Relationen und Algebraische Strukturen

Dr. Patryk Brzezinski Dr. Alexander Ullmann

Diskrete Mathematik 2 (I168)

3. Quartal 2024

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

Überblick

Organisatorisches

- Präsentation basiert auf: Vorlesungsskript zur Diskreten Mathematik (Prof. Dr. Frank Zimmermann)
- Teil 1: Relationen und Algebraischen Strukturen
  Teil 2: Kryptologie
- Moodle-Kurs zu DM2 Einschreibschlüssel: `DiMa2_I23abc`
- Foliensatz: Vorab über moodle abrufbar (ohne Lösungen); im Anschluss korrigierte Version in moodle
- Beweise, einige Beispiele, etc. nicht auf Folien (Mitschrieb sinnvoll)
- iPad-Notizen im Anschluss in moodle.
- Zusätzliche Übungsaufgaben zum Selbststudium in moodle (Lösungen erscheinen versetzt)
- Tutorium: N.N.
- Klausurtermin: KW41 (Prüfungswoche)

Überblick

Einleitung

- In der Informatik werden Relationen benutzt, um Beziehungen zwischen Objekten darzustellen.
- Als mathematisches Werkzeug sind sie in der theoretischen Wissenschaft nicht wegzudenken.
- Aber spätestens seit dem Durchbruch der relationalen Datenbanken ist Relationenalgebra in Form der SQL auch für den Praktiker von großer Bedeutung.
- Wir werden den Begriff der Relation in harmlosen Zusammenhängen zur Beschreibung von Ordnungen und Äquivalenzen nutzen.
- Ordnungen finden in vielen Bereichen eine Anwendung als Basis für Programmierverfahren oder mathematische Beweisansätze.
- Äquivalenzen bilden die Grundlage jeder Abstraktion, einem wissenschaftlichen Grundprinzip.
- Außerdem werden wir das Konzept der Abbildungen als spezielle Relationen einführen.

Wiederholung: Kartesisches Produkt

Definition (Geordnete Paare)

Es seien x und y beliebige Objekte. Dann heißt (x, y) (geordnetes) Paar.

Zwei geordnete Paare sind genau dann gleich, wenn sie in beiden Komponenten übereinstimmen:

$$(x, y) = (u, v) \Leftrightarrow (x = u \wedge y = v).$$

Beispiele

1. $(1, 2) = (1, 2)$ und $(1, 2) \neq (2, 1)$,
2. $(1, (1, 2)) \neq ((1, 1), 2)$,
3. $(1, \{1\}) \neq (1, 1)$ und $(1, \{1\}) = (1, \{x \in \mathbb{N} | x < 2\})$,
4. $(1, 2) \neq \{1, 2\}$,
5. $1 \neq (1, 1)$.

Wiederholung: Kartesisches Produkt

Definition (Kartesisches Produkt)

Seien M, N Mengen. Das Kartesische Produkt von M und N ist die Menge aller geordneten Paare:

$$M \times N := \{z \mid \exists x \in M \, \exists y \in N : z = (x, y)\}.$$

Man verwendet auch die Notation $M \times N = \{(x, y) \mid x \in M \wedge y \in N\}$.

Beispiele

1. Setze $M := \{1, 2\}$ und $N := \{3, 4, 5\}$, dann ist

$$M \times N = \{(1,3), (1,4), (1,5), (2,3), (2,4), (2,5)\}.$$

2. $\{1, 2\} \times \{2, 3\} = \{(1,2), (1,3), (2,2), (2,3)\}$,
3. $M \times \emptyset = \emptyset, \quad \emptyset \times N = \emptyset.$

Überblick

Einleitung

1. Der Begriff der Relation, den wir auf den Begriff der Menge und des kartesischen Produkts zurückführen, ist im Kern inhaltsgleich mit den zweistelligen Prädikaten.
2. Zweistellige Prädikate beschreiben „Beziehungen“ zwischen Objekten aus einem, oder allgemeiner gesehen aus zwei möglicherweise verschiedenen Betrachtungsbereichen.
3. Genau das können wir mit der Betrachtung von Paaren erreichen.

Allgemeine Relationen

Definition (Relation)

Eine Relation ist eine Menge von Paaren.

Eine Relation zwischen zwei Mengen M und N ist eine Teilmenge des kartesischen Produkts $M \times N$, also $R \subseteq M \times N$.

1. Wenn wir eine Relation als eine Teilmenge des kartesischen Produktes definieren, verstehen wir das so, dass für Paare (x, y), die in der Teilmenge stehen, das x in Beziehung zu y steht.
2. In der Definition für die Relation fehlt nun jeglicher Bezug auf eine konkrete Beziehung.
3. Es wird nur auf abstrakter Ebene ein Zusammenhang zwischen Objekten der Menge M und Objekten der Menge N geschaffen, der nicht weiter hinterfragt wird.
4. Es ist völlig nebensächlich, welche Beziehung die Relation erzeugt, es ist nicht einmal vorausgesetzt, dass es überhaupt solch eine Beziehung gibt.

Allgemeine Relationen

Identifiziert man die Menge $R \subseteq M \times N$ mit einem zweistelligen Prädikat R, so kann man statt $(x, y) \in R$ auch $x\ R\ y$ schreiben und sagt:

- x und y stehen in der Relation R, oder
- x steht in der Relation R zu y.

Ist $M = N$, so sagt man auch *R ist eine Relation auf M* oder *R ist eine Relation in M*.

Beispiel

Betrachte die Menge M aller Männer und F aller Frauen. Die Beziehung „ist Gatte von“ stellt eine Relation R dar, wobei $(x, y) \in R$ gilt genau dann, wenn „x ist Gatte von y“ wahr ist.

Setze $M := \{Hans, Klaus, Peter\}$ und $F := \{Lisa, Mona\}$, und Hans ist verheiratet mit Mona und Klaus ist verheiratet mit Lisa. Dann ist die Relation im Sinne der Definition gegeben durch:

$$R = \big\{(Hans, Mona), (Klaus, Lisa)\big\}.$$

Allgemeine Relationen

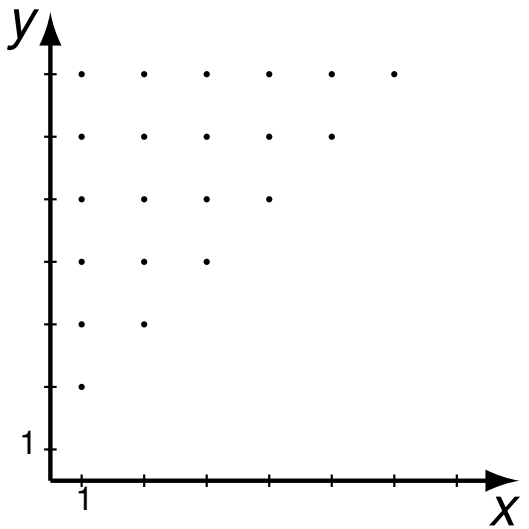
Beispiel

Auf der Menge der natürlichen Zahlen $\mathbb{N}$ kann man das zweistellige Prädikat „$\cdot < \cdot\cdot$“ auch als Relation auffassen. Das Paar (x, y) ist in der Relation (Menge) $<$, genau dann, wenn $x < y$, es gilt also:

$$(x, y) \in\ < \ \Leftrightarrow x < y, \quad \text{und } <= \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x < y\}.$$

(Alternative Notation: $R_< = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x < y\}$)

Visuell kann man sich die Relation $<$ wie folgt vorstellen:
In dem kartesischen Koordinatensystem sind die Punkte aus $\mathbb{N} \times \mathbb{N}$, die zur Relation $<$ gehören, dargestellt:



Allgemeine Relationen

Konkretes Beispiel

Setze $M := \{1, 2, 3\}$ und $N := \{2, 3\}$.
Dann gilt:
$M \times N = \{(1, 2), (1, 3), (2, 2), (2, 3), (3, 2), (3, 3)\}$.
Betrachte die Relation: „kleiner als“ (Symbol: $<$)

$$1 < 2, \quad 1 < 3, \quad 2 < 3.$$

Dann gilt:

$$<= (R_< =)\{(1, 2), (1, 3), (2, 3)\}.$$

Allgemeine Relationen

Zur visuellen Veranschaulichung von Relationen stehen verschiedene Methoden zur Verfügung:

1. Matrixschreibweise,
2. Pfeildiagramm,
3. vereinfachtes Pfeildiagramm.

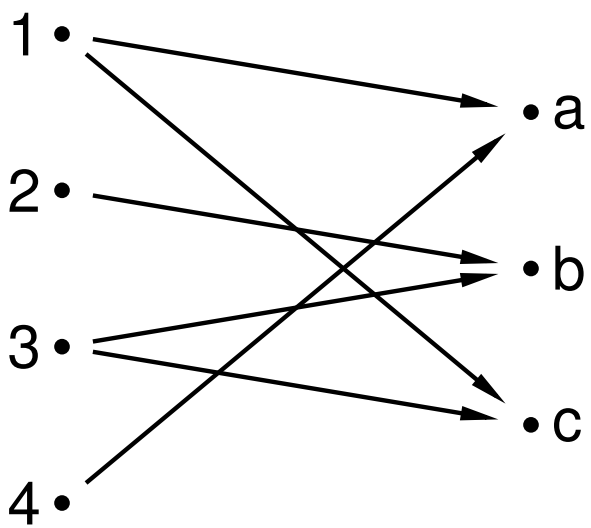
Matrixschreibweise

Gegeben seien $M := \{1, 2, 3, 4\}$, $N := \{a, b, c\}$ und $R := \{(1, a), (1, c), (2, b), (3, b), (3, c), (4, a)\}$.

M \ N	a	b	c
1	1	0	1
2	0	1	0
3	0	1	1
4	1	0	0

Pfeildiagramme

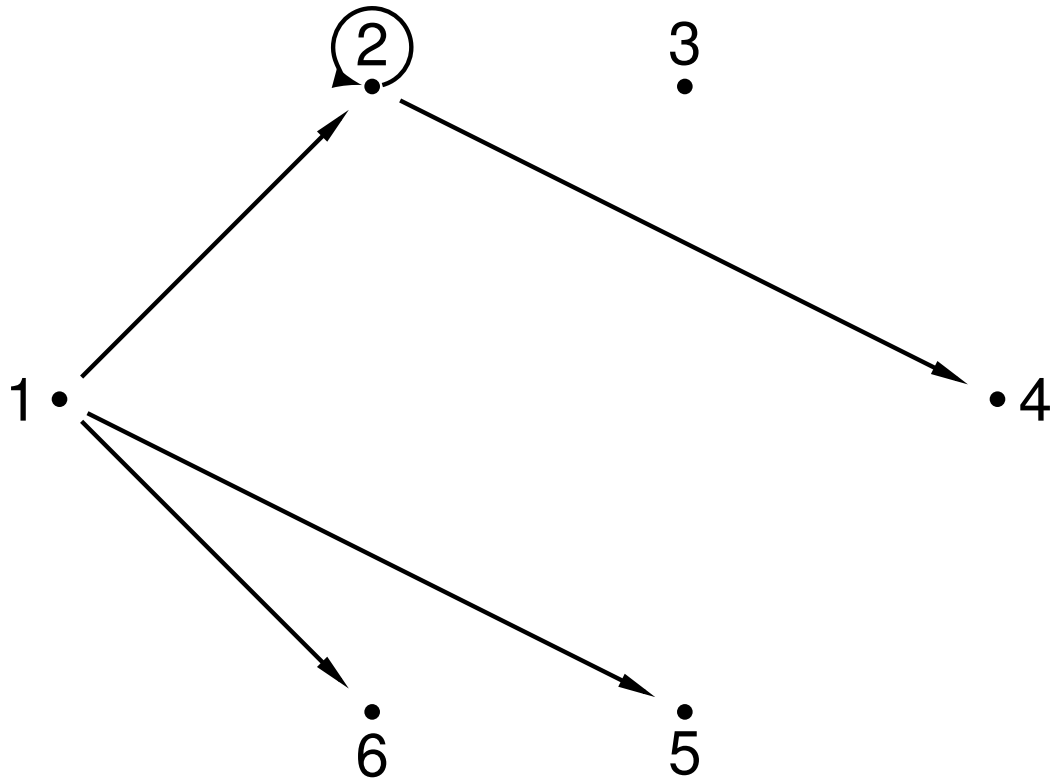
Gegeben seien $M := \{1, 2, 3, 4\}$, $N := \{a, b, c\}$ und $R := \{(1, a), (1, c), (2, b), (3, b), (3, c), (4, a)\}$.



Vereinfachtes Pfeildiagramm

Sind die beiden Mengen M und N identisch, dann bietet es sich an, das Pfeildiagramm zu vereinfachen.

Definiere $M := \{1, 2, 3, 4, 5, 6\}$ und
$R := \{(1, 2), (1, 5), (1, 6), (2, 2), (2, 4)\} \subseteq M \times M$.



Allgemeine Relationen

Bemerkung (Anzahl Relationen auf einer endlichen Menge)

Eine Abschätzung der Anzahl der möglichen Relationen in der Menge $M := \{1, 2, 3, 4, 5, 6\}$:

- Anzahl der möglichen Paare: $|M \times M| = |M| \cdot |M| = 6 \cdot 6 = 36$.
- Anzahl der möglichen Relationen:

  $|P(M \times M)| = 2^{|M \times M|} = 2^{36} = 68.719.476.736 \approx 68.7$ Milliarden

  (Alle Teilmengen des Kreuzprodukts sind Relationen. Eine Menge mit n Elementen hat 2^n Teilmengen.)
- Allgemein gilt für jede endliche Menge M:

  $$|P(M \times M)| = 2^{|M|^2}.$$

Allgemeine Relationen

Definition (Inverse Relation)

Es seien M, N beliebige Mengen und $R \subseteq M \times N$ eine Relation.
Die inverse Relation $R^{-1} \subseteq N \times M$ ist definiert durch:

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

Beispiele

1. Definiere $M := N := \{m \mid m \text{ ist Mann}\}$ und $R := \{(m, k) \in M \times M \mid m \text{ ist Vater von } k\}$. Es gilt dann:

$$R^{-1} = \{(k, m) \in M \times M \mid k \text{ ist Sohn von } m\}.$$

2. Definiere $M := N := \mathbb{N}$ und $R := \{(1,1), (1,2), (2,3), (4,3)\}$, dann gilt:

$$R^{-1} = \{(1,1), (2,1), (3,2), (3,4)\}.$$

Allgemeine Relationen

Beispiel

In der Matrixschreibweise erhält man die inverse Relation durch Spiegelung an der Hauptdiagonalen:

M \ N	a	b	c
1	1	0	1
2	0	1	0
3	0	1	1
4	1	0	0

spiegeln $\longrightarrow$

N \ M	1	2	3	4
a	1	0	0	1
b	0	1	1	0
c	1	0	1	0

Beispiel

Inverse Relation im Pfeildiagramm: Pfeilrichtung umdrehen.

Allgemeine Relationen

Definition (Verkettung von Relationen)

Seien M_1, M_2 und M_3 beliebige Mengen. Es seien $R_1 \subseteq M_1 \times M_2$ und $R_2 \subseteq M_2 \times M_3$ Relationen.

Die Verkettung oder auch Komposition $R_1 R_2 \subseteq M_1 \times M_3$ ist dann die folgende Relation zwischen M_1 und M_3:

$$R_1 R_2 := \{(x, z) \in M_1 \times M_3 \mid \exists y \in M_2 : (x, y) \in R_1 \wedge (y, z) \in R_2\}.$$

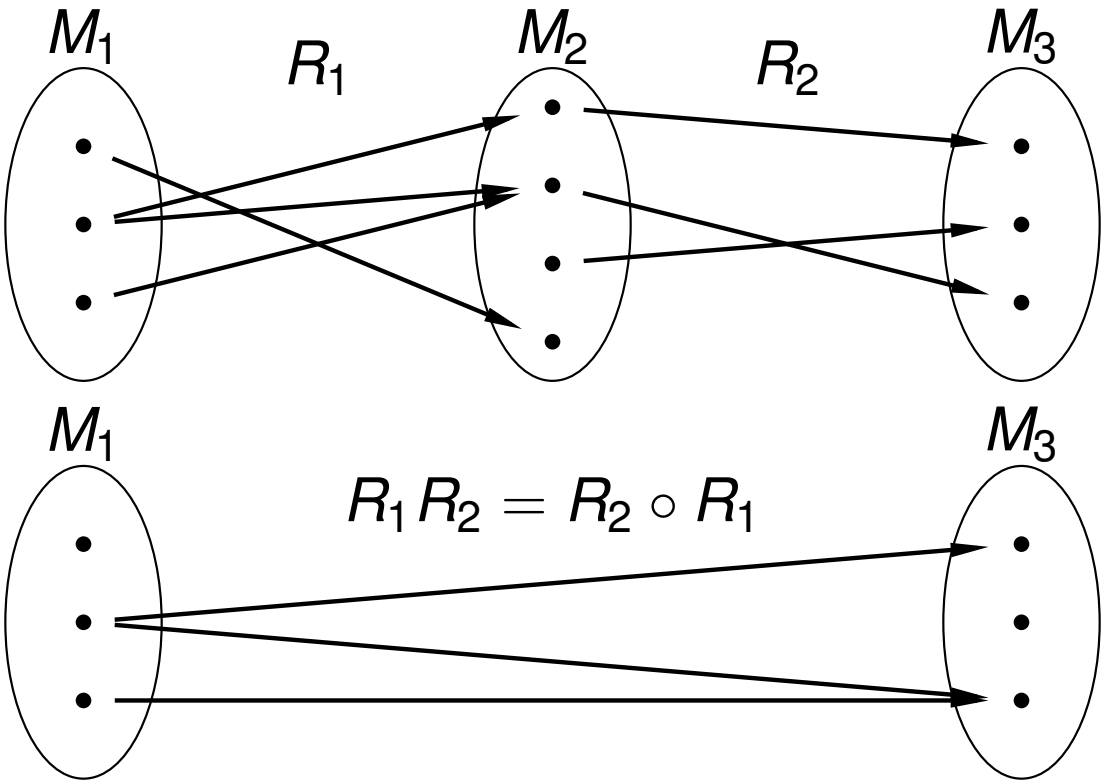
Wir verwenden für die Verkettung auch die Notation $R_2 \circ R_1 := R_1 R_2$ (lies: „R_2 Kringel R_1“ oder „R_2 nach R_1“.)

Hinweis

Man beachte bei der „Kringel-Schreibweise“ in der Notation die umgekehrte Reihenfolge der Relationen! Diese wird später von Vorteil sein, wenn es sich bei R_1 und R_2 um Abbildungen handelt (vgl. Kapitel Abbildungen).

Allgemeine Relationen

Beispiel



Allgemeine Relationen

Beispiel

Setze $M_1 := \{Karl, Otto, Fritz\}$,
$M_2 := M_3 := \{Karl, Otto, Fritz, Ilse, Berta, Anna\}$ sowie

$$\begin{aligned} R_1 &:= \text{„ist Vater von“} \\ &:= \{(Karl, Otto), (Karl, Fritz), (Otto, Berta)\} \subseteq M_1 \times M_2, \end{aligned}$$

$$\begin{aligned} R_2 &:= \text{„ist verheiratet mit“} \\ &:= \{(Otto, Ilse), (Fritz, Berta), (Karl, Anna), \\ &\quad (Ilse, Otto), (Berta, Fritz), (Anna, Karl)\} \subseteq M_2 \times M_3. \end{aligned}$$

Dann gilt:

$$\begin{aligned} R_1 R_2 &= \text{„ist Schwiegervater von“} \\ &= \{(Karl, Ilse), (Karl, Berta), (Otto, Fritz)\}. \end{aligned}$$

Otto ist Schwiegervater von Fritz, weil Fritz Berta, die Tochter seines Bruders (oder vielleicht Halbbruders) Otto geheiratet hat. Das ist zumindest in unserem Kulturkreis nicht üblich! Es könnte natürlich sein, dass Ilse Berta mit in die Ehe gebracht hat, sie also mit Otto gar nicht verwandt ist.

Allgemeine Relationen

Aufgabe

Setze $M := \{1, 2, 3, 4\}$ und $N := \{2, 3, 4, 5, 6, 7, 8\}$ sowie

$$R_1 := \big\{(1, 2), (2, 3), (3, 4)\big\} \subseteq M \times N$$

und

$$R_2 := \big\{(2, 2), (2, 4), (3, 2)\big\} \subseteq N \times M.$$

Bestimmen Sie $R_1 R_2$ und $R_2 R_1$

Lösung

Es gilt:

$$R_1 R_2 = \big\{(1, 2), (1, 4), (2, 2)\big\} \text{ und } R_2 R_1 = \big\{(2, 3), (3, 3)\big\}.$$

Allgemeine Relationen

Bemerkung (Verkettung mit der leeren Menge)

Die Verkettung mit der leeren Menge ergibt die leere Menge, das heißt, für jede Relation R gilt $R \circ \emptyset = \emptyset$ und $\emptyset \circ R = \emptyset$.

Satz (Assoziativgesetz Verkettung)

Es seien $R_1 \subseteq M_1 \times M_2, R_2 \subseteq M_2 \times M_3$ und $R_3 \subseteq M_3 \times M_4$ Relationen, dann gilt:

$$(R_1 R_2) R_3 = R_1 (R_2 R_3).$$

Anmerkung zum Verständnis:

$$R_1 R_2 \subseteq M_1 \times M_3 \text{ und } R_2 R_3 \subseteq M_2 \times M_4.$$

Das Assoziativgesetz besagt, dass **Klammersetzung** bei der Auswertung von mehreren Verkettungen nicht erforderlich ist. Die **Reihenfolge**, in der die Relationen stehen, ist aber sehr wichtig.

Allgemeine Relationen

Satz (Rechenregeln für die inverse Relation)

Es seien $R, R_1 \subseteq M_1 \times M_2$ und $R_2 \subseteq M_2 \times M_3$ Relationen, dann gilt:

1. $(R_1 R_2)^{-1} = R_2^{-1} R_1^{-1}$.

   Anmerkung zum Verständnis:

   $$R_1 R_2 \subseteq M_1 \times M_3 \text{ und } R_2^{-1} R_1^{-1} \subseteq M_3 \times M_1.$$

2. $(R^{-1})^{-1} = R$.

Allgemeine Relationen

Aufgabe

Seien M und N beliebige Mengen und $R \subseteq M \times N$ eine Relation. Welche der Aussagen ist richtig:

1. $\emptyset$ ist eine Relation zwischen M und N.
2. $M \times N$ ist eine Relation zwischen M und N.
3. R^{-1} ist nur definiert, wenn $R \neq \emptyset$.
4. $R^{-1} = \{(x, y) \mid (y, x) \in R\}$.
5. $\emptyset^{-1} = \emptyset$.

