenden kann. Dieser Kniff kommt in der Algebra immer wieder vor.

Auch Schritt 7 lässt sich mit der Sudoku-Regel lesen. Die Elemente 1 und a bilden die multiplikative Gruppe $K \setminus \{0\}$. In der Zeile von a steht innerhalb dieser Gruppe schon ein a, nämlich bei $a \cdot 1$. Für $a \cdot a$ bleibt nur 1.

4.4 Das Ergebnis

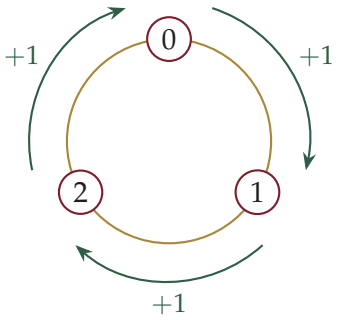
$+$	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

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

Prüft die Tafeln mit den Regeln aus Abschnitt 1.4. Beide sind symmetrisch zur Diagonalen, wie es bei kommutativen Verknüpfungen sein muss. In der Additionstafel steht in jeder Zeile und Spalte jedes Element genau einmal. In der Multiplikationstafel gilt das für den Teil ohne die Null.

4.5 Kontrolle: Rechnen modulo 3

Diese Tafeln kennt ihr vielleicht schon. Ersetzt a durch 2 und rechnet mit Resten bei Division durch 3. Das ist Rechnen auf einer Uhr mit drei Stunden: Nach der 2 kommt wieder die 0.



$1 + 1 = 2$	entspricht $1 + 1 = a$
$1 + 2 = 3 \to 0$	entspricht $1 + a = 0$
$2 + 2 = 4 \to 1$	entspricht $a + a = 1$
$2 \cdot 2 = 4 \to 1$	entspricht $a \cdot a = 1$

Der Pfeil bedeutet „Rest bei Division durch 3“. In Java ist das der Operator `%`: `(2 + 2) % 3` ergibt `1`.

Noch eine zweite Lesart: Wegen $1 + a = 0$ ist $a = -1$. Die Gleichung $a \cdot a = 1$ sagt dann nichts anderes als $(-1) \cdot (-1) = 1$. Minus mal minus ergibt plus, auch in diesem kleinen Körper.

4.6 Was haben wir bewiesen und was nicht?

Eindeutigkeit und Existenz

Bewiesen haben wir: *Wenn* es einen Körper mit drei Elementen gibt, *dann* sehen seine Tafeln so aus wie oben. Das ist die Eindeutigkeit, und nur danach war gefragt.

Nicht bewiesen haben wir, dass diese Tafeln wirklich alle Körperaxiome erfüllen. Dafür müsste man zum Beispiel Assoziativität und Distributivgesetz für alle Kombinationen nachrechnen. Das Rechnen modulo 3 zeigt aber, dass es einen solchen Körper tatsächlich gibt.

Diese beiden Fragen begegnen euch im Studium immer wieder getrennt: Gibt es ein Objekt mit bestimmten Eigenschaften? Und wenn ja, gibt es nur eines?

Häufiger Fehler

Einträge raten und nicht begründen. Wer die Tafeln vom Rechnen modulo 3 kennt und sie einfach hinschreibt, hat die Aufgabe nicht gelöst. Verlangt ist die Begründung, warum kein anderer Eintrag möglich ist.

„$c \cdot 0 = 0$ ist doch klar." In einem abstrakten Körper ist nur klar, was in den Axiomen steht oder daraus bewiesen wurde. Wenn die Regel in der Vorlesung schon bewiesen wurde, dürft ihr sie zitieren. Sonst gehört der Beweis dazu.

Die Verschiedenheit nicht nennen. Jeder Widerspruch in dieser Aufgabe beruht darauf, dass 0, 1 und a verschieden sind. Das sollte im Beweis stehen.

5 Überblick

Aufgabe	Ergebnis	Kerngedanke
1(a)	$(\mathcal{P}(M), \cup)$ ist Monoid mit Neutralelement $\varnothing$, $(\mathcal{P}(M), \cap)$ ist Monoid mit Neutralelement M	Neutralelement angeben und beide Gleichungen prüfen
1(b)	Für $M = \varnothing$ sind beide Gruppen	$\mathcal{P}(\varnothing) = \{\varnothing\}$ hat nur ein Element, das Neutralelement
1(c)	Für $M \neq \varnothing$ ist keines eine Gruppe	M hat bei $\cup$ kein Inverses, $\varnothing$ hat bei $\cap$ keines
2(a)	Links- und Rechtsinverses stimmen überein	$c * a * b$ auf zwei Arten klammern
2(b)	Aus $a * a = e$ für alle a folgt: kommutative Gruppe	Voraussetzung auf $a * b$ anwenden
3	Die Tafeln des Körpers mit drei Elementen stehen fest	Zelle für Zelle zwei von drei Möglichkeiten ausschließen

6 Selbsttest

Versucht die Fragen erst ohne die Lösungen. Sie stehen auf der nächsten Seite.