Lösung

1. $\emptyset$ ist eine Relation zwischen M und N, da auch $\emptyset$ eine Teilmenge von $M \times N$ ist, wie in der Definition einer Relation gefordert.
2. $M \times N$ ist eine Relation zwischen M und N, da auch $M \times N$ eine Teilmenge von $M \times N$ ist.

Allgemeine Relationen

Lösung

3. R^{-1} ist auch für $R = \emptyset$ definiert, da in der Definiton der inversen Relation keine Bedingung an die Relation R gestellt wird.
4. $R^{-1} = \{(x, y) \mid (y, x) \in R\}$ ist richtig, da x und y nur „lokale“ Variablennamen sind. Wichtig ist nur, dass die Reihenfolge vor und nach dem senkrechten Strich vertauscht wird.
5. $\emptyset^{-1} = \emptyset$ ist richtig, da $\emptyset^{-1} = \{(y, x) \mid (x, y) \in \emptyset\} = \emptyset$.

Allgemeine Relationen

Aufgabe

Seien M_1, M_2, M_3 beliebige Mengen und $R \subseteq S \subseteq M_1 \times M_2$ sowie $T \subseteq M_2 \times M_3$ beliebige Relationen. Beweisen oder widerlegen Sie:
1. $R^{-1} \subseteq S^{-1}$, 2. $S^{-1} \subseteq R^{-1}$, 3. $RT \subseteq ST$.

Lösung

- w Sei $(x, y) \in R^{-1}$. Dann gilt nach Def. der inversen Relation $(y, x) \in R$. Da $R \subseteq S$ vorausgesetzt ist, folgt $(y, x) \in S$ und deshalb wieder nach der Def. der inversen Relation $(x, y) \in S^{-1}$.
- f $M_1 := M_2 := \{1\}$ und $R := \emptyset, S := \{(1, 1)\}$ ist ein Gegenbeispiel, da $R^{-1} = \emptyset$ und $S^{-1} = \{(1, 1)\}$.
- w Sei $(x, z) \in RT$. Dann gibt es nach der Def. der Verkettung ein $y \in M_2$ so, dass $(x, y) \in R$ und $(y, z) \in T$. Da $R \subseteq S$ vorausgesetzt wird, ist $(x, y) \in S$ und daher wieder nach der Def. der Verkettung $(x, z) \in ST$.

Allgemeine Relationen

Aufgabe

Geben Sie Beispiele für Relationen $R_1 \subseteq M_1 \times M_2$ und $R_2 \subseteq M_2 \times M_1$ so an, dass

1. $R_1 R_2 = \emptyset$ und $R_2 R_1 \neq \emptyset$,
2. $R_1 R_2 = M_1 \times M_1$ und $R_2 R_1 \neq M_2 \times M_2$.

Lösung

1. $M_1 := M_2 := \{1, 2\}$ und $R_1 := \{(1, 1)\}$ und $R_2 := \{(2, 1)\}$.
   Dann ist $R_1 R_2 = \emptyset$ und $R_2 R_1 = \{(2, 1)\}$.
2. $M_1 := M_2 := \{1, 2\}$ und $R_1 := \{(1, 1), (2, 1)\}$ sowie
   $R_2 := \{(1, 1), (1, 2)\}$.
   Dann ist $R_1 R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$ und $R_2 R_1 = \{(1, 1)\}$.

Überblick

Eigenschaften von Relationen

In diesem Abschnitt betrachten wir nur Relationen auf einer festen Grundmenge M, also $R \subseteq M \times M$.

Definition (Identische Relationen)

Es sei M eine Menge.
Die Identische Relation ist $\mathrm{Id} := \mathrm{Id}_M := \{(x, x) \mid x \in M\}$.

Definition (Eigenschaften von Relationen)

Es sei M eine Menge und $R \subseteq M \times M$.

1. Die Relation R heißt reflexiv, wenn $\mathrm{Id}_M \subseteq R$, das heißt:

$$\forall x \in M : (x, x) \in R.$$

2. Die Relation R heißt irreflexiv, wenn $\mathrm{Id}_M \cap R = \emptyset$, das heißt:

$$\forall x \in M : (x, x) \notin R.$$

Eigenschaften von Relationen

Definition (Eigenschaften von Relationen)

3. Die Relation R heißt symmetrisch, wenn: $R^{-1} \subseteq R$, das heißt:

$$\forall x, y \in M : (x, y) \in R \Rightarrow (y, x) \in R.$$

4. Die Relation R heißt asymmetrisch, wenn: $R \cap R^{-1} = \emptyset$, das heißt.:

$$\forall x, y \in M : (x, y) \in R \Rightarrow (y, x) \notin R.$$

5. Die Relation R heißt antisymmetrisch, wenn: $R \cap R^{-1} \subseteq \mathrm{Id}_M$, das heißt:

$$\forall x, y \in M : ((x, y) \in R \wedge (y, x) \in R) \Rightarrow x = y,$$

das heißt: $\forall x, y \in M : ((x, y) \in R \wedge x \neq y) \Rightarrow (y, x) \notin R,$
das heißt: $\forall x, y \in M : (x, y) \in R \Rightarrow (x = y \vee (y, x) \notin R).$

6. Die Relation R heißt transitiv, wenn: $R \circ R \subseteq R$, das heißt:

$$\forall x, y, z \in M : ((x, y) \in R \wedge (y, z) \in R) \Rightarrow (x, z) \in R.$$

Eigenschaften von Relationen

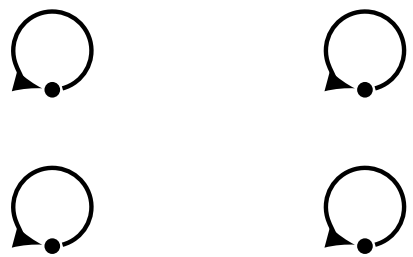
Bemerkung

Man beachte, dass die Aussageformen in (3) - (6) der Definition bedingte Aussagen sind. Keine der Eigenschaften *symmetrisch*, *asymmetrisch*, *antisymmetrisch* oder *transitiv* lässt den Schluss auf eine existierende Beziehung zu!

Eigenschaften von Relationen

Bemerkung

1. Bezüglich Id_M steht jedes Element aus M zu sich selbst in Relation, aber keine zwei verschiedenen Elemente stehen in der Relation Id_M. Das vereinfachte Pfeildiagramm von Id_M hat an jedem Knoten eine Schlinge und sonst keine Pfeile.



   In der Matrixdarstellung wird Id_M durch die Einheitsmatrix dargestellt.

2. Das vereinfachte Pfeildiagramm einer reflexiven Relation hat also ebenfalls an jedem Punkt eine Schlinge (und möglicherweise noch andere Pfeile).

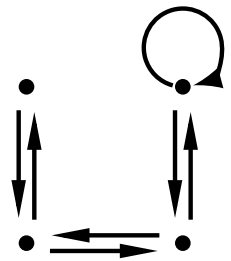
Eigenschaften von Relationen

Bemerkung

3. Es ist R genau dann reflexiv, wenn das Komplement (als Teilmenge von $M \times M$) von R irreflexiv ist. Im vereinfachten Pfeildiagramm einer irreflexiven Relation trägt kein Punkt eine Schlinge.

   Hinweis: Eine Relation kann weder reflexiv noch irreflexiv sein. R ist nicht reflexiv bedeutet nur, dass es *mindestens ein* $x \in M$ gibt mit $(x, x) \notin R$, hingegen bedeutet R irreflexiv, dass $(x, x) \notin R$ *für alle* $x \in M$ gilt.

4. Im vereinfachten Pfeildiagramm einer symmetrischen Relation gibt es genau dann einen Pfeil von x nach y, wenn es auch einen Pfeil von y nach x gibt.



symmetrische Relation

Eigenschaften von Relationen

Zu 4.

In der Matrixdarstellung wird eine symmetrische Relation durch eine symmetrische Matrix dargestellt (Matrix geht durch Spiegelung an der Hauptdiagonalen - von links oben nach rechts unten - in sich über).

Man findet auch die folgende Definition für Symmetrie: $R = R^{-1}$ bzw.

$$\forall x, y \in M : (x, y) \in R \Leftrightarrow (y, x) \in R.$$

In der Tat ist diese Definition äquivalent zu der Definition auf Folie 29: Dies sieht man formal, indem man dort die Variablen x und y in der Definition vertauscht.

Eigenschaften von Relationen

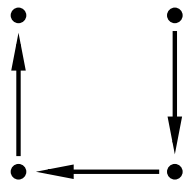
Bemerkung

5. Im vereinfachten Pfeildiagramm einer asymmetrischen Relation gibt es zwischen zwei Punkten *höchstens einen* Pfeil in einer Richtung, aber keinesfalls in beide Richtungen.

   Eine asymmetrische Relation ist sicher irreflexiv (keine Schlingen im vereinfachten Pfeildiagramm), denn es gilt insbesondere

   $$\forall x \in M : (x, x) \in R \Rightarrow (x, x) \notin R,$$

   also muss gelten $(x, x) \notin R$ für alle $x \in M$.

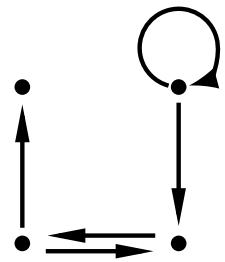


asymmetrische Relation

Eigenschaften von Relationen

Zu 5.

Hinweis: Eine Relation ist nicht entweder symmetrisch oder asymmetrisch. „Nicht symmetrisch“ bedeutet nur, dass es mindestens einen Pfeil (x, y) gibt, für den der Pfeil (y, x) in der umgekehrten Richtung fehlt.



nicht symmetrische und
nicht asymmetrische Relation

Eigenschaften von Relationen

Bemerkung

6. Im vereinfachten Pfeildiagramm einer antisymmetrischen Relation kann es zwischen verschiedenen Punkten höchstens einen Pfeil (eben in einer der beiden möglichen Richtungen) geben, aber es können auch Schlingen vorkommen im Unterschied zu asymmetrischen Relationen.
7. Für das vereinfachte Pfeildiagramm der Relation R bedeutet die Transitivität, dass aus der Existenz von Pfeilen von x nach y und von y nach z die Existenz eines Pfeils von x nach z folgt.

Eigenschaften von Relationen

Satz (Zusammenhänge unter den Eigenschaften)

1. Jede asymmetrische Relation ist irreflexiv.
2. Jede asymmetrische Relation ist antisymmetrisch.
3. Jede irreflexive Relation auf einer nichtleeren Menge ist nicht reflexiv.
4. Jede reflexive Relation auf einer nichtleeren Menge ist nicht irreflexiv.

Beispiel

Seien a, b, c paarweise verschiedene Objekte unser Anschauung oder unseres Denkens. Betrachten Sie die folgende Relation in der Menge $M := \{a, b, c\}$:

$$R := \{(a, a), (a, b), (b, b), (b, a)\}.$$

Wenn wir feststellen wollen, welche Eigenschaften diese Relation hat, dann kann man das durch Testen bzw. durch eine Wertetabelle machen.

Eigenschaften von Relationen

Lösung

Betrachte $M := \{a, b, c\}$ und

$$R := \{(a, a), (a, b), (b, b), (b, a)\}.$$

Die Relation R ist

1. nicht reflexiv, da $(c, c) \notin R$,
2. nicht irreflexiv, da $(a, a) \in R$,
3. symmetrisch (sieht man durch Testen aller Kandidaten bzw. mithilfe einer Wertetabelle),
4. nicht asymmetrisch, da z.B. $(a, b) \in R$ und $(b, a) \in R$ (oder einfacher: da R nicht irreflexiv ist),
5. nicht antisymmetrisch, da $(a, b) \in R$ und $(b, a) \in R$,
6. transitiv (sieht man durch Testen aller Kandidaten bzw. mithilfe einer Wertetabelle).

Eigenschaften von Relationen

Lösung

x	$(x, x) \in R$	$(x, x) \notin R$
a	wahr	falsch
b	wahr	falsch
c	falsch	wahr

Wie diese Wertetafel ergibt, ist die Relation weder reflexiv noch irreflexiv.

x	y	$(x, y) \in R \Rightarrow (y, x) \in R$	$(x, y) \in R \Rightarrow (y, x) \notin R$	$(x, y) \in R \Rightarrow (y, x) \notin R \vee x = y$
a	a	wahr	falsch	wahr
a	b	wahr	falsch	falsch
a	c	wahr	wahr	wahr
b	a	wahr	falsch	falsch
b	b	wahr	falsch	wahr
b	c	wahr	wahr	wahr
c	a	wahr	wahr	wahr
c	b	wahr	wahr	wahr
c	c	wahr	wahr	wahr

Diese Wertetafel zeigt, dass die Relation symmetrisch, nicht asymmetrisch und nicht antisymmetrisch ist.

Eigenschaften von Relationen

Wertetabelle zur Transitivität

x	y	z	$(x,y) \in R \wedge (y,z) \in R$	$(x,z) \in R$	$(x,y) \in R \wedge (y,z) \in R \Rightarrow (x,z) \in R$
a	a	a	wahr	wahr	wahr
a	a	b	wahr	wahr	wahr
a	a	c	falsch	falsch	wahr
a	b	a	wahr	wahr	wahr
a	b	b	wahr	wahr	wahr
a	b	c	falsch	falsch	wahr
a	c	a	falsch	wahr	wahr
a	c	b	falsch	wahr	wahr
a	c	c	falsch	falsch	wahr
b	a	a	wahr	wahr	wahr
b	a	b	wahr	wahr	wahr
b	a	c	falsch	falsch	wahr
b	b	a	wahr	wahr	wahr
b	b	b	wahr	wahr	wahr
b	b	c	falsch	falsch	wahr
b	c	a	falsch	wahr	wahr
b	c	b	falsch	wahr	wahr
b	c	c	falsch	falsch	wahr
c	a	a	falsch	falsch	wahr
c	a	b	falsch	falsch	wahr
c	a	c	falsch	falsch	wahr
c	b	a	falsch	falsch	wahr
c	b	b	falsch	falsch	wahr
c	b	c	falsch	falsch	wahr
c	c	a	falsch	falsch	wahr
c	c	b	falsch	falsch	wahr
c	c	c	falsch	falsch	wahr

Eigenschaften von Relationen

Beispiel

Es sei M die Menge aller Geraden in der 2-dimensionalen Ebene $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$. Die Relation $R :=$ „ist orthogonal zu“ ist

1. nicht reflexiv,
2. irreflexiv,
3. symmetrisch,
4. nicht asymmetrisch,
5. nicht antisymmetrisch,
6. nicht transitiv.

Eigenschaften von Relationen

Aufgabe

Finden Sie eine Menge M und eine Relation R, deren Eigenschaften „nicht symmetrisch“ und „nicht asymmetrisch“ sind.

Lösung

Setze $M := \{1, 2\}$ und $R := \{(1, 1), (1, 2)\}$. R ist

1. nicht symmetrisch, weil $(2, 1) \notin R$,
2. nicht asymmetrisch, weil $(1, 1) \in R$.

Eigenschaften von Relationen

Beispiel

Es sei M die Menge aller Menschen und R die Relation

„ist Bruder von“.

Die Relation ist:

- irreflexiv, weil keiner sein eigener Bruder ist, und wegen $M \neq \emptyset$ somit nicht reflexiv.
- nicht symmetrisch, weil $(\text{Hänsel}, \text{Gretel}) \in R$ und $(\text{Gretel}, \text{Hänsel}) \notin R$,
- nicht antisymmetrisch, weil $(\text{Castor}, \text{Pollux}) \in R$ und $(\text{Pollux}, \text{Castor}) \in R$, und damit auch nicht asymmetrisch.

Bitte beachten Sie, dass die Relation auch **nicht** transitiv ist. Der Grund hierfür ist etwas versteckt:
Castor ist Bruder von Pollux und Pollux ist Bruder von Castor. Aber Castor ist nicht Bruder von Castor.

Eigenschaften von Relationen

Definition

Sei M eine Menge und R eine Relation auf M. Dann wird die Relation R^n für alle $n \in \mathbb{N}_0$ rekursiv definiert durch

$$R^0 := \mathrm{Id}_M \quad \text{und} \quad R^n := R^{n-1} R \text{ für alle } n \in \mathbb{N}.$$

Bemerkung

Formal gilt

$$R^n = \{(x, y) \in M \times M | \exists z_0, \ldots, z_n \in M : z_0 = x \wedge z_n = y \wedge (z_0, z_1) \in R \wedge (z_1, z_2) \in R \wedge \ldots \wedge (z_{n-1}, z_n) \in R\},$$

das heißt im Pfeildiagramm:
Ein Paar (x, y) liegt in R^n, wenn man von x über genau n Pfeile aus R zu y gelangt.

Satz

Sei M eine Menge und R eine Relation auf M. Dann gilt:

(1) R ist transitiv $\Leftrightarrow$ $R = \bigcup_{n \in \mathbb{N}} R^n$.

(2) R ist transitiv und reflexiv $\Leftrightarrow$ $R = \bigcup_{n \in \mathbb{N}_0} R^n$.

Eigenschaften von Relationen

Definition (transitive/transitiv-reflexive Hülle)

Es sei $R \subseteq M \times M$ eine Relation.

1. Die Relation R^+, die durch

$$R^+ := \bigcup_{n \in \mathbb{N}} R^n$$

definiert wird, heißt transitive Hülle von R.

2. Die Relation R^*, die durch

$$R^* := R^+ \cup \mathrm{Id}_M = \bigcup_{n \in \mathbb{N}_0} R^n$$

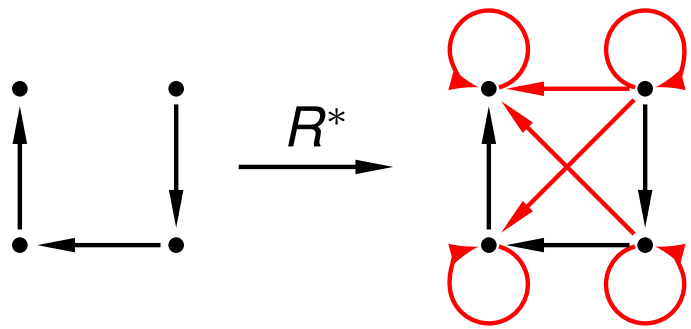
definiert wird, heißt transitiv reflexive Hülle von R.

Eigenschaften von Relationen

Bemerkung

Man kann die transitive Hülle R^+ aus dem Graphen der Relation R konstruieren: Wenn man indirekt (über mehrere Pfeile) von x nach y gelangen kann, so muss ein direkter Pfeil von x nach y hinzugefügt werden.

Beim Bilden der transitiv reflexiven Hülle R^* kommt zusätzlich an jedem $x \in M$ eine Schleife hinzu.



Bilden der transitiv reflexiven Hülle

Bildet man nur die transitive Hülle, so würden im obigen Beispiel die Schleifen nicht dazukommen.

Eigenschaften von Relationen

Satz (Charakterisierung der transitiv reflexiven Hülle)

R^* ist die kleinste transitive und reflexive Relation, die R umfasst, das heißt:

1. R^* ist transitiv und reflexiv, und $R \subseteq R^*$.
2. Ist S eine beliebige transitive und reflexive Relation mit $R \subseteq S$, dann ist auch $R^* \subseteq S$.

Bemerkung

Der Satz kann auch als Definition der transitiv reflexiven Hülle verwendet werden.

Eigenschaften von Relationen

Aufgabe

Definiere $M := \{0, 1, 2\}$.

Prüfen Sie die Relation $R := \{(0, 0), (0, 1), (1, 2)\}$ auf die Eigenschaften

„(ir-)reflexiv“ , „(a-/anti-)symmetrisch“ und „transitiv“.

Eigenschaften von Relationen

Lösung

$M := \{0, 1, 2\}$ und $R := \{(0, 0), (0, 1), (1, 2)\}$.

Die Relation R ist

1. nicht reflexiv, da $(1, 1) \notin R$,
2. nicht irreflexiv, da $(0, 0) \in R$,
3. nicht symmetrisch, da $(0, 1) \in R$ aber $(1, 0) \notin R$,
4. nicht asymmetrisch, da $(0, 0) \in R$ (oder einfacher: da R nicht irreflexiv ist),
5. antisymmetrisch, da $(0, 1), (1, 2) \in R$, aber $(1, 0), (2, 1) \notin R$,
6. nicht transitiv, da $(0, 1), (1, 2) \in R$, aber $(0, 2) \notin R$.

Eigenschaften von Relationen

Aufgabe

Geben Sie Beispiele für Relationen die

1. reflexiv, symmetrisch und nicht transitiv
2. irreflexiv, antisymmetrisch und transitiv
3. antisymmetrisch und nicht asymmetrisch

sind.

Lösung

Es gibt viele Beispiele für solche Relationen. Für alle Teilaufgaben setze $M := \{1, 2, 3\}$.

1. $R := \{(1,1), (2,2), (3,3), (1,2), (2,1), (2,3), (3,2)\}$.
2. $R := \emptyset$.
3. $R := \{(1,1)\}$.

Eigenschaften von Relationen

Aufgabe

Welche Eigenschaften hat die Relation „ist Geschwisterkind von“ auf der Menge der Menschen?

Lösung

Die Relation „ist Geschwisterkind von“ hat folgende Eigenschaften:

nicht reflexiv, irreflexiv, symmetrisch, nicht asymmetrisch, nicht antisymmetrisch, nicht transitiv.

Eigenschaften von Relationen

Aufgabe

Definiere $M := \{1, 2, 3, 4, 5, 6\}$ und die Relation

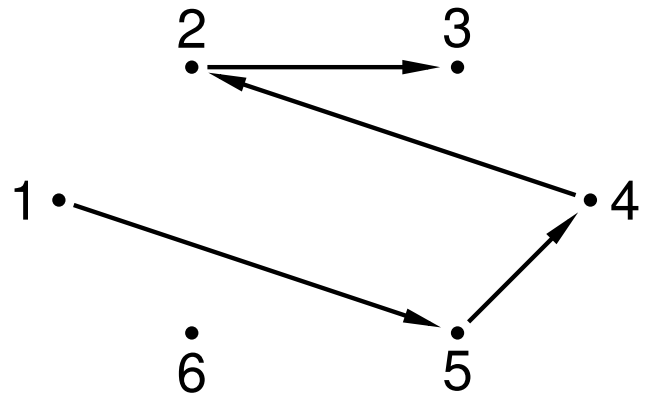
$$R := \{(1, 5), (2, 3), (4, 2), (5, 4)\}.$$

1. Stellen Sie die Relation als vereinfachtes Pfeildiagramm dar.
2. Bestimmen Sie die transitiv reflexive Hülle R^*.

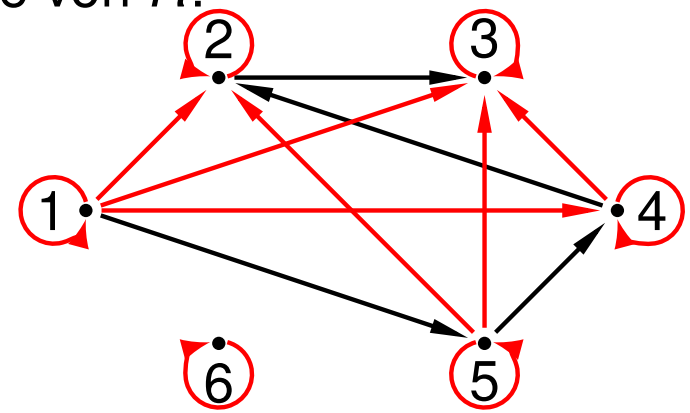
Eigenschaften von Relationen

Lösung

1. Vereinfachtes Pfeildiagramm von R:



2. Transitiv reflexive Hülle von R:



Also ergibt sich:
$R^* = R \cup \mathrm{Id}_M \cup \{(1,2),(1,3),(1,4),(4,3),(5,2),(5,3)\}$.

Überblick

Einleitung

1. Wir wollen in diesem Kapitel Ordnungen mit mathematischen Mitteln beschreiben.
2. Neben einfachen Sequenzen, wo die Elemente wie an einer Schnur aufgereiht werden, wollen wir aber auch Fälle mit einbeziehen, in denen es möglich ist, dass Elemente in mehreren „Strängen“ angeordnet werden.
3. Innerhalb eines Stranges liegt eine paarweise Vergleichbarkeit vor, außerhalb der Stranggrenzen jedoch nicht.
4. Als geeignetes mathematisches Mittel zur Beschreibung stellt sich hierbei der Begriff der Ordnungsrelation heraus.

Ordnungsrelationen

Definition ((strikte) Ordnungsrelation)

Eine Relation R auf der Menge M heißt Ordnungsrelation oder kurz eine Ordnung auf M, wenn sie die folgenden Eigenschaften besitzt:

1. reflexiv,
2. antisymmetrisch und
3. transitiv.

Eine Relation R auf einer Menge M heißt strikte Ordnungsrelation auf M, wenn sie die folgenden Eigenschaften besitzt:

1. asymmetrisch und
2. transitiv.

Ordnungsrelationen

Bemerkung

- Nimmt man alle Elemente (x, x) für $x \in M$ aus einer Ordnungsrelation heraus, erhält man eine strikte Ordnungsrelation. Es gilt also: Ist $R \subseteq M \times M$ eine Ordnungsrelation, so ist $R \setminus \mathrm{Id}_M$ eine strikte Ordnungsrelation.
- Nimmt man alle Elemente (x, x) für $x \in M$ zu einer strikten Ordnungsrelation hinzu, so erhält man eine Ordnungsrelation. Es gilt also: Ist $R \subseteq M \times M$ eine strikte Ordnungsrelation, so ist $R \cup \mathrm{Id}_M$ eine Ordnungsrelation.

Bemerkung

Wir verwenden $\sqsubseteq$ als allgemeines Symbol für eine Ordnungsrelation.

Schreibweise: $(x, y) \in \sqsubseteq \quad \Leftrightarrow \quad x \sqsubseteq y$.

Ebenso verwenden wir $x \sqsubset y$ statt „$x \sqsubseteq y$ und $x \neq y$“ als allgemeines Symbol für eine strikte Ordnungsrelation.

Ordnungsrelationen

Beispiele

1. Die Relation $\leq$ zwischen natürlichen Zahlen ist eine Ordnungsrelation. Die Relation $<$ zwischen natürlichen Zahlen ist eine strikte Ordnungsrelation.
2. Sei X eine beliebige nichtleere Menge und $M := P(X)$ die Potenzmenge von X. Dann ist $\subseteq$ eine Ordnungsrelation auf M (Übung moodle).
3. Auf den natürliche Zahlen $\mathbb{N}_0$ sei die Teilbarkeitsrelation „$|$“ definiert durch:

   $$\forall a, b \in \mathbb{N}_0 : \ a \mid b \ :\Leftrightarrow \ \exists c \in \mathbb{N}_0 : a \cdot c = b.$$

   Die Teilbarkeitsrelation „$|$“ ist eine Ordnungsrelation auf $\mathbb{N}_0$.
4. Auf den ganzen Zahlen $\mathbb{Z}$ sei die Teilbarkeitsrelation „$|$“ als Erweiterung der obigen Definition definiert durch:

   $$\forall a, b \in \mathbb{Z} : \ a \mid b \ :\Leftrightarrow \ \exists c \in \mathbb{Z} : a \cdot c = b.$$

   Die Teilbarkeitsrelation „$|$“ ist nun **keine Ordnungsrelation** auf $\mathbb{Z}$ mehr, weil sie nicht antisymmetrisch ist, denn $-1 \mid 1$ und $1 \mid -1$ aber $1 \neq -1$.

Ordnungsrelationen

Definition (totale und partielle Ordnungsrelation)

Eine Ordnungsrelation $\sqsubseteq$ in der Menge M heißt total, wenn je zwei Elemente von M bezüglich $\sqsubseteq$ vergleichbar sind, das heißt:

$$\forall x, y \in M : x \sqsubseteq y \vee y \sqsubseteq x.$$

Andernfalls heißt $\sqsubseteq$ partielle Ordnung oder Teilordnung.

Ordnungsrelationen

Beispiele

1. $\leq$ ist eine totale Ordnungsrelation in $\mathbb{N}$, denn für je zwei natürliche Zahlen x und y gilt $x \leq y$ oder $y \leq x$. Den Fall, dass zwei natürliche Zahlen nicht vergleichbar sind, gibt es nicht.
2. $\subseteq$ ist i.a. keine totale Ordnungsrelation, denn hat die Menge X mindestens zwei verschiedene Elemente a, b, dann sind $\{a\}$ und $\{b\}$ jeweils nicht Teilmengen voneinander, also nicht vergleichbar.
3. Die Teilbarkeitsrelation $|$ auf $\mathbb{N}_0$ ist auch nur eine partielle Ordnung, denn 2 teilt nicht 3 und 3 teilt nicht 2. D.h. in Bezug auf die Relation $|$ sind 2 und 3 nicht vergleichbar.

Ordnungsrelationen

Zur übersichtlicheren Veranschaulichung von Ordnungsrelationen verwendet man den Begriff der Nachbarschaftsrelation.

Definition (Nachbarschaftsrelation)

1. Es sei $\sqsubset$ eine strikte Ordnungsrelation auf der Menge M. Die Nachbarschaftsrelation $\sqsubset^N$ wird wie folgt definiert:

$$x \sqsubset^N y :\Leftrightarrow x \sqsubset y \text{ und es gibt kein } z \in M \text{ mit } x \sqsubset z \text{ und } z \sqsubset y.$$

2. Es sei $\sqsubseteq$ eine Ordnungsrelation auf der Menge M mit der zugehörigen strikten Ordnungsrelation $\sqsubset$ $\left(\sqsubset = \sqsubseteq \setminus \mathrm{Id}_M \right)$. Dann ist $\sqsubseteq^N := \sqsubset^N$ die Nachbarschaftsrelation von $\sqsubseteq$.

Bemerkung

Die Nachbarschaftsrelation $\sqsubseteq^N$ ist nicht reflexiv und i.a. nicht transitiv.

Ordnungsrelationen

Beispiel

Es sei $\subseteq$ die Ordnungsrelation in der Potenzmenge $P(X)$ der Menge $X = \{1, 2, 3\}$. Es ist

$$P(X) = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\big\}.$$

Für die Nachbarschaftsrelation $\subseteq^N$ ergibt sich

$$\begin{aligned}\subseteq^N \;=\; \Big\{ &(\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{3\}),\\ &(\{1\}, \{1,2\}), (\{1\}, \{1,3\}),\\ &(\{2\}, \{1,2\}), (\{2\}, \{2,3\}),\\ &(\{3\}, \{1,3\}), (\{3\}, \{2,3\}),\\ &(\{1,2\}, \{1,2,3\}),\\ &(\{1,3\}, \{1,2,3\}),\\ &(\{2,3\}, \{1,2,3\})\Big\}.\end{aligned}$$

Ordnungsrelationen

Ein sehr nützliches Hilfsmittel zur Veranschaulichung von Ordnungsrelationen ist das „Hasse Diagramm“ (Helmut Hasse 1898-1979, deutscher Mathematiker, lehrte u.a. in Kiel).

Definition (Hasse Diagramm)

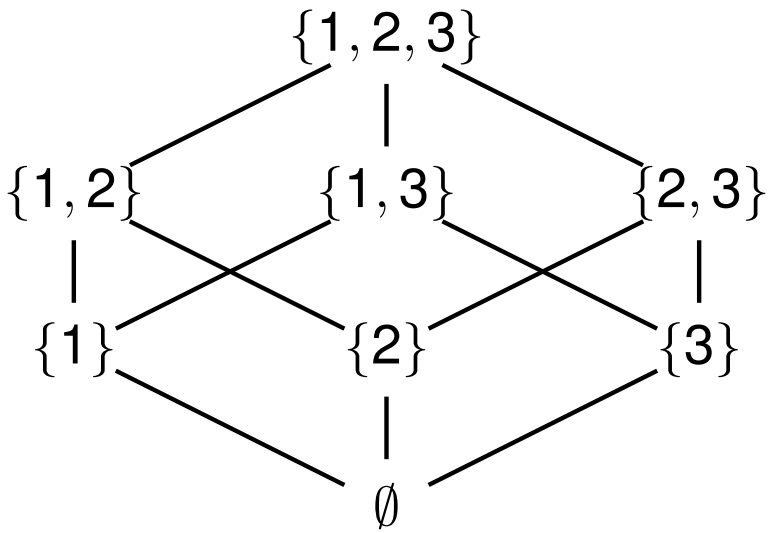
Das Hasse Diagramm einer Ordnungsrelation ist das vereinfachte Pfeildiagramm der zugehörigen Nachbarschaftsrelation, wobei zusätzlich die folgende Konvention bei der Darstellung verwendet wird:

Die Elemente der Grundmenge M werden so auf dem Papier angeordnet, dass gemäß der Ordnungsrelation **größere Elemente oberhalb der kleineren** stehen, und zwei in der Ordnungsrelation **direkt benachbarte Elemente** ohne Pfeilspitze miteinander verbunden werden.

Ordnungsrelationen

Beispiel

Aufgrund der vorgegebenen Pfeilrichtung (von unten nach oben) kann man die Pfeilspitzen weglassen. Damit sieht das Hasse Diagramm der Relation aus dem letzten Beispiel folgendermaßen aus:

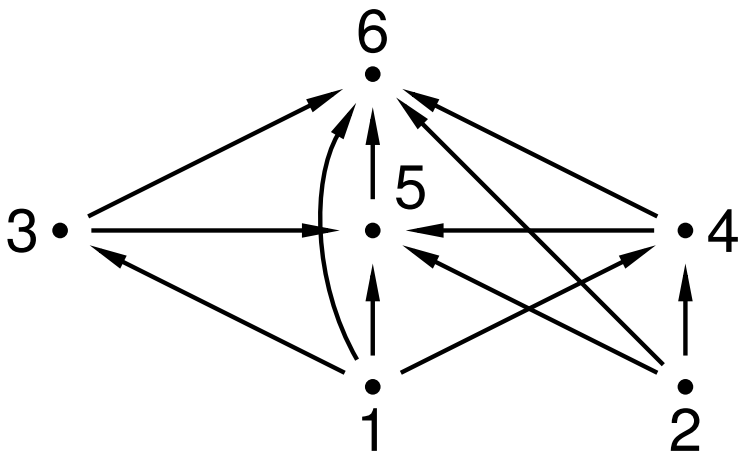


Hasse Diagramm der Teilmengenbeziehung in $P(\{1,2,3\})$

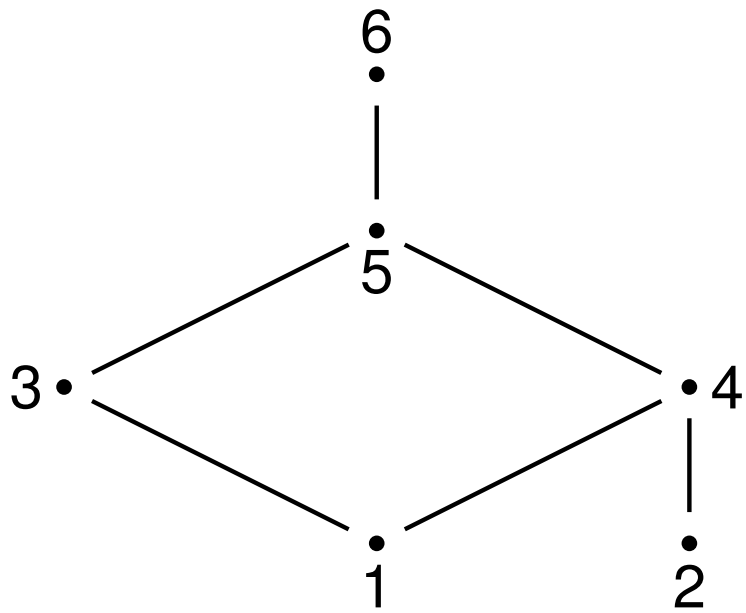
Ordnungsrelationen

Beispiel

Eine strikte Ordnung auf $M = \{1, 2, 3, 4, 5, 6\}$ sei durch ihren Graphen gegeben:



Graph von der Ordnung



Hasse Diagramm

Ordnungsrelationen

Satz (Informationserhaltungssatz für Hasse Diagramme)

Es sei $\sqsubseteq$ eine Ordnungsrelation auf der Menge M.

Dann gilt:

$$(\sqsubseteq^N)^* \subseteq \sqsubseteq .$$

Ist M eine **endliche** Menge, so gilt:

$$(\sqsubseteq^N)^* = \sqsubseteq .$$

Bemerkung

Der Satz besagt, dass es zur Beschreibung einer Ordnungsrelation in einer endlichen Menge vollständig ausreicht, die Nachbarschaftsrelation zu kennen. Durch Bilden der transitiv reflexiven Hülle kann man die Relation immer vollständig rekonstruieren. Damit ist das Hasse Diagramm eine sinnvolle Darstellungsmöglichkeit für Ordnungsrelationen. Obwohl es nicht alle Beziehungen darstellt, können alle Beziehungen aus ihm hergeleitet werden.

Ordnungsrelationen

Bemerkung

Für unendliche Mengen ist es im allgemeinen nicht möglich, eine Ordnungsrelation aus ihrer Nachbarschaftsrelation und damit aus dem Hasse-Diagramm zurückzugewinnen.

Wir betrachten dafür zunächst ein positives Beispiel.

Beispiel

Es sei $\leq$ auf $\mathbb{N}$ die gewöhnliche Ordnung der natürlichen Zahlen. Hier bringt die Nachbarschaftsrelation jede Zahl n mit ihrem Nachfolger $n+1$ in Beziehung, denn zwischen diesen beiden Zahlen gibt es keine dritte.

Es gilt also

$$\leq^N = \{(n, n+1) \mid n \in \mathbb{N}\}.$$

Bildet man die transitiv reflexive Hülle dieser Nachbarschaftsrelation, so kann man problemlos die Ordnung rekonstruieren.

Ordnungsrelationen

Beispiel

Betrachten wir nun die gewöhnliche Anordnung der **reellen Zahlen** $\mathbb{R}$.

Hier haben wir das Problem, dass zwischen zwei reellen Zahlen immer noch eine dritte liegt. Das führt dazu, dass die Nachbarschaftsrelation leer ist. Aus der leeren Nachbarschaftsrelation können wir die Ordnung der reellen Zahlen natürlich nicht rekonstruieren. Wir haben also einen **totalen Informationsverlust**.

Für die Darstellung von Ordnungsrelationen in unendlichen Mengen ist das Hasse Diagramm keine geeignete Darstellungsmethode, da hier ein Informationsverlust zu befürchten ist.

Ordnungsrelationen

Beispiel

Ein weiteres sehr häufig verwendetes Beispiel für eine Ordnungsrelation, bei der ein Informationsverlust auftritt, ist die Ordnung, die man in einem Lexikon anwendet.

Je zwei Einträge in einem Lexikon stehen in einer festgelegten Reihenfolge, und jeder, der ein Lexikon benutzt, kennt sie, sonst würde er keinen Eintrag finden. Diese Ordnung trägt den Namen **lexikografische Ordnung**.

Die transitive Hülle dieser Nachbarschaftsrelation würde zwar die Einträge „a“, „aa“ „aaa“ usw. wieder in Beziehung setzen, nicht jedoch „a“ und „ab“.

Es tritt ein *partieller Informationsverlust* auf. Zur Darstellung der lexikografischen Ordnung eignet sich das Hasse Diagramm also nicht.

Ordnungsrelationen

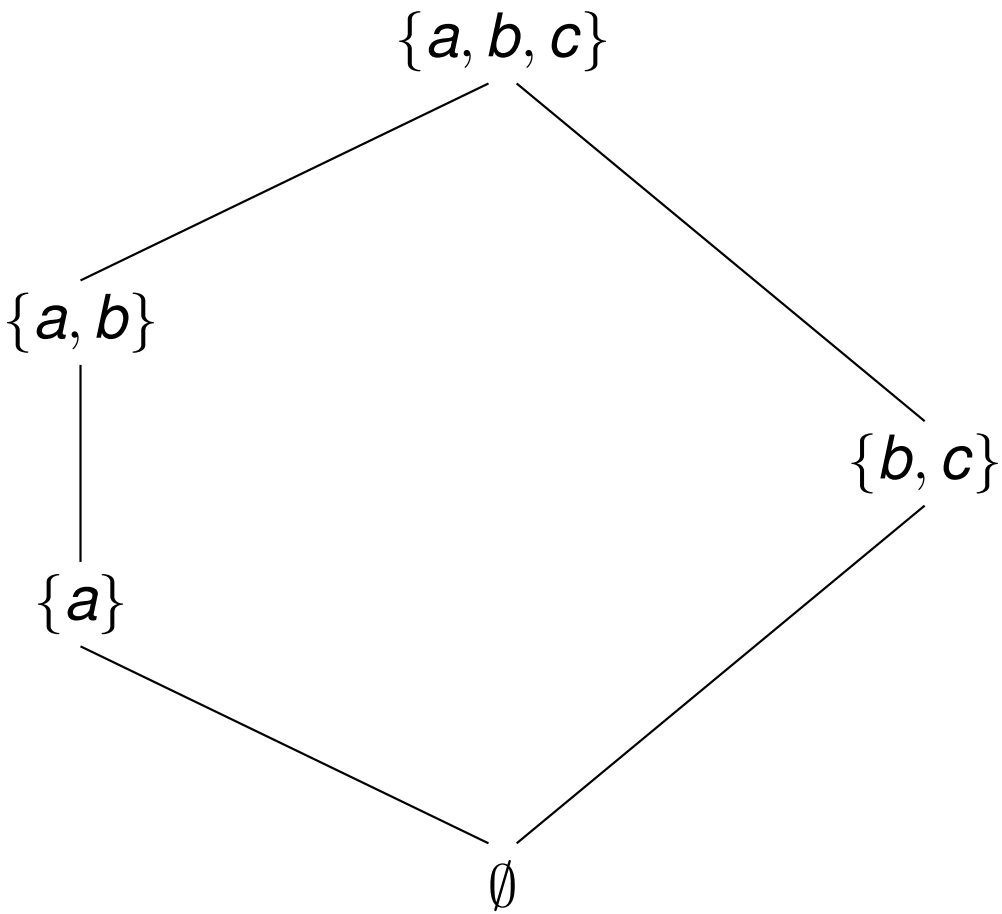
Aufgabe

Geben Sie das Hasse Diagramm für die folgenden Mengen und Relationen an:

1. $\subseteq$ in der Menge $\{\emptyset, \{a, b\}, \{b, c\}, \{a, b, c\}, \{a\}\}$.
2. $|$ (teilt) in der Menge $\{2, 3, 4, 5, 6, 8, 10\}$.
3. $|$ (teilt) in der Menge $\{0, 1, 2, 3, 4, 5, 6, 8, 10\}$.