1. Ist $(\mathbb{N}_0, \max)$ mit $a * b = \max(a, b)$ ein Monoid? Ist es eine Gruppe?
2. Ist $(\mathbb{Z}, *)$ mit $a * b = a - b$ eine Halbgruppe?
3. Sei $M = \{1, 2, 3\}$. Welche Elemente von $(\mathcal{P}(M), \cap)$ sind invertierbar?
4. Wahr oder falsch: In jeder kommutativen Gruppe gilt $a * a = e$ für alle a.
5. In einem Monoid gelte $a * b = e$. Folgt daraus, dass a invertierbar ist?
6. Berechnet im Körper $K = \{0, 1, a\}$ aus Aufgabe 3 die Elemente $-a$, a^{-1} und $a \cdot (1 + a) + 1$.
7. Diese Tafel gehört zu einer Verknüpfung auf $\{x, y, z\}$. Gibt es ein Neutralelement? Ist die Verknüpfung kommutativ? Kann es eine Gruppe sein?

$*$	x	y	z
x	x	y	z
y	y	y	z
z	z	z	z

Lösungen zum Selbsttest

1. Ja, es ist ein Monoid. Das Maximum zweier Zahlen aus $\mathbb{N}_0$ liegt in $\mathbb{N}_0$, die Verknüpfung ist assoziativ, und 0 ist neutral, denn $\max(0, a) = a = \max(a, 0)$. Eine Gruppe ist es nicht: Für jedes b ist $\max(1, b) \geq 1$, also nie 0. Die 1 hat kein Inverses. Das ist dieselbe Einbahnstraße wie bei der Vereinigung.

2. Nein. $(5 - 3) - 1 = 1$, aber $5 - (3 - 1) = 3$. Die Verknüpfung ist nicht assoziativ.

3. Nur M selbst. Aus $A \cap B = M$ folgt $M \subseteq A$, also $A = M$.

4. Falsch. In $(\mathbb{Z}, +)$ ist $1 + 1 = 2 \neq 0$. Aufgabe 2(b) gilt nur in der einen Richtung.

5. Nein, nicht ohne Weiteres. Im Monoid der Abbildungen $\mathbb{N}_0 \to \mathbb{N}_0$ gilt $g \circ f = \mathrm{id}$ für die Abbildungen aus Abschnitt 3.3, aber g ist nicht invertierbar, weil g nicht injektiv ist: $g(0) = g(1) = 0$. Erst wenn es zusätzlich ein c mit $c * a = e$ gibt, folgt die Invertierbarkeit.

6. $-a = 1$, denn $a + 1 = 0$. $\quad a^{-1} = a$, denn $a \cdot a = 1$. $\quad a \cdot (1 + a) + 1 = a \cdot 0 + 1 = 0 + 1 = 1$.

7. Das Neutralelement ist x, denn seine Zeile und seine Spalte wiederholen die Kopfzeile. Die Tafel ist symmetrisch, die Verknüpfung ist also kommutativ. Eine Gruppe kann es nicht sein: In der Zeile von z steht dreimal z, das verletzt die Sudoku-Regel. Außerdem kommt x in den Zeilen von y und z nicht vor, beide haben also kein Inverses.

WEITER GEHT'S

Jetzt bist du dran:
Teste dein Wissen.

Zu Linearer Algebra I gibt es auf meiner Tutoriumsseite einen eigenen Übungsbereich. Nach jeder Antwort steht eine Erklärung, warum sie stimmt oder nicht.

- **Klausurmodus** – Fragen mit Uhr, Auswertung am Ende
- **Zufallsaufgaben** – jedes Mal neue Zahlen
- **Karteikarten** – Begriffe und Sätze, bis sie sitzen
- **Beweis-Werkstatt** – Beweise Schritt für Schritt zusammensetzen

Kostenlos und ohne Anmeldung – einfach QR-Code scannen oder den Link anklicken.

mirkan-analysis.de /lineare-algebra-1