Ordnungsrelationen

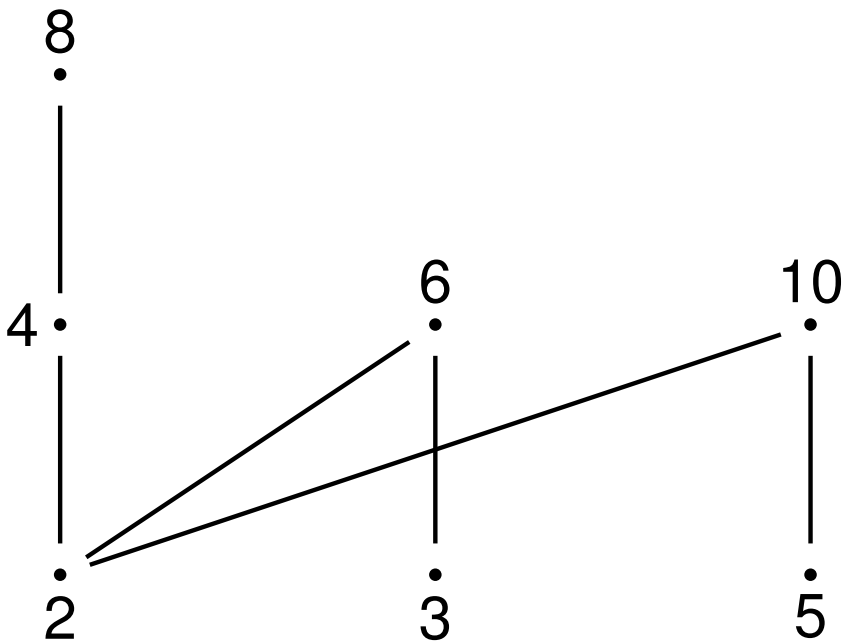
Lösung 1 $\left(\{\emptyset, \{a, b\}, \{b, c\}, \{a, b, c\}, \{a\}\}, \subseteq\right)$



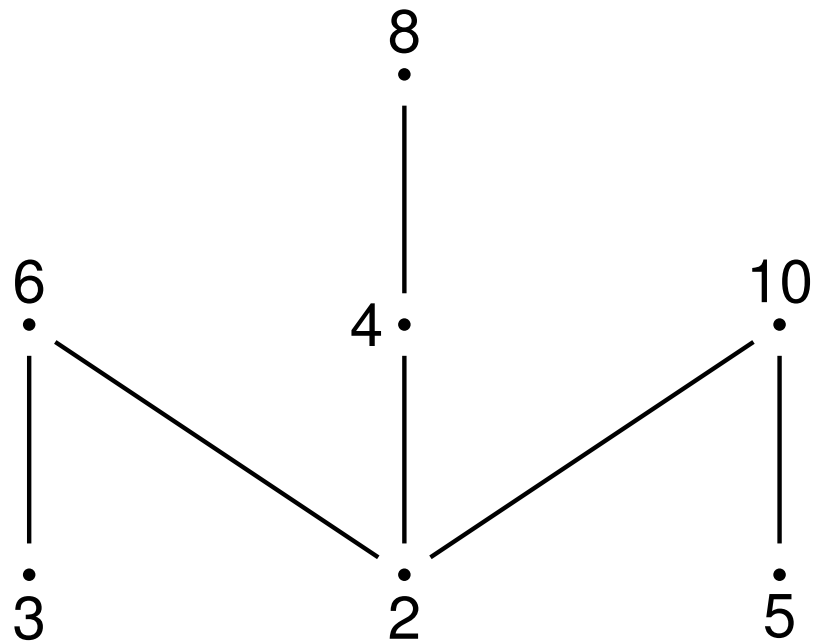
Hasse Diagramm

Ordnungsrelationen

Lösung 2 $\left(\{2,3,4,5,6,8,10\}, |\ \right)$



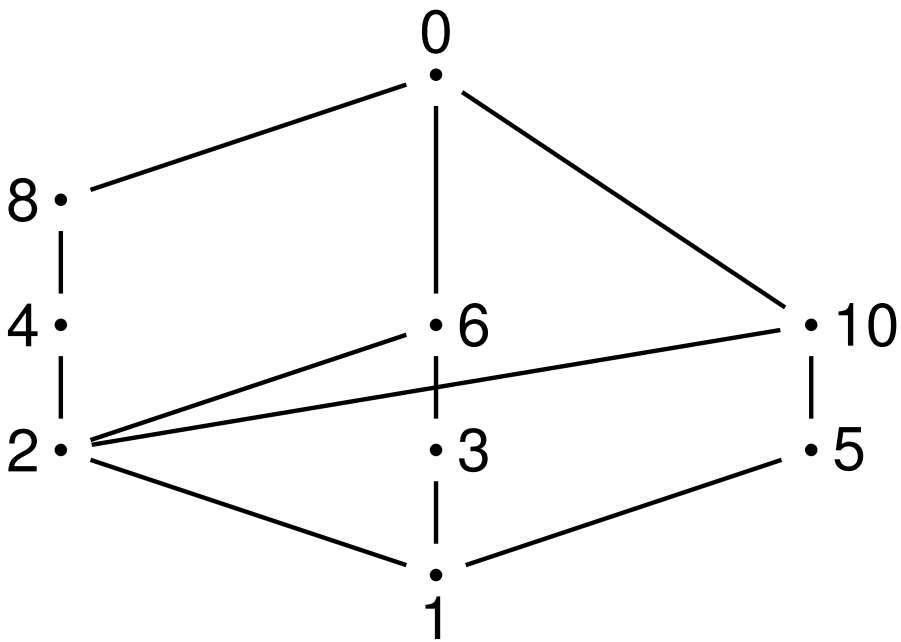
Hasse Diagramm



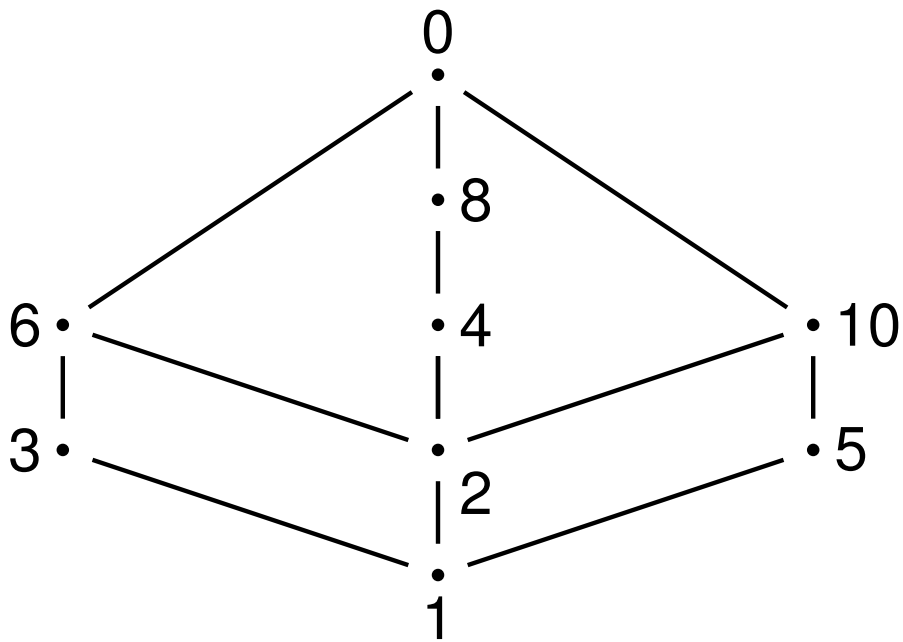
Hasse Diagramm

Ordnungsrelationen

Lösung 3 $(\{0, 1, 2, 3, 4, 5, 6, 8, 10\}, |)$



Hasse Diagramm



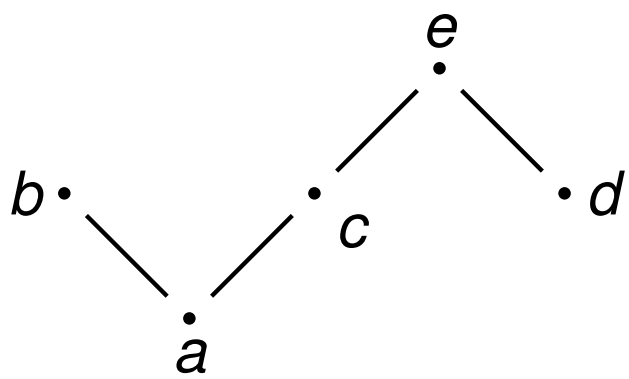
Hasse Diagramm

Man beachte: Nach Definition gilt $x \mid 0$ für jedes $x \in \mathbb{Z}$!

Ordnungsrelationen

Aufgabe

Gegeben ist das folgende Hasse Diagramm:



Geben Sie die zugehörige Ordnungsrelation an.

Lösung

$M = \{a, b, c, d, e\}$ und
$\sqsubseteq = \{(a, b), (a, c), (c, e), (d, e), (a, a), (b, b), (c, c), (d, d), (e, e), (a, e)\}$.

Überblick

Größte und maximale Elemente

Definition (größte und maximale Elemente)

Es sei $\sqsubseteq$ eine Ordnungsrelation auf der Menge M. Es sei $A \subseteq M$ eine beliebige Teilmenge und $b \in M$.

- b heißt größtes Element von A, falls $b \in A$ und für alle $x \in A$ gilt $x \sqsubseteq b$ (d.h.: $\forall x \in A : x \sqsubseteq b$).
- b heißt maximales Element von A, falls $b \in A$ und es gibt kein $x \in A$ mit $b \sqsubset x$ (d.h.: $\neg(\exists x \in A : b \sqsubset x)$).

Ein **größtes Element** der Menge A hat also drei Eigenschaften:

- Es gehört zu der Menge A.
- Es ist mit allen Elementen aus A vergleichbar.
- Bei dem Vergleich stellt sich heraus, dass es größer als jedes andere Element der Menge ist.

Größte und maximale Elemente

Ein **maximales Element** hat dagegen die folgenden „abgeschwächten“ Eigenschaften:

- Es gehört zur Menge A.
- Es ist nicht unbedingt mit allen Elementen vergleichbar.
- Aber innerhalb der Menge der vergleichbaren Elemente ist es größtes Element.

Bemerkung

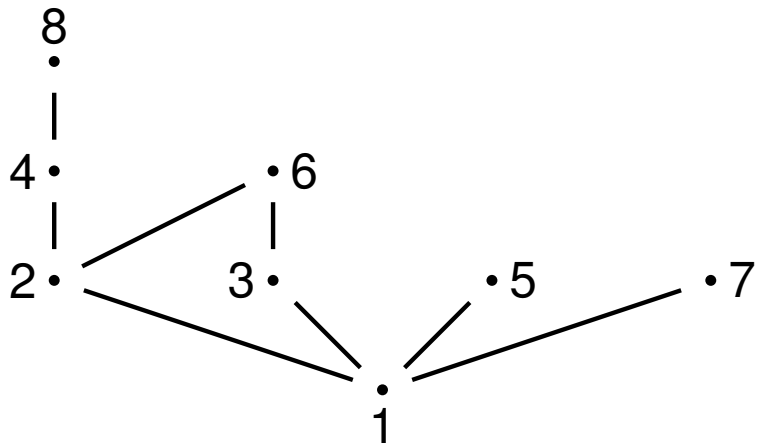
Mit der „es gibt kein . . .“ Aussage lässt sich häufig schwer arbeiten. Deshalb formuliert man die negative Aussage üblicherweise in eine positive um. Es gilt:

$$\begin{aligned}
\neg(\exists x \in A : b \sqsubset x) &\Leftrightarrow \forall x \in A : \neg(b \sqsubset x) \\
&\Leftrightarrow \forall x \in A : \neg(b \sqsubseteq x \wedge x \neq b) \\
&\Leftrightarrow \forall x \in A : \neg(b \sqsubseteq x) \vee x = b \\
&\Leftrightarrow \forall x \in A : b \sqsubseteq x \Rightarrow x = b.
\end{aligned}$$

Größte und maximale Elemente

Beispiel

Definiere $M := \{1, 2, 3, 4, 5, 6, 7, 8\}$ und betrachte auf M die Ordnungsrelation $|$ („teilt“). Das zugehörige Hasse Diagramm ist:



- $5, 6, 7, 8$ sind maximale Elemente von M und M hat kein größtes Element.
- Betrachte $A := \{1, 2, 3, 6\}$. Dann ist 6 größtes und maximales Element von A.
- Betrachte $B := \{2, 3\}$. Dann sind $2, 3$ maximale Elemente von B, und B hat kein größtes Element.
- Betrachte $C := \{2, 3, 5, 6\}$. Dann sind $5, 6$ maximale Elemente von C, und C hat kein größtes Element.

Größte und maximale Elemente

Satz (Existenz maximaler Elemente)

Sei M eine Menge mit einer Ordnungsrelation $\sqsubseteq$. Dann besitzt jede endliche nichtleere Teilmenge $A \subseteq M$ ein maximales Element.

Satz (Eigenschaften von größten Elementen)

Sei M eine Menge mit einer Ordnungsrelation $\sqsubseteq$. Sei $A \subseteq M$. Dann gilt:

1. Es gibt höchstens ein größtes Element in der Menge A.
2. Jedes größte Element der Menge A ist auch maximales Element von A.

Erinnerung: Prinzip

Eine Eindeutigkeitsaussage (Es gibt höchstens ein . . .) wird dadurch bewiesen, dass man annimmt, es gäbe zwei, und man beweist, dann dass diese beiden identisch sein müssen.

Kleinste und minimale Elemente

Analog werden die Begriffe kleinste und minimale Elemente definiert.

Definition (Kleinste und minimale Elemente)

Es sei $\sqsubseteq$ eine Ordnungsrelation in der Menge M. Es sei $A \subseteq M$ eine beliebige Teilmenge und $b \in M$.

- b heißt kleinstes Element von A, falls $b \in A$ und für alle $x \in A$ gilt $b \sqsubseteq x$ (d.h.: $\forall x \in A : b \sqsubseteq x$).
- b heißt minimales Element von A, falls $b \in A$ und es gibt kein $x \in A$ mit $x \sqsubset b$ (d.h.: $\neg(\exists x \in A : x \sqsubset b)$, bzw. $\forall x \in A : x \sqsubseteq b \Rightarrow x = b$).

Bemerkung

(1) Ist R eine Ordnungsrelation, so ist auch R^{-1} eine Ordnungsrelation. (Beweis: Übung moodle)

(2) Offenbar gilt: b ist genau dann kleinstes (resp. minimales) Element von A bezüglich R, wenn b größtes (resp. maximales) Element von A bezüglich R^{-1} ist. (Beweis: Übung moodle)

Kleinste und minimale Elemente

Mit der letzten Bemerkung erhalten wir das folgende Analogon zu den Sätzen von Folie 77 für minimale und kleinste Elemente:

Satz (Existenz minimaler Elemente)

Sei M eine Menge mit einer Ordnungsrelation $\sqsubseteq$. Dann besitzt jede endliche nichtleere Teilmenge $A \subseteq M$ ein minimales Element.

Satz (Eigenschaften von kleinsten Elementen)

Sei M eine beliebige Menge mit einer Ordnungsrelation $\sqsubseteq$. Sei $A \subseteq M$. Dann gilt:

1. Es gibt höchstens ein kleinstes Element in der Menge A.
2. Jedes kleinste Element der Menge A ist auch minimales Element von A.

Hinweis: Zu Übungszwecken wird empfohlen, diese Sätze nochmal direkt zu beweisen, ohne die vorherige Bemerkung zu verwenden!

Kleinste/größte und minimale/maximale Elemente

Aufgabe

Setze $M := \{a, b, c, d, e\}$ und

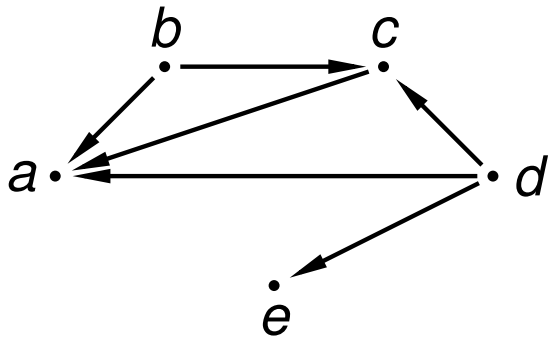
$$\sqsubset := \{(b, a), (c, a), (b, c), (d, c), (d, a), (d, e)\}.$$

1. Überzeugen Sie sich davon, dass es sich bei $\sqsubset$ um eine strikte Ordnungsrelation handelt. Bezeichne die zugehörige Ordnungsrelation (wie üblich) mit $\sqsubseteq$.
2. Erstellen Sie das Hasse-Diagramm von $\sqsubseteq$.
3. Bestimmen Sie alle maximalen/minimalen/größten/kleinsten Elemente der Teilmengen
   - M,
   - $A := \{a, b, c, d\}$,
   - $B := \{a, b, c, e\}$.

Kleinste/größte und minimale/maximale Elemente

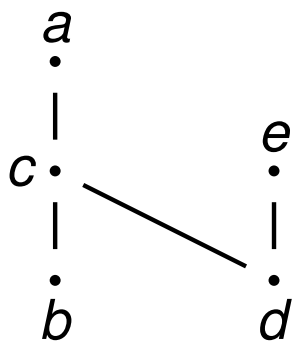
Lösung

1. Vereinfachtes Pfeildiagramm von $\sqsubset$:



Es gibt keine Schleifen und Rückpfeile. Damit ist $\sqsubset$ asymmetrisch. Außerdem ist $\sqsubset$ transitiv, da aus $b \sqsubset c$ und $c \sqsubset a$ auch $b \sqsubset a$ sowie aus $d \sqsubset c$ und $c \sqsubset a$ auch $d \sqsubset a$ gilt.

2. Hasse-Diagramm von $\sqsubseteq$:



Kleinste/größte und minimale/maximale Elemente

Lösung

3. Es ergeben sich die folgenden kleinste/größte und minimale/maximale Elemente:

	M	$A = \{a, b, c, d\}$	$B = \{a, b, c, e\}$
minimale El.	b, d	b, d	b, e
kleinste El.	–	–	–
maximale El.	a, e	a	a, e
größte El.	–	a	–

Obere Schranken und Suprema

Definition (obere/untere Schranke, obere/untere Grenze, Supremum/Infimum)

Es sei $\sqsubseteq$ eine Ordnungsrelation auf der Menge M. Es sei $A \subseteq M$ und $g \in M$.

1. g heißt obere (untere) Schranke von A, falls gilt:
   $$\forall x \in A : x \sqsubseteq g \ (g \sqsubseteq x).$$
2. g heißt obere (untere) Grenze von A, falls g minimales (maximales) Element der Menge der oberen (unteren) Schranken ist.
3. g heißt Supremum (Infimum) von A, falls g kleinstes (größtes) Element der Menge der oberen (unteren) Schranken ist. Dann definieren wir:
   $$g := \sup A \ (g := \inf A).$$

Obere Schranken und Suprema

Warnung

Beliebige Teilmengen müssen im allgemeinen weder obere (untere) Schranken, obere (untere) Grenzen noch Supremum (Infimum) besitzen.

Es gilt jedoch:

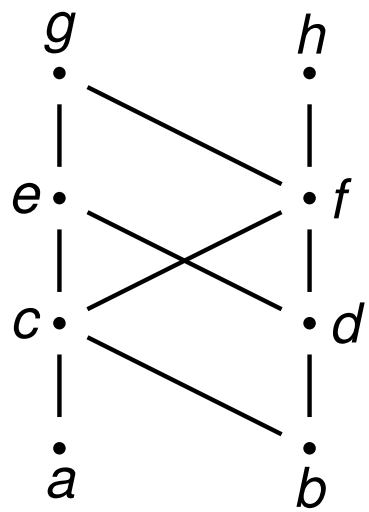
Bemerkung

Wenn ein Supremum (Infimum) existiert, dann ist es eindeutig, da eine Menge immer höchstens ein kleinstes (größtes) Element hat. Deshalb ist die Schreibweise $\sup A$ und $\inf A$ gerechtfertigt.

Obere Schranken und Suprema

Aufgabe

Es sei $\sqsubseteq$ die Ordnungsrelation in der Menge $M = \{a, b, c, d, e, f, g, h\}$, die durch das folgende Hasse Diagramm gegeben ist:



Hasse Diagramm

Untersuchen Sie die folgenden Teilmengen $\{a, b\}, \{c, d\}$ und $\{f, g, h\}$ auf obere/untere Schranken, obere/untere Grenzen, Suprema/Infima, größte/kleinste und maximale/minimale Elemente.

Obere Schranken und Suprema

Lösung

	$A := \{a, b\}$	$B := \{c, d\}$	$C := \{f, g, h\}$
obere Schranken	c, e, f, g, h	e, f, g, h	—
obere Grenzen	c	e, f	—
Supremum	$\sup(A) = c$	—	—
größtes Element	—	—	—
maximale Elemente	a, b	c, d	g, h
untere Schranken	—	b	a, b, c, d, f
untere Grenzen	—	b	f
Infimum	—	b	$\inf(C) = f$
kleinstes Element	—	—	f
minimale Elemente	a, b	c, d	f

Obere Schranken und Suprema

Satz (Existenzsatz größtes/kleinstes Element)

Hat eine endliche Menge nur ein maximales (minimales) Element, so ist dieses bereits das größte (kleinste) Element.

Satz (Existenzsatz Supremum/Infimum)

Hat eine Menge nur eine obere (untere) Grenze, so ist diese bereits das Supremum (Infimum).

Obere Schranken und Suprema

Aufgabe

Erfolg im Leben misst sich z.B. in Geld oder in Liebe. Ein Mensch kann in jeder dieser Kategorien 0 (nichts), 1 (wenig) oder 2 (viel) haben. Die Stufen des Erfolgs sind also:

- (0,0) = (kein Geld, keine Liebe),
- (1,0) = (wenig Geld, keine Liebe),
- (0,1) = (kein Geld, wenig Liebe),
- ...
- (2,2) = (viel Geld, viel Liebe).

„erfolgreicher (oder gleich) sein“ bedeutet mehr oder gleich viel Geld zu haben **und** mehr oder gleich viel Liebe zu haben, wir betrachten also die folgende Ordnungsrelation:

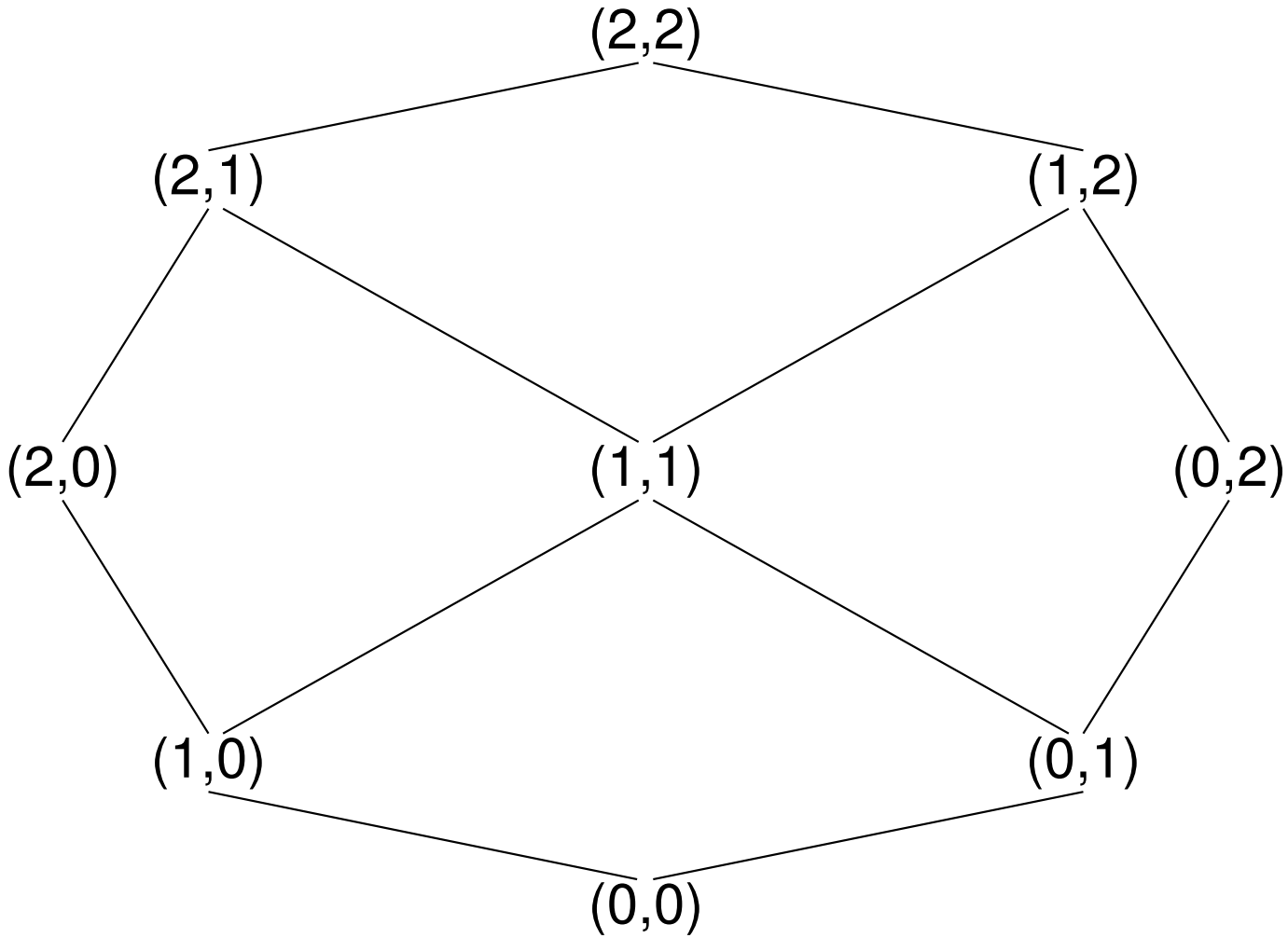
$$(a_2, b_2) \text{ ist erfolgreicher (oder gleich) } (a_1, b_1) :\Leftrightarrow (a_1, b_1) \sqsubseteq (a_2, b_2) :\Leftrightarrow a_1 \leq a_2 \wedge b_1 \leq b_2.$$

Beispiel: (2,1) ist erfolgreicher als (1,1). Aber: Es lässt sich nicht sagen, ob (1,0) erfolgreicher als (0,1) ist oder umgekehrt.

1. Stellen Sie die Relation „$\sqsubseteq$“ als Hasse Diagramm dar.
2. Ermitteln Sie die oberen Schranken und Suprema für die Mengen: $\{(0,1),(1,0)\}$, $\{(1,1),(2,0)\}$ und $\{(0,1),(1,1)\}$.
3. Können Sie eine Formel zur Berechnung des Supremums zweier Paare angeben? (**Hinweis:** Für Zahlen a, b ist $\sup\{a, b\}$ die größere der beiden Zahlen.)

Obere Schranken und Suprema

Lösung (1) (Hasse Diagramm)



Obere Schranken und Suprema

Lösung 2 und 3

(2)

A	obere Schranken	Supremum
$\{(0,1),(1,0)\}$	$(1,1),(1,2),(2,1),(2,2)$	$(1,1)$
$\{(1,1),(2,0)\}$	$(2,1),(2,2)$	$(2,1)$
$\{(0,1),(1,1)\}$	$(1,1),(1,2),(2,1),(2,2)$	$(1,1)$

(3) $\sup\{(a_1,a_2),(b_1,b_2)\} = \big(\sup\{a_1,b_1\},\sup\{a_2,b_2\}\big)$.

Obere Schranken und Suprema

Aufgabe

Beweisen Sie die folgende Aussage:
Gegeben sei eine Ordnungsrelation $\sqsubseteq$ auf einer Menge M und eine Teilmenge $A \subseteq M$. Wenn es ein größtes Element g in A gibt, dann sind alle maximalen Elemente von A gleich diesem g.

Lösung

$\big[$ z.z.: $\forall g \in M : \big(g$ größtes Element von $A\big)$
$\Rightarrow \big(\forall m \in M : m$ maximales Element von $A \Rightarrow m = g\big)\big]$

Sei $g \in M$ größtes Element von A. Sei $m \in M$ ein maximales Element von A.

[Zu zeigen: $m = g$]

Da g größtes Element ist, gilt $a \sqsubseteq g$ für alle $a \in A$, und wegen $m \in A$ folgt damit auch $m \sqsubseteq g$. Da m maximales Element ist, gilt

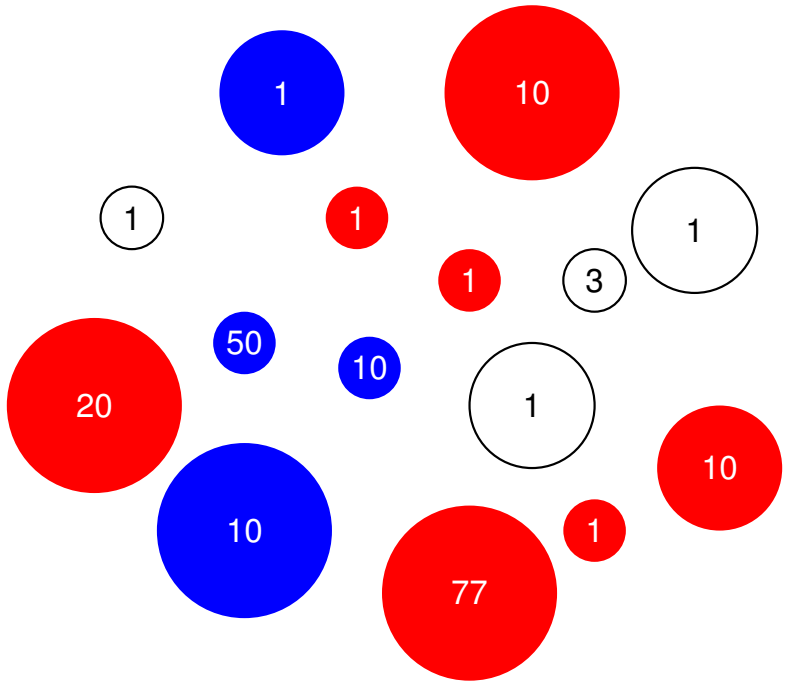
$$\forall a \in A : m \sqsubseteq a \Rightarrow m = a.$$

Wegen $g \in A$, und da wir bereits gezeigt haben, dass $m \sqsubseteq g$ ist, folgt damit $m = g$.

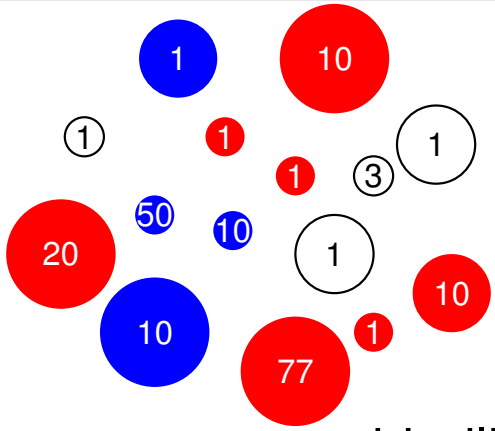
Überblick

Einleitung

- Eines der wichtigsten Prinzipien der Mathematik, wie in jeder Wissenschaft, ist die Abstraktion ...
- ... also das Zusammenfassen von Objekten, die sich in bestimmten Eigenschaften gleichen, aber gleichzeitig das Nichtbeachten von Unterschieden in anderen Eigenschaften.
- Betrachten Sie z.B. folgende Menge von „Münzen“.



Einleitung



- Wir können diese Menge unter unterschiedlichen Gesichtspunkten betrachten, z.B. Größe, Farbe, Nennwert, ... (andere Kriterien möglich)
- Der Abstraktionsvorgang ist nun nichts anderes, als sich **ein Merkmal** herauszunehmen und **alle anderen zu ignorieren**.
- So könnten wir z.B. die Größe herausnehmen und alle anderen Eigenschaften vernachlässigen.
- Wir betrachten dann zwei Münzen als äquivalent, wenn sie die **gleiche Größe** haben, andernfalls sind sie nicht äquivalent.
- Äquivalenzrelationen sind eine Verallgemeinerung dieses Vorgehens. Sie fassen die wesentlichen Eigenschaften von Relationen wie „hat gleiche Farbe“ und „hat gleiche Größe“ zusammen.

Äquivalenzrelationen

Definition (Äquivalenzrelation)

Sei M eine Menge und $R \subseteq M \times M$ eine Relation in M.
R heißt Äquivalenzrelation, falls gilt

1. R ist reflexiv,
2. R ist symmetrisch, und
3. R ist transitiv.

Bemerkung

Wir verwenden $\equiv$ als allgemeines Symbol für eine Äquivalenzrelation.
Will man mehrere Äquivalenzrelationen unterscheiden, so kann man das Symbol $\equiv$ mit einem Index versehen, etwa $\equiv_{\text{Farbe}}$ oder $\equiv_{\text{Größe}}$.

Äquivalenzrelationen

- Ist eine Äquivalenzrelation gegeben, kann man sogenannte Äquivalenzklassen bilden.
- Äquivalenzklassen sind die Zusammenfassung der Objekte, die in der betrachteten Eigenschaft übereinstimmen.
- Die Äquivalenzklassen sind dann die abstrahierten Objekte.

Definition (Äquivalenzklassen)

Sei M eine Menge und $\equiv$ eine Äquivalenzrelation.
Für jedes $x \in M$ ist die Äquivalenzklasse $[x]$ definiert durch:

$$[x] := \{y \in M \mid y \equiv x\}.$$

Die Menge der Äquivalenzklassen wird mit $M/\equiv$ bezeichnet, also:

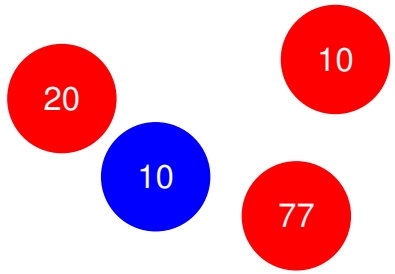
$$M/\equiv := \{[x] \mid x \in M\}.$$

Äquivalenzrelationen

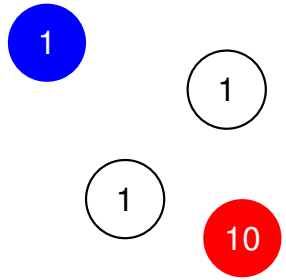
Beispiel

Das folgende Beispiel zeigt die Äquivalenzklassen im Beispiel „Münzen“, wenn die Unterscheidung nach der Größe erfolgt:

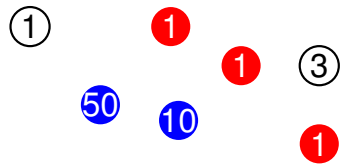
- Äquivalenzklasse „groß“:



- Äquivalenzklasse „mittel“:



- Äquivalenzklasse „klein“:



Äquivalenzrelationen

Bemerkung (Eigenschaften von Äquivalenzklassen)

Sei M eine Menge und $\equiv$ eine Äquivalenzrelation in M. Dann gilt für alle $x, y, z \in M$:

1. $x \in [x]$,
2. $y \in [x] \Rightarrow x \in [y]$,
3. $\big(z \in [y] \wedge y \in [x]\big) \Rightarrow z \in [x]$.

Satz (Äquivalenz und Äquivalenzklassen)

Sei M eine Menge und $\equiv$ eine Äquivalenzrelation in M. Dann sind für alle $x, y \in M$ die folgenden Aussagen äquivalent:

1. $y \equiv x$,
2. $y \in [x]$,
3. $[y] = [x]$.

Äquivalenzrelationen

Aufgabe

Auf $M := \{-2, -1, 0, 1, 2, 3\}$ definiere die Relation $\equiv$ durch

$$x \equiv y :\Leftrightarrow |x| = |y| \quad \text{für alle } x, y \in M.$$

1. Zeigen Sie, dass $\equiv$ eine Äquivalenzrelation ist.
2. Wie sehen die Äquivalenzklassen [0] und [1] aus?
3. Bestimmen Sie die Menge $M/\equiv$.

Äquivalenzrelationen

Lösung

1. Seien $x, y, z \in M$.

   „$\equiv$ *reflexiv*“: [z.z.: $x \equiv x$]
   Es gilt: $|x| = |x|$, also: $x \equiv x$.

   „$\equiv$ *symmetrisch*“: [z.z.: $x \equiv y \Rightarrow y \equiv x$]
   Es gelte $x \equiv y$, also $|x| = |y|$. Dann gilt auch $|y| = |x|$, also $y \equiv x$.

   „$\equiv$ *transitiv*“: [z.z.: $(x \equiv y \wedge y \equiv z) \Rightarrow x \equiv z$]
   Es gelte $x \equiv y$ und $y \equiv z$, also $|x| = |y|$ und $|y| = |z|$. Dann gilt $|x| = |y| = |z|$, also $|x| = |z|$, also $x \equiv z$.

2. $[0] = \{0\}$, und $[1] = \{1, -1\}$.

3. $M/\equiv = \{[0], [1], [2], [3]\} = \{\{0\}, \{1, -1\}, \{2, -2\}, \{3\}\}$.

Äquivalenzrelationen

Definition (Repräsentanten)

Es sei M eine Menge und $\equiv$ eine Äquivalenzrelation auf M. Sei $K \in M/\equiv$ eine Äquivalenzklasse. Für jedes $x \in K$ gilt dann $K = [x]$, und man nennt x einen Repräsentanten der Äquivalenzklasse K.

Definition (Repräsentantensystem)

Eine Teilmenge $V \subseteq M$, die aus jeder Äquivalenzklasse genau einen Repräsentanten enthält, nennt man ein Repräsentantensystem von $M/\equiv$.

- Für jeden Repräsentanten y von $[x]$ gilt $[x] = [y]$.
- Im vorherigen Beispiel sind sowohl 1 als auch -1 Repräsentanten der Äquivalenzklasse $[1]$, denn $[1] = \{-1, 1\} = [-1]$.
- Die Wahl **geeigneter Repräsentanten** wird später im Zusammenhang mit Restklassen eine wichtige Rolle spielen.

Äquivalenzrelationen

Äquivalenzklassen haben zwei wichtige Eigenschaften:

1. Zusammengenommen ergeben sie die ganze Menge, und
2. zwei verschiedene Äquivalenzklassen überschneiden sich nicht.

Satz (Zerlegung in Äquivalenzklassen)

Sei M eine Menge und $\equiv$ eine Äquivalenzrelation in M. Die Menge der Äquivalenzklassen $M/\equiv = \{[x] \mid x \in M\}$ bildet eine Zerlegung der Menge M in disjunkte Mengen, das bedeutet:

1. $\bigcup_{x \in M} [x] = M$,
2. $\forall x, y \in M : [x] \cap [y] = \emptyset \vee [x] = [y]$.

Äquivalenzrelationen

Aufgabe

Können Äquivalenzklassen auch leer sein?

Aufgabe

Geben Sie alle Äquivalenzrelationen auf der Menge $M := \{1, 2, 3\}$ an. Ordnen Sie diese bezüglich der Teilmengenbeziehung.

Äquivalenzrelationen

Lösung

1. Nein, denn es gilt für

$M \neq \emptyset$: $x \in [x]$ für alle $x \in M$.
$M = \emptyset$: $M/\equiv = \emptyset$, d.h. es gibt keine Äquivalenzklassen.

2. Es gibt theoretisch $2^{3\cdot 3} = 512$ Relationen auf M. Aber Reflexifität und Symmetrie schränken bereits auf $2^3 = 8$ Möglichkeiten ein. Z.B. mit Matrix:

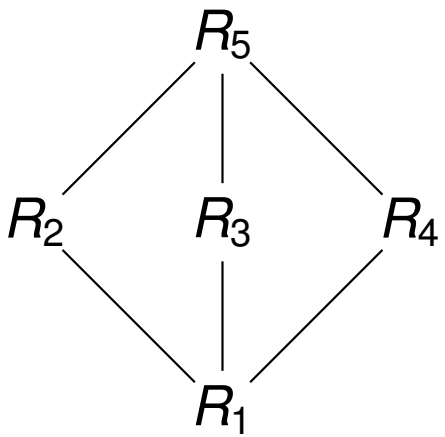
	1	2	3
1	1	0/1	0/1
2	$*$	1	0/1
3	$*$	$*$	1

Tatsächlich sind es zusammen mit Transitivität genau 5:
$R_1 := \mathrm{Id}_M = \{(1,1),(2,2),(3,3)\}$,
$R_2 := \mathrm{Id}_M \cup \{(1,2),(2,1)\}$
$R_3 := \mathrm{Id}_M \cup \{(1,3),(3,1)\}$
$R_4 := \mathrm{Id}_M \cup \{(2,3),(3,2)\}$
$R_5 := \mathrm{Id}_M \cup \{(1,2),(1,3),(2,1),(3,1),(2,3),(3,2)\} = M \times M$

Äquivalenzrelationen

Lösung

Hasse Diagramm der Äquivalenzrelationen bzgl. $\subseteq$:



Überblick

Einleitung

- Wir beschäftigen uns in diesem Abschnitt mit einer speziellen Äquivalenzrelation, nämlich der Kongruenz modulo $m \in \mathbb{N}$.
- Diese wird im weiteren Verlauf der Vorlesung und insbesondere im zweiten Teil der Vorlesung (Kryptologie) wieder aufgenommen.

Wiederholung (Teilbarkeitsrelation)

Es ist $| \subseteq \mathbb{Z} \times \mathbb{Z}$ definiert durch: $a \mid b \Leftrightarrow \exists c \in \mathbb{Z} : a \cdot c = b$.

Definition (Kongruenz modulo m)

Sei $m \in \mathbb{N}$. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen kongruent modulo m, in Zeichen $a \equiv_m b$, genau dann wenn $m \mid (b - a)$.
Die Zahl m wird als Modulus bezeichnet.

Bemerkung

Durch diese Definition wird eine Relation $\equiv_m \subseteq \mathbb{Z} \times \mathbb{Z}$ festgelegt.

Restklassen

Satz ($\equiv_m$ als Äquivalenzrelation)

Sei $m \in \mathbb{N}$. Dann ist $\equiv_m$ eine Äquivalenzrelation auf $\mathbb{Z}$.

Definition (Restklassen)

Die Äquivalenzklassen der Relation $\equiv_m$ heißen Restklassen modulo m. Für $a \in \mathbb{Z}$ wird die zugehörige Restklasse $[a]_m$ geschrieben. Die Menge $\mathbb{Z}/\equiv_m$ aller Restklassen modulo m wird mit $\mathbb{Z}_m$ bezeichnet.

Restklassen

Beispiel (Restklassen mod 2)

Die Äquivalenzklassen der Relation $\equiv_2$ sehen folgendermaßen aus:

$$\begin{aligned}
[0]_2 &= \{a \in \mathbb{Z} \mid a \equiv_2 0\} = \{a \in \mathbb{Z} \mid 2 \mid a\} \\
&= \{0, 2, 4, 6, 8, \ldots, -2, -4, -6, -8, \ldots\} \\
&= \text{Menge aller geraden Zahlen.}
\end{aligned}$$

$$\begin{aligned}
[1]_2 &= \{a \in \mathbb{Z} \mid a \equiv_2 1\} = \{a \in \mathbb{Z} \mid 2 \mid (a-1)\} \\
&= \{1, 3, 5, 7, \ldots, -1, -3, -5, -7, \ldots\} \\
&= \text{Menge aller ungeraden Zahlen.}
\end{aligned}$$

Restklassen

Beispiel (Restklassen mod 5)

Die Äquivalenzklassen der Relation $\equiv_5$ sind:

$$
\begin{aligned}
[0]_5 &= \{0, 5, 10, 15, \ldots, -5, -10, -15, \ldots\}, \\
[1]_5 &= \{1, 6, 11, 16 \ldots, -4, -9, -14, \ldots\}, \\
[2]_5 &= \{2, 7, 12, 17, \ldots, -3, -8, -13, \ldots\}, \\
[3]_5 &= \{3, 8, 13, 18, \ldots, -2, -7, -12, \ldots\}, \\
[4]_5 &= \{4, 9, 14, 19, \ldots, -1, -6, -11, \ldots\}, \\
[5]_5 &= [0]_5, \\
[6]_5 &= [1]_5, \\
[7]_5 &= [2]_5, \\
\vdots \quad &= \quad \vdots \\
[-1]_5 &= [4]_5, \\
[-2]_5 &= [3]_5, \\
\vdots \quad &= \quad \vdots
\end{aligned}
$$

Restklassen

Wiederholung aus Disk. Math. 1 (Teilen mit Rest)

Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit

$$a = q \cdot b + r \quad \text{und } 0 \leq r < |b|.$$

Beispiele

- $a = 12, b = 5$. Dann gilt $a = 2 \cdot b + 2$, also Rest $r = 2$.
- $a = -12, b = 5$. Dann gilt $a = -3 \cdot b + 3$, also Rest $r = 3$.
- $a = 12, b = -5$. Dann gilt $a = -2 \cdot b + 2$, also Rest $r = 2$.
- $a = -12, b = -5$. Dann gilt $a = 3 \cdot b + 3$, also Rest $r = 3$.

Beobachtung

Es gilt $[12]_5 = [2]_5$ und $[-12]_5 = [3]_5$.

Restklassen

Satz (Charakterisierung von Restklassen)

Sei $m \in \mathbb{N}$, dann liegen zwei Zahlen $a, b \in \mathbb{Z}$ genau dann in derselben Restklasse modulo m, wenn a und b bei ganzzahliger Division durch m denselben Rest haben.

Kanonisches Repräsentantensystem von $\mathbb{Z}_m$

Sei $m \in \mathbb{N}$. Dann ist $V = \{0, 1, \ldots, m-1\}$ ein Repräsentantensystem von $\mathbb{Z}_m$, es gilt also

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

Die Repräsentanten $0, 1, \ldots, m-1$ heißen kanonische Repräsentanten.

Darstellung von Restklassen

Für alle $a, m \in \mathbb{Z}$ verwenden wir die Notation $m\mathbb{Z} := \{mk \mid k \in \mathbb{Z}\}$ und

$$a + m\mathbb{Z} := \{a + mk \mid k \in \mathbb{Z}\} = \{b \in \mathbb{Z} \mid b - a \in m\mathbb{Z}\} = \{b \in \mathbb{Z} \mid a \equiv_m b\}.$$

Dann gilt $[a]_m = a + m\mathbb{Z}$ für alle $a \in \mathbb{Z}$ und $m \in \mathbb{N}$.

Restklassen

Aufgabe

(a) Geben Sie die Restklassen zu den Relationen $\equiv_3$ und $\equiv_6$ an.

(b) Bestimmen Sie für $m = 3$ und $m = 6$ zu den Zahlen $21, 100, 102$ jeweils die zugehörige Restklasse $[r]_m$ mit $0 \leq r < m$.

(c) Welche der Inklusionen $[a]_3 \subseteq [b]_6$ oder $[b]_6 \subseteq [a]_3$ mit $a, b \in \{0, 1, 2, 3, 4, 5\}$ sind möglich?

Restklassen

Lösung

(a) $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ mit

$$\begin{aligned} [0]_3 &= \quad 3\mathbb{Z} \quad &&= \{\ldots, -6, -3, 0, 3, 6, \ldots\}, \\ [1]_3 &= 1 + 3\mathbb{Z} &&= \{\ldots, -5, -2, 1, 4, 7, \ldots\}, \\ [2]_3 &= 2 + 3\mathbb{Z} &&= \{\ldots, -4, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$ mit $[a]_6 = a + 6\mathbb{Z}$ für alle $a \in \mathbb{Z}$.

(b) Jeweils Teilen mit Rest durch 6 bzw. 3:

$$\begin{aligned} 21 &= 7 \cdot 3 + 0 \quad &&\rightsquigarrow \quad [21]_3 = [0]_3, \\ 21 &= 3 \cdot 6 + 3 \quad &&\rightsquigarrow \quad [21]_6 = [3]_6, \\ 100 &= 33 \cdot 3 + 1 \quad &&\rightsquigarrow \quad [100]_3 = [1]_3, \\ 100 &= 16 \cdot 6 + 4 \quad &&\rightsquigarrow \quad [100]_6 = [4]_6, \\ 102 &= 34 \cdot 3 + 0 \quad &&\rightsquigarrow \quad [102]_3 = [0]_3, \\ 102 &= 17 \cdot 6 + 0 \quad &&\rightsquigarrow \quad [102]_6 = [0]_6. \end{aligned}$$

Restklassen

Lösung

(c) Beobachtung: Es kann **keine** Inklusion $[a]_3 \subseteq [b]_6$ gelten, denn:
Ist $x \in [a]_3$, so gilt auch $x + 3 \in [a]_3$, aber für $x \in [b]_6$ gilt: $x + 3 \notin [b]_6$.

Es sind also nur Inklusionen der folgenden Gestalt möglich: $[b]_6 \subseteq [a]_3$.
Mit Hilfe von (a) ergibt sich:

$$\begin{aligned} 0 \in [0]_6 &\subseteq [0]_3, \\ 1 \in [1]_6 &\subseteq [1]_3, \\ 2 \in [2]_6 &\subseteq [2]_3, \\ 3 \in [3]_6 &\subseteq [0]_3, \\ 4 \in [4]_6 &\subseteq [1]_3, \\ 5 \in [5]_6 &\subseteq [2]_3. \end{aligned}$$

Allgemein gilt: $[a]_6, [a+3]_6 \subseteq [a]_3$ für $a \in \{0, 1, 2\}$, denn:

$$[a + j \cdot 3]_6 = a + j \cdot 3 + 6\mathbb{Z} \subseteq a + j \cdot 3 + 3\mathbb{Z} = a + 3\mathbb{Z} = [a]_3.$$

Überblick

Einleitung

- Abbildungen spielen in der Mathematik eine sehr wichtige Rolle.
- In diesem Abschnitt werden die grundlegenden Definitionen und Notationen eingeführt.
- **Idee:** Eine Abbildung ist ein mathematisches Objekt, das festlegt, wie den Elementen einer Menge, dem sogenannten Definitionsbereich, Elemente einer anderen Menge, dem sogenannten Zielbereich, *zugeordnet* werden.
- Dabei muss die *Zuordnungsvorschrift* eindeutig sein, d.h. jedem Element des Definitionsbereichs darf höchstens ein Element des Zielbereichs zugeordnet werden.
- Damit ist der Begriff der Abbildung mit zwei Eigenschaften verknüpft:
  1. Existenz und
  2. Eindeutigkeit.

Links- und Rechtseindeutigkeit

Bevor wir zum Begriff der Abbildung kommen, werden wir die beiden Aspekte Existenz und Eindeutigkeit zunächst in allgemeiner Form für Relationen formulieren. Im Anschluss werden wir Abbildungen als spezielle Relationen definieren, die einer gewissen Existenz- und Eindeutigkeitsaussage genügen.

Wir beginnen mit dem Eindeutigkeitsbegriff.

Definition (Links- (Rechts)eindeutigkeit)

Seien M, N beliebige Mengen und $R \subseteq M \times N$ eine Relation.

R heißt links-(rechts)eindeutig falls gilt:

$$\forall x_1, x_2 \in M \, \forall y \in N : \big((x_1, y) \in R \wedge (x_2, y) \in R\big) \Rightarrow x_1 = x_2$$

$$\big(\forall y_1, y_2 \in N \, \forall x \in M : \big((x, y_1) \in R \wedge (x, y_2) \in R\big) \Rightarrow y_1 = y_2. \big)$$

Bemerkung

An einigen Stellen ist die folgende Variante der Definitionen besser geeignet:
R ist genau dann links-(rechts)eindeutig falls gilt:

$$\forall (x_1, y_1), (x_2, y_2) \in R : y_1 = y_2 \Rightarrow x_1 = x_2$$

$$\big(\forall (x_1, y_1), (x_2, y_2) \in R : x_1 = x_2 \Rightarrow y_1 = y_2. \big)$$

Links- und Rechtseindeutigkeit

Bemerkung

Linkseindeutigkeit kann man folgendermaßen im Pfeildiagramm visualisieren:

Wenn zwei Pfeile bei $y \in N$ ankommen, dann muss der Ausgangspunkt dieser zwei Pfeile identisch sein, also liegt eigentlich nur ein Pfeil vor.

Anders ausgedrückt: Bei jedem $y \in N$ kommt höchstens ein Pfeil an.

Entsprechend bedeutet Rechtseindeutigkeit:

Von jedem $x \in M$ geht höchstens ein Pfeil aus.

Links- und Rechtseindeutigkeit

Beispiele

(a) Die Relation $R := \{(1,2),(2,1),(2,3)\}$ ist linkseindeutig, aber nicht rechtseindeutig.

(b) Die Relation $R := \{(1,2),(2,1),(3,2)\}$ ist rechtseindeutig, aber nicht linkseindeutig.

(c) Die Relation $R := \{(1,1),(1,2),(2,2)\}$ ist weder links- noch rechtseindeutig.

(d) Die Relation $R := \{(1,2),(2,1),(3,3)\}$ ist links- und rechtseindeutig.

Links- und Rechtseindeutigkeit

Satz (Zusammenhang Links- und Rechtseindeutigkeit)

Seien M, N Mengen und $R \subseteq M \times N$ eine Relation.

R ist genau dann links-(rechts)eindeutig, wenn R^{-1} rechts-(links)eindeutig ist.

Satz (Verkettung und Eindeutigkeit)

Seien M, N, L Mengen und $R_1 \subseteq M \times N$ und $R_2 \subseteq N \times L$ links-(rechts)eindeutige Relationen.

Dann ist $R_1 R_2$ links-(rechts)eindeutig.

Links- und Rechtstotalität

Neben der Eindeutigkeit spielt **Existenz** bei der Definition von Abbildungen eine Rolle.

Definition (Links- (Rechts)totalität)

Seien M, N Mengen und $R \subseteq M \times N$ eine Relation. R heißt links-(rechts)total falls gilt:

$$\forall x \in M \, \exists y \in N : (x, y) \in R$$

$$\big(\forall y \in N \, \exists x \in M : (x, y) \in R \big).$$

Links- und Rechtstotalität

Satz (Zusammenhang Links- und Rechtstotalität)

Seien M, N beliebige Mengen und $R \subseteq M \times N$ eine Relation.
R ist genau dann links-(rechts)total, wenn R^{-1} rechts-(links)total ist.

Satz (Verkettung und totale Relationen)

Seien M, N, L beliebige Mengen und $R_1 \subseteq M \times N$ und $R_2 \subseteq N \times L$ links-(rechts)totale Relationen.

Dann ist $R_1 R_2$ links-(rechts)total.

(Beweis: Übungsaufgabe in moodle)

Links-/Rechtseindeutigkeit und Links-/Rechtstotalität

Aufgabe

Untersuchen Sie die folgenden Relationen $R \subseteq M \times N$ jeweils auf Links-/Rechtseindeutigkeit und Links-/Rechtstotalität.

1. $M := N := \{x \mid x \text{ ist Mensch}\}$, und für alle $x, y \in M$ definiere

   $$xRy :\Leftrightarrow y \text{ ist biologische Mutter von } x.$$

2. $M := \{0, 1, 2\}$, $N := \{1, 3\}$, und

   $$R := \{(x, y) \in M \times N \mid y - x = 1\}.$$

3. $M := N := \mathbb{N}$, und

   $$R := \{(n^2, n) \mid n \in \mathbb{N}\} = \{(k, n) \in \mathbb{N} \times \mathbb{N} \mid k = n^2\}.$$

4. $M := N := P(\{1, 2, 3\})$, und R sei die Inklusions-Relation $\subseteq$ auf M.

Links-/Rechtseindeutigkeit und Links-/Rechtstotalität

Lösung

1. R ist rechtseindeutig, denn jeder Mensch hat genau eine biologische Mutter,
   R ist nicht linkseindeutig, denn einige Frauen haben mehrere Kinder,
   R ist linkstotal, denn jeder Mensch hat eine biologische Mutter,
   R ist nicht rechtstotal, denn nicht jeder Mensch ist Mutter.
2. $R = \{(0,1),(2,3)\}$ ist links-, rechtseindeutig und rechtstotal, aber nicht linkstotal.
3. Linkseindeutigkeit:

   $\left[\text{z.z.: } \forall k_1, k_2 \in \mathbb{N} \forall n \in \mathbb{N} : \left((k_1, n) \in R \wedge (k_2, n) \in R\right) \Rightarrow k_1 = k_2\right]$

   Seien $k_1, k_2 \in \mathbb{N}$ und $n \in \mathbb{N}$. Es gelte: $(k_1, n) \in R$ und $(k_2, n) \in R$.
   Nach Definition von R gilt: $k_1 = n^2 = k_2$.

Links-/Rechtseindeutigkeit und Links-/Rechtstotalität

Lösung

Rechtseindeutigkeit:

$\left[\text{z.z.: } \forall n_1, n_2 \in \mathbb{N} \forall k \in \mathbb{N} : \left((k, n_1) \in R \wedge (k, n_2) \in R\right) \Rightarrow n_1 = n_2\right]$

Seien $n_1, n_2 \in \mathbb{N}$ und $k \in \mathbb{N}$. Es gelte: $(k, n_1) \in R$ und $(k, n_2) \in R$.
Nach Definition R gilt: $n_1^2 = k = n_2^2$. Also gilt:
$0 = n_1^2 - n_2^2 = \underbrace{(n_1 + n_2)}_{\geq 2 \neq 0} \cdot \underbrace{(n_1 - n_2)}_{=0}$. Also ist $n_1 = n_2$.

Rechtstotalität: nach Definition.
Nicht Linkstotalität: $(2, n) \notin R$ für alle $n \in \mathbb{N}$.

4. R ist weder links- noch rechtseindeutig, denn es gilt z.B. $(\emptyset, \emptyset), (\emptyset, \{1\}) \in R$ und $(\emptyset, \{1\}), (\{1\}, \{1\}) \in R$.

   R ist rechts- und linkstotal, denn R ist z.B. reflexiv, d.h. für alle $A \in M$ gilt $(A, A) \in R$.

Definition und Notationen

Definition (Abbildung)

Seien M, N beliebige Mengen. Eine Relation R zwischen M und N, d.h. $R \subseteq M \times N$, heißt Abbildung (oder auch Funktion) von M nach N, wenn R rechtseindeutig und linkstotal ist. Das heißt:

Zu jedem $x \in M$ existiert **genau ein** $y \in N$ so, dass $(x, y) \in R$ ist.

Mit Quantoren schreibt man dies so:

1. $\forall x \in M \, \exists y \in N : (x, y) \in R$,
2. $\forall (x_1, y_1), (x_2, y_2) \in R : x_1 = x_2 \Rightarrow y_1 = y_2$.

Bemerkung (Schreibweisen und Bezeichnungen)

Wenn R eine Abbildung von M nach N bezeichnet, schreibt man auch $R : M \to N$.

Ist $(x, y) \in R$, so nennt man y das Bild von x unter R und schreibt $R(x) := y$, und die Abbildung wird insgesamt notiert als $R : M \to N, x \mapsto R(x)$ (lies: „x wird abgebildet auf $R(x)$“).

Für Abbildungen verwendet man häufig auch kleine Buchstaben wie $f, g, \ldots$.

Wohldefiniertheit

Aufgabe

Auf $\mathbb{Z}$ definiere die Äquivalenzrelation $x \equiv y :\Leftrightarrow |x| = |y|$ für alle $x, y \in \mathbb{Z}$, und setze $M := \mathbb{Z}/\equiv \; = \{[x] \mid x \in \mathbb{Z}\}$. Welche der folgenden Relationen zwischen M und $\mathbb{Z}$ ist auch eine Abbildung von M nach $\mathbb{Z}$?

$$f := \{([x], x) \mid x \in \mathbb{Z}\}, \qquad g := \{([x], x^2) \mid x \in \mathbb{Z}\}.$$

Wohldefiniertheit

Lösung

[z.z.: f ist keine Abbildung, d.h.:
f ist nicht linkstotal oder f ist nicht rechtseindeutig]

Zur Linkstotalität:
$\left[\text{z.z.: } \forall [x] \in M \, \exists y \in \mathbb{Z} : ([x], y) \in f\right]$
Sei $[x] \in M$. Setze $y := x \in \mathbb{Z}$. Dann gilt: $([x], y) = ([x], x) \in f$.
Also ist f linkstotal.

Zur nicht Rechtseindeutigkeit:
$\Big[\text{z.z.: } \neg\big(\forall([x_1], y_1), ([x_2], y_2) \in f : [x_1] = [x_2] \Rightarrow y_1 = y_2\big)$, d.h.:
$\exists\,([x_1], y_1), ([x_2], y_2) \in f : [x_1] = [x_2] \wedge y_1 \neq y_2\Big]$
Setze $([x_1], y_1) := ([1], 1) \in f$ und $([x_2], y_2) := ([-1], -1) \in f$.
Dann gilt: $[x_1] = [1] = [-1] = [x_2]$ und $y_1 = 1 \neq -1 = y_2$.

Wohldefiniertheit

Lösung

[z.z.: g ist eine Abbildung, d.h.:
g ist linkstotal und g ist rechtseindeutig]

Zur Linkstotalität:
$\left[\text{z.z.: } \forall [x] \in M \, \exists y \in \mathbb{Z} : ([x], y) \in g\right]$
Sei $[x] \in M$. Setze $y := x^2 \in \mathbb{Z}$. Dann gilt: $([x], y) = ([x], x^2) \in g$.
Also ist g linkstotal.

Zur Rechtseindeutigkeit:
$\left[\text{z.z.: } \forall ([x_1], y_1), ([x_2], y_2) \in g : [x_1] = [x_2] \Rightarrow y_1 = y_2)\right]$
Seien $([x_1], y_1), ([x_2], y_2) \in g$. Dann gilt: $y_1 = x_1^2$ und $y_2 = x_2^2$.
Es gelte: $[x_1] = [x_2]$. Daraus folgt: $x_1 \equiv x_2$, d.h.: $|x_1| = |x_2|$, d.h.:
$y_1 = x_1^2 = |x_1|^2 = |x_2|^2 = x_2^2 = y_2$.

Wohldefiniertheit

Bemerkung (Wohldefiniertheit)

Die obige Situation tritt oft auf, wenn man Abbildungen definiert, deren Definitionsbereich $M = X/\equiv$ eine **Menge von Äquivalenzklassen** ist, und man die Abbildung **repräsentantenweise** definiert. Ist die entsprechende Relation rechtseindeutig (wie dies bei g der Fall ist), so sagt man auch, die Abbildung

$$g : M \to \mathbb{Z}, [x] \mapsto x^2$$

ist **wohldefiniert**, oder auch: Die Abbildungsvorschrift $[x] \mapsto x^2$ bzw. die Definition $g([x]) := x^2$ auf M ist **unabhängig vom Repräsentanten**.

Definitions- und Zielbereich, Bild

Definition (Definitionsbereich und Bild)

Sei $f : M \to N$ eine Abbildung von M nach N.

- Man nennt M den Definitionsbereich der Abbildung f und schreibt $\mathrm{Def}(f) := M$.
- N heißt Wertebereich oder auch Zielbereich der Abbildung.
- Unter dem Bild der Abbildung f versteht man die Menge aller Bildelemente, d.h. die Menge
$$\mathrm{Bild}(f) := \{y \in N \mid \exists x \in M : y = f(x)\}.$$
- Allgemeiner definiert man für jede Teilmenge $A \subseteq M$
$$f[A] := \{y \in N \mid \exists x \in A : y = f(x)\}$$
als das Bild von A unter der Abbildung f.

Definitions- und Zielbereich, Bild

Bemerkung (Gleichheit von Abbildungen)

Seien M, N, K, L Mengen und $f : M \to N$, $g : K \to L$ Abbildungen. Dann sind die Abbildungen f und g gleich genau dann, wenn gilt:

1. $M = K$ und $N = L$, das heißt, Definitions- und Zielbereich von f und g stimmen überein, und
2. $\forall x \in M : f(x) = g(x)$, das heißt, f und g stimmen auf dem Definitionsbereich punktweise überein.

Einschränkung von Abbildungen

Es kommt vor, dass man dieselbe Abbildungsvorschrift beibehalten, die Abbildung allerdings nur noch auf einer Teilmenge des Definitionsbereich betrachten möchte.

Definition (Einschränkung einer Abbildung)

Sei $f : M \to N$ eine Abbildung und $A \subseteq M$. Dann heißt $f|_A := f \cap (A \times N)$ die Einschränkung oder auch Restriktion von f auf A. Es handelt sich hierbei wiederum um eine Abbildung

$$f|_A : A \to N, x \mapsto f(x).$$

Injektivität/Surjektivität/Bijektivität

Definition (Sur-, In- und Bijektivität)

Eine Abbildung $f : M \to N$ heißt

- injektiv, wenn f linkseindeutig, $\left(\forall\, x_1, x_2 \in M : f(x_1) = f(x_2) \Rightarrow x_1 = x_2\right)$
- surjektiv, wenn f rechtstotal, $\left(\forall\, y \in N \exists\, x \in M : f(x) = y\right)$
- bijektiv, wenn f injektiv und surjektiv (also linkseindeutig und rechtstotal)

ist.

Injektive/Surjektive/Bijektive Abbildungen im Pfeildiagramm

Im Pfeildiagramm drücken sich die Eigenschaften injektiv/surjektiv/bijektiv einer Abbildung $f : M \to N$ folgendermaßen aus:

1. f ist injektiv genau dann, wenn jedes Element des Zielbereichs N von höchstens einem Pfeil getroffen wird.
2. f ist surjektiv genau dann, wenn jedes Element des Zielbereichs N von mindestens einem Pfeil getroffen wird.
3. f ist bijektiv genau dann, wenn jedes Element des Zielbereichs N von genau einem Pfeil getroffen wird.

Abbildungen

Aufgabe

Welche der folgenden Abbildungen ist injektiv/surjektiv/bijektiv?

1. $f : \mathbb{Z} \to \mathbb{N}_0, x \mapsto x^2$,
2. $g : \mathbb{N} \to \mathbb{Z}, x \mapsto x^2$,
3. $h : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}, (x, y) \mapsto x - y$.

Abbildungen

Lösung

1. $\left[\text{z.z.: } f \text{ ist nicht injektiv, d.h.: } \exists x_1, x_2 \in \mathbb{Z} : f(x_1) = f(x_2) \wedge x_1 \neq x_2\right]$
   Setze $x_1 := -1 \in \mathbb{Z}$ und $x_2 := 1 \in \mathbb{Z}$. Es gilt:
   $f(x_1) = f(-1) = (-1)^2 = 1 = 1^2 = f(1) = f(x_2)$ und $x_1 = -1 \neq 1 = x_2$.
   $\left[\text{z.z.: } f \text{ ist nicht surjektiv, d.h.: } \exists y \in \mathbb{N}_0 \, \forall x \in \mathbb{Z} : f(x) \neq y\right]$
   Setze $y := 2 \in \mathbb{N}_0$. Sei $x \in \mathbb{Z}$. Ist $|x| \leq 1$, so ist auch $x^2 = |x|^2 \leq 1^2 = 1$, und ist $|x| > 1$, so gilt $|x| \geq 2$ und damit $x^2 = |x|^2 \geq 2^2 = 4$, und damit in beiden Fällen insbesondere $f(x) = x^2 \neq 2 = y$.
   Insbesondere ist f nicht bijektiv.
2. $\left[\text{z.z.: } g \text{ ist injektiv, d.h.: } \forall x_1, x_2 \in \mathbb{N} : g(x_1) = g(x_2) \Rightarrow x_1 = x_2\right]$
   Seien $x_1, x_2 \in \mathbb{N}$. Es gelte: $g(x_1) = g(x_2)$, d.h.: $x_1^2 = x_2^2$. Es ergibt sich:
   $0 = x_1^2 - x_2^2 = \underbrace{(x_1 + x_2)}_{\geq 2 \neq 0} \cdot \underbrace{(x_1 - x_2)}_{=0}$, also $x_1 = x_2$.
   $\left[\text{z.z.: } g \text{ ist nicht surjektiv, d.h.: } \exists y \in \mathbb{Z} \, \forall x \in \mathbb{N} : g(x) \neq y\right]$
   Setze $y := -1 \in \mathbb{Z}$. Sei $x \in \mathbb{N}$. Es gilt: $g(x) = x^2 \geq 0$, also $g(x) \neq -1 = y$.
   Insbesondere ist g nicht bijektiv.

Abbildungen

Lösung

3. $\big[$z.z.: h ist nicht injektiv, d.h.:
$\exists (x_1, y_1), (x_2, y_2) \in \mathbb{N} \times \mathbb{N} : h(x_1, y_1) = h(x_2, y_2) \wedge (x_1, y_1) \neq (x_2, y_2)\big]$
Setze $(x_1, y_1) := (1, 1) \in \mathbb{N} \times \mathbb{N}$ und $(x_2, y_2) := (2, 2) \in \mathbb{N} \times \mathbb{N}$. Es gilt:
$h(x_1, y_1) = h(1, 1) = 1 - 1 = 0 = 2 - 2 = h(2, 2) = h(x_2, y_2)$ und
$(x_1, y_1) = (1, 1) \neq (2, 2) = (x_2, y_2)$.

   $\big[$z.z.: h ist surjektiv, d.h.: $\forall z \in \mathbb{Z}\, \exists (x, y) \in \mathbb{N} \times \mathbb{N} : h(x, y) = z\big]$
   Sei $z \in \mathbb{Z}$.

   1. Fall: $z \in \mathbb{N}_0$. Setze $(x, y) := (z + 1, 1) \in \mathbb{N} \times \mathbb{N}$. Es gilt:
   $h(x, y) = x - y = (z + 1) - 1 = z$.

   2. Fall: $z \leq -1$. Setze $(x, y) := (1, 1 - z)$. Wegen $z \leq -1$ ist dann
   $1 - z \geq 1 - (-1) = 2$, also ist $y \in \mathbb{N}$ und damit auch $(x, y) \in \mathbb{N} \times \mathbb{N}$.
   Es gilt: $h(x, y) = x - y = 1 - (1 - z) = z$.

   Insbesondere ist h nicht bijektiv.

Abbildungen

Satz (Abbildungen und Mächtigkeit)

Seien M, N endliche Mengen.

1. Gibt es eine injektive Abbildung $f : M \to N$, dann hat N mindestens so viele Elemente wie M.
2. Gibt es eine surjektive Abbildung $f : M \to N$, dann hat N höchstens so viele Elemente wie M.
3. Gibt es eine bijektive Abbildung $f : M \to N$, dann hat N genau so viele Elemente wie M.

Bemerkung (Gleichmächtigkeit von beliebigen Mengen)

Den vorhergehenden Satz nimmt man zum Anlass, auch für beliebige (möglicherweise unendliche) Mengen M, N die Begriffe „gleichmächtig“ und „gleichmächtig oder mächtiger“ zu definieren:

N heißt gleichmächtig zu M, wenn es eine bijektive Abbildung $f : M \to N$ gibt, und N heißt gleichmächtig oder mächtiger als M, wenn es eine injektive Abbildung $f : M \to N$ gibt.

Abbildungen

Ohne Beweis formulieren wir die folgende wichtige Charakterisierung endlicher Mengen:

Satz (Das Endlichkeitsprinzip)

Ein Menge M ist genau dann endlich, wenn für jede Abbildung $f : M \to M$ die folgenden Aussagen äquivalent sind:

(1) f ist injektiv.

(2) f ist surjektiv.

(3) f ist bijektiv.

Abbildungen

Verkettung von Abbildungen

Seien M, N, L Mengen und $f : M \to N$ und $g : N \to L$ Abbildungen. Nach den Sätzen *Verkettung und Eindeutigkeit* (Folie 118) und *Verkettung und totale Relationen* (Folie 120) ist auch die Verkettung $fg = g \circ f \subseteq M \times L$ wieder linkstotal und rechtseindeutig, also eine Abbildung.

Dabei gilt für alle $x \in M, z \in L$:

$$\begin{aligned} z = (g \circ f)(x) &\Leftrightarrow (x, z) \in fg \Leftrightarrow \exists\, y \in N : (x, y) \in f \wedge (y, z) \in g \\ &\Leftrightarrow \exists y \in N : y = f(x) \wedge z = g(y) \Leftrightarrow z = g(f(x)). \end{aligned}$$

Die zugehörige Abbildungsvorschrift lautet also

$$g \circ f : M \to L, x \mapsto g(f(x)).$$

und dies begründet die andere Reihenfolge der Notation von f und g bei der „Kringel“-Notation.

Man bezeichnet $g \circ f$ auch als die Hintereinanderausführung von f und g.

Abbildungen

Beispiel

Definiere $f : \mathbb{Z} \to \mathbb{N}_0, n \mapsto n^2$ und $g : \mathbb{N}_0 \to \mathbb{Z}, n \mapsto n - 1$.

Dann erhalten wir:

$g \circ f : \mathbb{Z} \to \mathbb{Z}$ mit $(g \circ f)(n) = g(f(n)) = g(n^2) = n^2 - 1$ für alle $n \in \mathbb{Z}$,

und

$f \circ g : \mathbb{N}_0 \to \mathbb{N}_0$ mit $(f \circ g)(n) = f(g(n)) = f(n-1) = (n-1)^2$ für alle $n \in \mathbb{N}_0$.

Insbesondere gilt: $g \circ f \neq f \circ g$.

Abbildungen

Eine weitere Folgerung aus den Sätzen *Verkettung und Eindeutigkeit* (Folie 118) und *Verkettung und totale Relationen* (Folie 120) ist:

Satz (Verkettung und Abbildungseigenschaften)

Seien M, N, L Mengen und $f : M \to N$ und $g : N \to L$ surjektive (bzw. injektive, bzw. bijektive) Abbildungen.

Dann ist

$$g \circ f : M \to L, x \mapsto g(f(x))$$

eine surjektive (bzw. injektive, bzw. bijektive) Abbildung.

Satz (Notwendige Bedingung für Sur- und Injektivität der Verkettung)

Seien M, N, L Mengen und $f : M \to N$ sowie $g : N \to L$ Abbildungen.

Ist $g \circ f : M \to L, x \mapsto g(f(x))$ eine surjektive (injektive) Abbildung, dann ist g surjektiv (f injektiv).

(Beweis: Übungsaufgabe in moodle)

Abbildungen

Aus der Definition der bijektiven Abbildung in Verbindung mit den Sätzen *Zusammenhang Links- und Rechtseindeutigkeit* (Folie 118) und *Zusammenhang Links- und Rechtstotalität* (Folie 120) ergibt sich folgender Satz:

Satz (Bijektive Abbildungen)

Eine Abbildung $f : M \to N$ ist genau dann bijektiv, wenn ihre Umkehrrelation $f^{-1} \subseteq N \times M$ eine Abbildung (von N nach M) ist.

Definition (Umkehrabbildung)

Ist die Abbildung $f : M \to N$ bijektiv, so nennt man die Abbildung $f^{-1} : N \to M$ die Umkehrabbildung von f.

Satz (Umkehrabbildung)

Ist die Abbildung $f : M \to N$ bijektiv, so gilt:

$$f^{-1} \circ f = \mathrm{Id}_M, \quad \text{und} \quad f \circ f^{-1} = \mathrm{Id}_N .$$

Abbildungen

Satz (Umkehrabbildung)

Sei $f : M \to N$ eine Abbildung. Gilt für eine Abbildung $g : N \to M$

$$g \circ f = \mathrm{Id}_M \qquad \text{und} \qquad f \circ g = \mathrm{Id}_N,$$

so ist g die Umkehrabbildung von f, d.h.: $f^{-1} := g$.

Beispiel

Betrachte die bijektive Abbildung $f : \mathbb{N} \to \mathbb{N}_0, n \mapsto n - 1$.

Dann ist die Umkehrabbildung von f gegeben durch

$$f^{-1} : \mathbb{N}_0 \to \mathbb{N}, m \mapsto m + 1.$$

Es gilt für alle $m \in \mathbb{N}_0$:

$$(f \circ f^{-1})(m) = f(f^{-1}(m)) = f(m+1) = m + 1 - 1 = m = \mathrm{Id}_{\mathbb{N}_0}(m).$$

Weiter gilt für alle $n \in \mathbb{N}$:

$$(f^{-1} \circ f)(n) = f^{-1}(f(n)) = f^{-1}(n-1) = n - 1 + 1 = n = \mathrm{Id}_{\mathbb{N}}(n).$$

Überblick

Einleitung

- Wir wollen das Lösen von Gleichungen mit mathematischen Mitteln von Grund auf untersuchen.
- Dabei muss zunächst beschrieben werden, was überhaupt eine Gleichung ist.
- Um das Problem mit einer in der Mathematik üblichen Allgemeinheit anpacken zu können, werden wir den Begriff der Verknüpfung einführen.
- Aus der Schule kennt man die Verknüpfungen Addition und Multiplikation von ganzen, rationalen und reellen Zahlen.
- Neben einer Lösungsformel interessieren den Mathematiker auch Existenz- und Eindeutigkeitssätze.
- Die Frage, welche Voraussetzungen man braucht, um generell gültige Existenz- und Eindeutigkeitssätze für das Lösen von Gleichungen zu erhalten, wird durch die Einführung der algebraischen Struktur der Gruppe beantwortet.

Einleitung

- Der mathematische Begriff der Gruppe hat auch viele andere Motivationen, die hier aber nicht angesprochen werden.
- Wir betrachten den Begriff der Gruppe in erster Linie als geeignete algebraische Struktur zur abstrakten Formulierung des Lösens von Gleichungen, insbesondere zur Behandlung von Existenz- und Eindeutigkeitssätzen.
- In den nächsten Abschnitten soll auch das Arbeiten mit Axiomensystemen geübt werden.
- Als Voraussetzung ist nur zugelassen, was in den Axiomen festgelegt ist oder was schon als Satz bewiesen wurde.

Überblick

Einleitung

- Um den Begriff einer Gleichung mathematisch allgemein formulieren zu können, starten wir mit einer Menge von Objekten, mit denen wir rechnen wollen.
- Dazu müssen zwei Dinge festliegen:
  - → Mit welchen Objekten wird gerechnet?
  - → Was bedeutet „Rechnen“ überhaupt?
- In der Schule lernt man, mit Zahlen zu rechnen.
- Wir verallgemeinern dies und lassen als Grundmenge beliebige Rechenobjekte zu.
  - → Das können Zahlen sein, müssen es aber nicht.
  - → Welcher Art diese Objekte sind, ist zunächst einmal egal: Murmeln, Mengen, Relationen, Abbildungen oder Zahlen.
  - → Wichtig ist nur, dass wir uns auf eine Menge der möglichen Rechenobjekte festlegen.

Einleitung

- Zahlen werden in der Schule addiert, multipliziert, subtrahiert und dividiert.
  - → Auch hier geht man von einer allgemeineren Sichtweise aus: Was Rechnen bedeutet, wird völlig offen gelassen, es ist nur wichtig, dass das Ergebnis immer eindeutig festgelegt ist.

Definition (Verknüpfung, algebraische Struktur)

Sei M eine beliebige nichtleere Menge. Eine Verknüpfung „$\circ$“ in der Menge M ist eine Abbildung $\circ : M \times M \to M$.

Für Verknüpfungen verwenden wir die sogenannte Infix Notation, das heißt, wir schreiben $x \circ y$ statt $\circ(x, y)$ für alle $x, y \in M$ ($x \circ y$ spricht man „x kringel y“).

Das Paar $(M, \circ)$ wird algebraische Struktur genannt (genauer: algebraische Struktur mit **einer** 2-stelligen Verknüpfung).

Verknüpfungen

Eine Verknüpfung liegt also dann vor, wenn je zwei Rechenobjekten immer genau ein Rechenergebnis in der Grundmenge zugeordnet wird.

Beispiele

1. Für $M := \mathbb{N}$ ist die Addition von natürlichen Zahlen eine Verknüpfung in $\mathbb{N}$. $(\mathbb{N}, +)$ ist also eine algebraische Struktur.
2. Für $M := \mathbb{Z}$ ist die Addition von ganzen Zahlen eine Verknüpfung in $\mathbb{Z}$. $(\mathbb{Z}, +)$ ist also eine weitere algebraische Struktur.
3. Für $M := \mathbb{N}$ ist die Subtraktion von natürlichen Zahlen **keine** Verknüpfung in $\mathbb{N}$, weil durch die Subtraktion der Bereich der natürlichen Zahlen verlassen wird.
4. Für $M := \mathbb{Z}$ ist die Substraktion von ganzen Zahlen eine Verknüpfung in $\mathbb{Z}$. $(\mathbb{Z}, -)$ ist also eine algebraische Struktur.
5. Sei X eine nichtleere Menge und $M := P(X \times X)$ die Menge aller Relationen auf X. Dann ist die Verkettung von Relationen eine Verknüpfung auf M. Also ist $(M, \circ)$ eine algebraische Struktur.

Verknüpfungen

Aus dem Rechnen mit Zahlen und aus der Diskreten Mathematik 1 sind die Assoziativ- und Kommutativgesetze bekannt. Im Kontext der algebraischen Struktur formuliert man:

Definition (Assoziativgesetz)

Die algebraische Struktur $(M, \circ)$ heißt assoziativ, falls gilt:

$$\forall x, y, z \in M : (x \circ y) \circ z = x \circ (y \circ z).$$

Definition (Kommutativgesetz)

Die algebraische Struktur $(M, \circ)$ heißt kommutativ, falls gilt:

$$\forall x, y \in M : x \circ y = y \circ x.$$

Verknüpfungen

Beispiele

1. $(\mathbb{Z}, +)$ ist assoziativ und kommutativ.
2. $(\mathbb{Z}, \cdot)$ ist assoziativ und kommutativ.
3. $(\mathbb{Z}, -)$ ist nicht assoziativ und nicht kommutativ.
4. $(\mathbb{Q} \setminus \{0\}, /)$ ist nicht assoziativ und nicht kommutativ.
5. Sei X eine mindestens 2-elementige Menge und $M := P(X \times X)$. Dann ist $(M, \circ)$ assoziativ und nicht kommutativ.

Verknüpfungen

Zur Beschreibung von algebraische Struktur kann man Verknüpfungstafeln verwenden.

Beispiel (Permutationen der Zahlen 1,2,3)

Es sei M die Menge aller Bijektionen $f : \{1,2,3\} \to \{1,2,3\}$ (solche Bijektionen bezeichnet man auch als Permutationen der Menge $\{1,2,3\}$). Die Hintereinanderausführung „$\circ$“ von Funktionen ist eine Verknüpfung in dieser Menge.

Diese Menge enthält die folgenden Elemente in der sogenannten Permutationsnotation:

$$\mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \tau_{23} := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_{13} := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\tau_{12} := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \rho_1 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Damit ergibt sich für die Verkettung folgende Verknüpfungstafel:

$\circ$	Id	τ_{23}	τ_{13}	τ_{12}	ρ_1	ρ_2
Id	Id	τ_{23}	τ_{13}	τ_{12}	ρ_1	ρ_2
τ_{23}	τ_{23}	Id	ρ_1	ρ_2	τ_{13}	τ_{12}
τ_{13}	τ_{13}	ρ_2	Id	ρ_1	τ_{12}	τ_{23}
τ_{12}	τ_{12}	ρ_1	ρ_2	Id	τ_{23}	τ_{13}
ρ_1	ρ_1	τ_{12}	τ_{23}	τ_{13}	ρ_2	Id
ρ_2	ρ_2	τ_{13}	τ_{12}	τ_{23}	Id	ρ_1

Verknüpfungen

Prinzip (Kommutativgesetz und Verknüpfungstafel)

Eine algebraische Struktur ist genau dann kommutativ, wenn die Verknüpfungstafel spiegelsymmetrisch an der Hauptdiagonalen ist.

Bemerkung

Leider gibt es keine einfache Methode, das Assoziativgesetz an der Verknüpfungstafel zu erkennen.

Verknüpfungen

Lösen von Gleichungen in algebraischen Strukturen

Wenn wir von dem Lösen einer Gleichung in einer algebraischen Struktur $(M, \circ)$ reden, gehen wir davon aus, dass wir bei gegebenen $a, b \in M$ ein $x \in M$ so suchen, dass

$$a \circ x = b, \quad \text{oder} \quad x \circ a = b.$$

Vorgegeben sind also das Ergebnis b und ein Operand a, und gesucht ist der zweite Operand x.

Bei algebraischen Strukturen, in denen kein Kommutativgesetz gilt, muss man zwischen dem Lösen einer Gleichung mit der Unbekannten rechts und einer Gleichung mit der Unbekannten links unterscheiden.

Verknüpfungen

Beispiele:

1. $M := \mathbb{Z}$ mit kommutativer Verknüpfung „$+$“:
   $5 + x = 7 \rightsquigarrow$ Lösung: $x = 2$.
2. $M := \mathbb{Z}$ mit nicht kommutativer Verknüpfung „$-$“:
   $5 - x = 7 \rightsquigarrow$ Lösung: $x = -2$,
   $x - 5 = 7 \rightsquigarrow$ Lösung: $x = 12$.
3. $M := \mathbb{Q}$ mit kommutativer Verknüpfung „$\cdot$“:
   $5 \cdot x = 7 \rightsquigarrow$ Lösung: $x = \frac{7}{5}$.

Verknüpfungen

Definition (Existenzsatz)

Sei $(M, \circ)$ eine algebraische Struktur. Wir sagen, dass ein rechts-(links)seitiger Existenzsatz für das Lösen von Gleichungen gilt, falls

$$\forall a, b \in M \; \exists x \in M : a \circ x = b,$$

$$(\forall a, b \in M \; \exists x \in M : x \circ a = b).$$

Wir sagen, dass ein Existenzsatz für das Lösen von Gleichungen gilt, falls ein rechts- und linksseitiger Existenzsatz gilt.

Definition (Eindeutigkeitssatz)

Sei $(M, \circ)$ eine algebraische Struktur. Wir sagen, dass ein rechts-(links)seitiger Eindeutigkeitssatz für das Lösen von Gleichungen gilt, falls

$$\forall a, b \in M \; \forall x_1, x_2 \in M : (a \circ x_1 = b \wedge a \circ x_2 = b) \Rightarrow x_1 = x_2,$$

$$(\forall a, b \in M \; \forall x_1, x_2 \in M : (x_1 \circ a = b \wedge x_2 \circ a = b) \Rightarrow x_1 = x_2).$$

Wir sagen, dass ein Eindeutigkeitssatz für das Lösen von Gleichungen gilt, falls ein rechts- und linksseitiger Eindeutigkeitssatz gilt.

Verknüpfungen

Beispiele

In den algebraischen Strukturen aus den Beispielen gelten folgende Sätze:

1. $(\mathbb{N}, +)$ erfüllt den Eindeutigkeitssatz, nicht aber den Existenzsatz.
2. $(\mathbb{Z}, +)$ erfüllt den Eindeutigkeitssatz und den Existenzsatz.
3. $(\mathbb{N}, \cdot)$ erfüllt den Eindeutigkeitssatz, nicht aber den Existenzsatz.
4. $(\mathbb{Z}, \cdot)$ erfüllt weder Eindeutigkeitssatz noch den Existenzsatz.
5. $(\mathbb{Q}_{>0}, \cdot)$ erfüllt sowohl den Eindeutigkeitssatz als auch den Existenzsatz.
6. $(\mathbb{Q}_{>0}, /)$ erfüllt sowohl den Eindeutigkeitssatz als auch den Existenzsatz.

Verknüpfungen

Prinzip (Existenzsatz und Verknüpfungstafel)

Sei $(M, \circ)$ eine algebraische Struktur.

Der Existenzsatz „$\forall a, b \in M \; \exists x \in M : a \circ x = b$“ ist genau dann richtig, wenn in jeder Zeile der Verknüpfungstafel jedes Element aus M mindestens einmal vorkommt.

Der Existenzsatz „$\forall a, b \in M \; \exists x \in M : x \circ a = b$“ ist genau dann richtig, wenn in jeder Spalte der Verknüpfungstafel jedes Element aus M mindestens einmal vorkommt.

Prinzip (Eindeutigkeitssatz und Verknüpfungstafel)

Sei $(M, \circ)$ eine algebraische Struktur.

Der Eindeutigkeitssatz
„$\forall a, b \in M \; \forall x_1, x_2 \in M : (a \circ x_1 = b \wedge a \circ x_2 = b) \Rightarrow x_1 = x_2$“ ist genau dann richtig, wenn in jeder Zeile der Verknüpfungstafel jedes Element aus M höchstens einmal vorkommt.

Der Eindeutigkeitssatz
„$\forall a, b \in M \; \forall x_1, x_2 \in M : (x_1 \circ a = b \wedge x_2 \circ a = b) \Rightarrow x_1 = x_2$“ ist genau dann richtig, wenn in jeder Spalte der Verknüpfungstafel jedes Element aus M höchstens einmal vorkommt.

Verknüpfungen

Beispiel

Setze $M := \{a, b, c, d\}$. Gegeben sei die algebraische Struktur

$\circ$	a	b	c	d
a	a	c	d	b
b	a	d	d	b
c	c	b	a	d
d	c	c	b	d

Betrachte die folgenden Gleichungen:

$a \circ x = a \rightsquigarrow$ eindeutige Lösung: $x = a$,
$a \circ x = b \rightsquigarrow$ eindeutige Lösung: $x = d$,
$a \circ x = c \rightsquigarrow$ eindeutige Lösung: $x = b$,
$a \circ x = d \rightsquigarrow$ eindeutige Lösung: $x = c$,
$b \circ x = a \rightsquigarrow$ eindeutige Lösung: $x = a$,
$b \circ x = b \rightsquigarrow$ eindeutige Lösung: $x = d$,
$b \circ x = c \rightsquigarrow$ keine Lösung,
$b \circ x = d \rightsquigarrow$ Lösungen: $x = b, c$,
$x \circ a = a \rightsquigarrow$ Lösungen: $x = a, b$,
$x \circ a = b \rightsquigarrow$ keine Lösung,
$x \circ a = c \rightsquigarrow$ Lösungen: $x = c, d$,
$x \circ a = d \rightsquigarrow$ keine Lösung.

Verknüpfungen

Kommt in einer Verknüpfungstafel einer endlichen algebraischen Struktur ein Element in einer Zeile nicht vor, so muss ein anderes doppelt vorkommen, weil es genauso viele Spalten wie Elemente gibt.

Aus demselben Grund muss auch ein Element fehlen, wenn ein anderes Element doppelt vorkommt.

Damit haben wir folgenden Satz bewiesen:

Satz (Existenz- und Eindeutigkeitssätze in endlichen Algebraischen Strukturen)

Sei $(M, \circ)$ eine endliche algebraische Struktur. Dann sind äquivalent:

$$\forall a, b \in M \; \exists x \in M : a \circ x = b$$

und

$$\forall a, b \in M \; \forall x_1, x_2 \in M : (a \circ x_1 = b \wedge a \circ x_2 = b) \Rightarrow x_1 = x_2.$$

Entsprechendes gilt, wenn die Unbekannte von links verknüpft wird.

Verknüpfungen

Aufgaben

1. Erfüllt die Menge der Bijektionen von $\{1, 2, 3\}$ mit der Verkettung einen Existenz- und Eindeutigkeitssatz?
2. Für alle $a, b \in \mathbb{Q}$ definiere als Verknüpfung den Mittelwert $a \circ b := \frac{a+b}{2}$. Ist $(\mathbb{Q}, \circ)$ eine algebraische Struktur? Wenn ja, welche Eigenschaften erfüllt sie?

Verknüpfungen

Lösung

1. Die Menge der Bijektionen von $\{1,2,3\}$ mit der Verkettung erfüllt die Existenz- und Eindeutigkeitssätze.

$\circ$	Id	τ_{23}	τ_{13}	τ_{12}	ρ_1	ρ_2
Id	Id	τ_{23}	τ_{13}	τ_{12}	ρ_1	ρ_2
τ_{23}	τ_{23}	Id	ρ_1	ρ_2	τ_{13}	τ_{12}
τ_{13}	τ_{13}	ρ_2	Id	ρ_1	τ_{12}	τ_{23}
τ_{12}	τ_{12}	ρ_1	ρ_2	Id	τ_{23}	τ_{13}
ρ_1	ρ_1	τ_{12}	τ_{23}	τ_{13}	ρ_2	Id
ρ_2	ρ_2	τ_{13}	τ_{12}	τ_{23}	Id	ρ_1

2. Zur algebraischen Struktur:
   $\circ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, (a,b) \mapsto \frac{a+b}{2}$ ist eine Abbildung, da
   $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, (a,b) \mapsto a+b$ und $h : \mathbb{Q} \to \mathbb{Q}, a \mapsto \frac{a}{2}$ Abbildungen sind, und $\circ = h \circ + = + h$.
   [Es reicht z.z.: $\forall a, b \in \mathbb{Q} : a \circ b \in \mathbb{Q}$]
   Offensichtlich gilt: $a \circ b = \frac{a+b}{2} \in \mathbb{Q}$ für alle $a, b \in \mathbb{Q}$.

Verknüpfungen

Lösung

Zur nicht Assoziativität: Seien $a, b, c \in \mathbb{Q}$. Es gilt:

$$(a \circ b) \circ c = \frac{a}{4} + \frac{b}{4} + \frac{c}{2} \overset{\text{i.a.}}{\neq} \frac{a}{2} + \frac{b}{4} + \frac{c}{4} = a \circ (b \circ c).$$

Konkretes Beispiel:
Setze $a := 8, b := 0, c := 4$. Dann gilt: $a \circ b = 4$, also
$(a \circ b) \circ c = 4 \circ 4 = 4$, und $b \circ c = 2$, also $a \circ (b \circ c) = 8 \circ 2 = 5$.

Zur Kommutativität: Seien $a, b \in \mathbb{Q}$.
Es gilt: $a \circ b = \frac{a+b}{2} = \frac{b+a}{2} = b \circ a$.

Zum Existenz- und Eindeutigkeitssatz: Seien $a, b \in \mathbb{Q}$.
Es gilt für alle $x \in \mathbb{Q}$:

$$a \circ x = b \Leftrightarrow \frac{a+x}{2} = b \Leftrightarrow x = 2b - a.$$

Damit gibt es genau eine Lösung und die Existenz- und Eindeutigkeitssätze gelten.

Verknüpfungen

Aufgaben

Gegeben ist eine unvollständige Verknüpfungstafel. Ergänzen Sie die Verknüpfungstafel so, dass sowohl Existenz als auch der Eindeutigkeitssätze für die Zeilen und die Spalten gelten.

$\circ$	a	b	c	d	e	f
a	e	c		f	a	d
b	d				b	
c				e		
d		f			d	a
e	a		c		e	f
f	c	d		b	f	

Verknüpfungen

Lösung

$\circ$	a	b	c	d	e	f
a	e	c	b	f	a	d
b	d	e	f	a	b	c
c	f	a	d	e	c	b
d	b	f	e	c	d	a
e	a	b	c	d	e	f
f	c	d	a	b	f	e

Überblick

Einleitung

- In diesem Abschnitt sollen die Restklassen als Rechenobjekte erschlossen werden.
- Das verwendete Konstruktionsprinzip ist ein sehr typisches Beispiel für die Thematik der Abstraktion.
- Abstraktionen ergeben nur dann Sinn, wenn die „Beziehungen“ unter den Objekten zu „Beziehungen“ zwischen den Äquivalenzklassen werden.

Definition (Restklassenaddition)

Sei $m \in \mathbb{N}$ ein fester Modulus. Für beliebige $a, b \in \mathbb{Z}$ definieren wir:

$$[a]_m \oplus [b]_m := [a + b]_m.$$

Restklassenoperationen

- Diese Definition hat eine Hürde: Die Summe zweier Restklasse wird über deren **Repräsentanten** definiert.
- Um sicherzustellen, dass es sich wirklich um eine Verknüpfung, also eine wohldefinierte Abbildung handelt, ist daher noch die **Unabhängigkeit** der Definition **von der Wahl der Repräsentanten** zu zeigen.
- Diese Thematik wurde bereits im Kapitel über Abbildungen erörtert. Wegen Ihrer zentralen Bedeutung wird sie an dieser Stelle nochmals als Prinzip festgehalten.

Prinzip (Unabhängigkeit vom Repräsentanten)

Legt man in einer Definition einer Eigenschaft von Äquivalenzklassen diese Eigenschaft durch den Rückgriff auf Repräsentanten fest, so muss man die Unabhängigkeit der Definition von der speziellen Wahl eines Repräsentanten beweisen.

Restklassenoperationen

Satz (Restklassenaddition)

Sei $m \in \mathbb{N}$. In der Menge $\mathbb{Z}_m$ der Restklassen modulo m ist $\oplus$ eine Verknüpfung, d.h. $(\mathbb{Z}_m, \oplus)$ ist eine algebraische Struktur.

Beispiel (Rechnen mit Vorteil)

Bei der Restklassenaddition hilft die geschickte Wahl eines Repräsentanten, Berechnungen einfacher zu gestalten:

- $[683]_2 \oplus [281]_2 = [1]_2 \oplus [1]_2 = [2]_2 = [0]_2$,
- $[34]_{12} \oplus [17]_{12} = [-2]_{12} \oplus [5]_{12} = [3]_{12}$,
- $[52]_{18} \oplus [52]_{18} = [-2]_{18} \oplus [-2]_{18} = [-4]_{18} = [14]_{18}$.

Restklassenoperationen

Bemerkung

Sei $a \in \mathbb{Z}$. Wiederholtes Addieren schreibt man auch als Multiplikation mit dem Wiederholungsfaktor $n \in \mathbb{N}$:

$$\underbrace{[a]_m \oplus [a]_m \oplus \ldots \oplus [a]_m}_{n\text{-mal}} =: n \cdot [a]_m.$$

Wie man leicht mit Induktion sieht, gilt für alle $n \in \mathbb{N}$:

$$n \cdot [a]_m = [n \cdot a]_m.$$

Beispiel

$13 \cdot [57]_{12} = 13 \cdot [-3]_{12} = [13 \cdot (-3)]_{12} = [-39]_{12} = [9]_{12}.$

Restklassenoperationen

Entsprechend der Restklassenaddition können wir auch die **Multiplikation** für Restklassen definieren.

Definition (Restklassenmultiplikation)

Sei $m \in \mathbb{N}$ ein fester Modulus. Für alle $a, b \in \mathbb{Z}$ definiere:

$$[a]_m \otimes [b]_m := [a \cdot b]_m.$$

Satz (Restklassenmultiplikation)

Sei $m \in \mathbb{N}$ ein fester Modulus. In der Menge $\mathbb{Z}_m$ der Restklassen modulo m ist $\otimes$ eine Verknüpfung, d.h. $(\mathbb{Z}_m, \otimes)$ ist eine algebraische Struktur.

Restklassenoperationen

Beispiel (Rechnen mit Vorteil)

Auch bei der Restklassenmultiplikation hilft die geschickte Wahl eines Repräsentanten Berechnungen zu vereinfachen:

- $[68]_{13} \otimes [28]_{13} = [3]_{13} \otimes [2]_{13} = [3 \cdot 2]_{13} = [6]_{13}$,
- $[34]_{12} \otimes [17]_{12} = [-2]_{12} \otimes [5]_{12} = [-2 \cdot 5]_{12} = [-10]_{12} = [2]_{12}$,
- $[52]_{18} \otimes [52]_{18} = [-2]_{18} \otimes [-2]_{18} = [-2 \cdot (-2)]_{18} = [4]_{18}$.

Bemerkung

Sei $a \in \mathbb{Z}$. Wiederholtes Multiplizieren schreibt man auch als Potenz mit dem Exponenten $n \in \mathbb{N}$:

$$\underbrace{[a]_m \otimes [a]_m \otimes \ldots \otimes [a]_m}_{n\text{-mal}} =: [a]_m^n.$$

Dann gilt für alle $n \in \mathbb{N}$:

$$[a]_m^n = [a^n]_m.$$

Restklassenoperationen

Beispiel ($[57]^3_{12}$)

$$[57]^3_{12} \quad = \quad [(-3)]^3_{12} = [(-3)^3]_{12} = [-27]_{12} = [9]_{12}.$$

Wenn die Unabhängigkeit vom Repräsentanten gezeigt ist, lassen sich sehr leicht Gesetze, die in den ganzen Zahlen gelten, auf die Restklassen übertragen:

Satz (Rechengesetze Restklassen)

Seien $m \in \mathbb{Z}$ ein fester Modulus und $a, b, c \in \mathbb{Z}$ beliebig. Dann gilt:

1. $[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$,
2. $\big([a]_m \oplus [b]_m\big) \oplus [c]_m = [a]_m \oplus \big([b]_m \oplus [c]_m\big)$,
3. $[a]_m \otimes [b]_m = [b]_m \otimes [a]_m$,
4. $\big([a]_m \otimes [b]_m\big) \otimes [c]_m = [a]_m \otimes \big([b]_m \otimes [c]_m\big)$.

Restklassenoperationen

Aufgabe 1

Erstellen Sie eine Verknüpfungstafel für $(\mathbb{Z}_6, \oplus)$.
Gelten Existenz- und Eindeutigkeitssätze?

Aufgabe 2

Berechnen Sie folgende Restklassenausdrücke. Geben Sie für das Ergebnis jeweils den kanonischen Repräsentanten aus $\{0, \ldots, m-1\}$ an.

1. $[57]_{13} \otimes [38]_{13}$,
2. $[23016]_{256} \otimes [1024]_{256}$,
3. $[26]_{57} \otimes [59]_{57}$,
4. $[58]_{57}^{12}$,
5. $[55]_{57}^{5} \otimes [60]_{57}$.

Restklassenoperationen

Aufgabe 3

(a) Erstellen Sie eine Verknüpfungstafel für $(\mathbb{Z}_6, \otimes)$.

(b) Welche der folgenden Gleichungen sind lösbar? Sind die Lösungen eindeutig?

1. $[3]_6 \otimes x = [2]_6$,
2. $[5]_6 \otimes x = [1]_6$,
3. $[5]_6 \otimes x = [3]_6$,
4. $[4]_6 \otimes x = [1]_6$,
5. $[4]_6 \otimes x = [2]_6$,
6. $[4]_6 \otimes x = [3]_6$.

(c) Wenn Sie die $[0]_6$ aus der Grundmenge $\mathbb{Z}_6$ herausnehmen, gelten dann die Existenz und Eindeutigkeitssätze?

Restklassenoperationen

Lösung zu Aufgabe 1

Wir notieren der Übersichtlichkeit halber statt der Restklasse $[a]_m$ nur den Repräsentanten a.

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Jedes Element steht in jeder Zeile (und Spalte) genau einmal, daher gelten Existenz- und Eindeutigkeitssatz.

Lösung von Gleichung $[a]_m \oplus x = [b]_m$ ist $x = [b - a]_m$.

Restklassenoperationen

Lösung zu Aufgabe 2

1. $[57]_{13} \otimes [38]_{13} = [5]_{13} \otimes [-1]_{13} = [-5]_{13} = [8]_{13}$,
2. $[23016]_{256} \otimes [1024]_{256} = [23016]_{256} \otimes [0]_{256} = [23016 \cdot 0]_{256} = [0]_{256}$,
3. $[26]_{57} \otimes [59]_{57} = [26]_{57} \otimes [2]_{57} = [52]_{57}$,
4. $[58]_{57}^{12} = [1]_{57}^{12} = [1^{12}]_{57} = [1]_{57}$,
5. $[55]_{57}^{5} \otimes [60]_{57} = [(-2)]_{57}^{5} \otimes [3]_{57} = [(-32) \cdot 3]_{57} = [-96]_{57} = [18]_{57}$.

Restklassenoperationen

Lösung zu Aufgabe 3

(a) Wir notieren der Übersichtlichkeit halber statt der Restklasse $[a]_m$ nur den Repräsentanten a.

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(b) Ablesen an der Verknüpfungstafel:

1. $[3]_6 \otimes x = [2]_6 \rightsquigarrow$ keine Lösung,
2. $[5]_6 \otimes x = [1]_6 \rightsquigarrow$ eindeutige Lösung $x = [5]_6$,
3. $[5]_6 \otimes x = [3]_6 \rightsquigarrow$ eindeutige Lösung $x = [3]_6$,
4. $[4]_6 \otimes x = [1]_6 \rightsquigarrow$ keine Lösung,
5. $[4]_6 \otimes x = [2]_6 \rightsquigarrow$ Lösungen $x = [2]_6, [5]_6$,
6. $[4]_6 \otimes x = [3]_6 \rightsquigarrow$ keine Lösung.

(c) Die Existenz- und Eindeutigkeitssätze gelten nicht, da nicht in jeder Zeile bzw. Spalte alle Elemente genau einmal vorkommen.

Überblick

Definition

Definition (Gruppe)

Eine algebraische Struktur $(G, \circ)$ heißt Gruppe, wenn gilt:

1. $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$. (Assoziativgesetz)
2. Es gibt ein $e \in G$ mit folgenden Eigenschaften:

   (a) $\forall a \in G : e \circ a = a$ (e ist linksneutrales Element von G),
   (b) $\forall a \in G \exists a' \in G : a' \circ a = e$ (Existenz linksinverser Elemente).

Bemerkung

In der Literatur wird in der Definition einer Gruppe häufig zusätzlich gefordert, dass e auch links- und rechtsneutral ist, dass also $e \circ a = a = a \circ e$ für alle $a \in G$ gilt, und dass für jedes $a \in G$ ein links- und rechtsinverses Element existiert, also ein $a' \in G$ mit $a' \circ a = e = a \circ a'$.

Wir werden zeigen, dass unsere Forderungen vollkommen ausreichen und wir die weiteren Forderungen aus unseren bisherigen ableiten können.

Die Gruppenaxiome

Bemerkung

Wir werden in der Vorlesung manchmal von den **vier Gruppenaxiomen** sprechen:

(G1) Dabei sehen wir die Abgeschlossenheit der Abbildung $\circ$ bezüglich G als unser erstes Axiom,

(G2) die Erfüllung des Assoziativgesetzes als zweites,

(G3) die Existenz eines linksneutralen Elementes als drittes Axiom

(G4) und die Existenz linksinverser Elemente als viertes Axiom an.

Bemerkung

Im Folgenden werden wir, solange keine Missverständnisse zu befürchten sind, für eine Gruppe $(G, \circ)$ nur G schreiben.

Gruppen und Verknüpfungstafeln

Prinzip (Gruppe und Verknüpfungstafel)

Die Axiome G3 und G4 kann man leicht an der Verknüpfungstafel erkennen:

Für G3: Zunächst prüft man, ob es eine Zeile gibt, in der genau die Tafelüberschrift steht.

Für G4: Dann prüft man, ob dieses Element in jeder Spalte vorkommt.

Beispiel (Gruppe der Bijektionen der Menge $\{1,2,3\}$)

Anhand der Gruppentafel (Folie 150) kann man erkennen, dass die Menge der Bijektionen der Menge $\{1,2,3\}$ die Forderungen der Gruppen-Definition erfüllt.

$\circ$	Id	τ_{23}	τ_{13}	τ_{12}	ρ_1	ρ_2
Id	Id	τ_{23}	τ_{13}	τ_{12}	ρ_1	ρ_2
τ_{23}	τ_{23}	Id	ρ_1	ρ_2	τ_{13}	τ_{12}
τ_{13}	τ_{13}	ρ_2	Id	ρ_1	τ_{12}	τ_{23}
τ_{12}	τ_{12}	ρ_1	ρ_2	Id	τ_{23}	τ_{13}
ρ_1	ρ_1	τ_{12}	τ_{23}	τ_{13}	ρ_2	Id
ρ_2	ρ_2	τ_{13}	τ_{12}	τ_{23}	Id	ρ_1

Das Assoziativgesetz für die Verkettung von Relationen wurde in Satz „Assoziativgesetz Verkettung“ (Folie 22) bewiesen. Damit ist die Menge der Bijektionen der Menge $\{1,2,3\}$ eine Gruppe. Diese wird im folgenden mit S_3 bezeichnet.

Die symmetrische Gruppe

Satz (Symmetrische Gruppe)

Sei X eine Menge. Wir betrachten die Menge aller bijektiven Abbildungen von X auf sich selbst, d.h. die Menge

$$S(X) := \{f : X \to X \mid f \text{ bijektiv}\}.$$

Die Menge $S(X)$ mit der Verkettung von Funktionen ist eine Gruppe.

G1: Abgeschlossenheit:
Folgt aus Satz „Verkettung und Abbildungseigenschaften“ Folie 140.

G2: Assoziativgesetz:
Folgt aus Satz „Assoziativgesetz Verkettung“ Folie 22.

G3: Neutrales Element: $\mathrm{Id}_X : X \to X, x \mapsto x$.

G4: Inverse Elemente:
Zu $f \in S(X)$ ist die Umkehrabbildung f^{-1} inverses Element (siehe F.141).

Abelsche Gruppen und Beispiele

Definition (Abelsche Gruppe)

Ist G eine Gruppe und gilt ferner noch das Kommutativgesetz

$$a \circ b = b \circ a \text{ für alle } a, b \in G,$$

so heißt G kommutative Gruppe oder auch abelsche Gruppe. Anstatt von „$\circ$“ verwendet man dann meist „$+$“.

Beispiele

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sind abelsche Gruppen (linksneutrales Element der Addition ist 0, linksinverses Element zu a ist $-a$), $(\mathbb{N}_0, +)$ aber nicht, da es für $0 \neq a \in \mathbb{N}_0$ kein linksinverses Element bezüglich der Addition in $\mathbb{N}_0$ gibt.
2. $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{C}\backslash\{0\}, \cdot)$ sind abelsche Gruppen (mit 1 als linksneutralem Element und $\frac{1}{a}$ als linksinversem Element zu a).
3. $(\{0\}, +)$ und $(\{1\}, \cdot)$ sind abelsche Gruppen.
4. Die Gruppe $(S_3, \circ)$ ist nicht kommutativ.

Beispiel: $(\mathbb{Z}_3, \oplus)$

Bei Verknüpfungen auf „kleinen“ Mengen, wie etwa $(\mathbb{Z}_3, \oplus)$, erstellt man häufig Verknüpfungstafeln. Wir notieren der Übersichtlichkeit halber statt der Restklasse $[a]_3$ in der Verknüpfungstafel nur den kanonischen Repräsentanten a:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Diese Verknüpfungstafel verrät uns folgendes:

G1: $\mathbb{Z}_3$ ist bezüglich $\oplus$ abgeschlossen,

G3: $[0]_3$ ist das linksneutrale Element,

G4: $[2]_3$ das linksinverse Element zu $[1]_3$, $[1]_3$ das linksinverse Element zu $[2]_3$ und $[0]_3$ das linksinverse Element zu sich selbst.

Die Tatsache, dass die Verknüpfungstafel spiegelsymmetrisch zu ihrer Hauptdiagonalen ist, bedeutet, dass das Kommutativgesetz gilt.
Das Assoziativgesetz (G2) wurde auf Folie 170 allgemein bewiesen.

Die Gruppe $(\mathbb{Z}_m, \oplus)$

Satz (Restklassengruppe mit Addition)

Sei $m \in \mathbb{N}$ ein fester Modulus. Dann ist $(\mathbb{Z}_m, \oplus)$ eine kommutative Gruppe.

G2: Das Assoziativgesetz „erbt“ man vom Assoziativgesetz der ganzen Zahlen (vgl. Folie 170, Rechengesetze Restklassen).

G3: Das neutrale Element ist $[0]_m$.

G4: Das inverse Element zur Restklasse $[a]_m$ ist die Restklasse $[-a]_m$.

- Das Kommutativgesetz „erbt“ man wiederum vom Kommutativgesetz der ganzen Zahlen (vgl. Folie 170, Rechengesetze Restklassen).

Elementare Gruppeneigenschaften

Aus der Definition folgen für eine Gruppe G die Eigenschaften:

Satz (Elementare Gruppeneigenschaften)

Sei $(G, \circ)$ eine Gruppe.

1. Sei $e \in G$ linksneutrales Element und $a, a' \in G$ so, dass $a' \circ a = e$. Dann gilt auch $a \circ a' = e$. Man nennt a' dann nur noch ein inverses Element zu a.
2. Sei $e \in G$ linksneutrales Element. Dann gilt $a \circ e = a$ für alle $a \in G$ und man nennt e dann ein neutrales Element.
3. Es gibt genau ein neutrales Element $e \in G$.
4. Zu jedem $a \in G$ gibt es genau ein inverses Element $a' \in G$ (welches dann mit a^{-1} bezeichnet wird).
5. $\forall a \in G : (a^{-1})^{-1} = a$.
6. $\forall a, b \in G : (a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Gruppen und Lösen von Gleichungen

Satz (Charakterisierung Gruppe)

Eine assoziative algebraische Struktur $(G, \circ)$ ist genau dann eine Gruppe, wenn $G \neq \emptyset$ ist und in $(G, \circ)$ der Existenzsatz für Gleichungen gilt, wenn also gilt:

1. Die Gleichung $a \circ x = b$ ist für alle $a, b \in G$ in G lösbar.
2. Die Gleichung $x \circ a = b$ ist für alle $a, b \in G$ in G lösbar.

Satz (Eindeutigkeit der Lösbarkeit von Gleichungen)

Sei $(G, \circ)$ eine beliebige Gruppe. Dann gilt:

1. Es gibt für alle $a, b \in G$ höchstens eine Lösung der Gleichung $a \circ x = b$.
2. Es gibt für alle $a, b \in G$ höchstens eine Lösung der Gleichung $x \circ a = b$.

Gruppen und Lösen von Gleichungen

Der im Beweis verwendete Schluss wird beim Rechnen in Gruppen oft benutzt und daher extra notiert:

Satz (Kürzungsregel in Gruppen)

Sei $(G, \circ)$ eine Gruppe. Dann gilt für alle $a, b_1, b_2 \in G$:

$$a \circ b_1 = a \circ b_2 \Rightarrow b_1 = b_2, \quad \text{und} \quad b_1 \circ a = b_2 \circ a \Rightarrow b_1 = b_2.$$

Durch Kombination der beiden Sätze von Folie 184 erhält man außerdem den folgenden

Satz (Existenzsatz $\Rightarrow$ Eindeutigkeitssatz)

Sei $(G, \circ)$ eine assoziative algebraische Struktur, in der der Existenzsatz für Gleichungen gilt. Dann gilt auch der Eindeutigkeitssatz für Gleichungen.

Gruppen und Lösen von Gleichungen

Eine weitere Folgerung aus den Sätzen von Folie 184 ist

Satz (Existenz und Eindeutigkeit von Lösungen)

In einer Gruppe besitzt jede Gleichung **genau eine** Lösung.

- Die Tatsache, dass $(\mathbb{N}_0, +)$ keine Gruppe darstellt, spiegelt sich zum Beispiel in der Tatsache wider, dass kein $x \in \mathbb{N}_0$ existiert, welches die Gleichung $1 + x = 0$ erfüllt.
- Dies ist natürlich nichts anderes als das von uns schon angesprochene Fehlen inverser Elemente bezüglich der Addition in $\mathbb{N}_0$.
- Um jedoch jede Gleichung, die uns begegnen könnte, lösen zu können, haben wir unseren „Zahlenbegriff“ immer wieder erweitert:
  $(\mathbb{N}, +) \rightsquigarrow (\mathbb{Z}, +)$, $(\mathbb{N}, \cdot) \rightsquigarrow (\mathbb{Q}^+, \cdot)$, ...

Ordnung einer Gruppe

Definition (Ordnung einer Gruppe)

Unter der Ordnung einer Gruppe versteht man die Anzahl ihrer Elemente.
Für die Ordnung einer Gruppe G schreibt man $|G|$ oder $\operatorname{ord}(G)$.

Beispiel

- Die Gruppe S_3 hat die Ordnung 6.
- Die Gruppe $(\mathbb{Z}_m, \oplus)$ hat die Ordnung m.
- Sei X eine unendliche Menge. Die Gruppe $\big(S(X), \circ\big)$ hat die Ordnung ∞.

Aufgaben

Aufgabe 1

Setze $G := \mathbb{Q}\backslash\{1\}$, und definiere auf G die Verknüpfung

$$x \circ y := x + y - xy \quad \text{für alle } x, y \in G.$$

In moodle wird als Aufgabe gestellt werden, dass G eine Gruppe ist mit neutralem Element 0.
Bestimmen Sie für alle $x \in G$ das inverse Element.

Aufgabe 2

Es sei M eine Menge und $G := P(M)$. Auf G betrachten wir als Verknüpfung die *symmetrische Differenz*

$$A \Delta B = (A \backslash B) \cup (B \backslash A) = (A \cup B) \backslash (A \cap B).$$

In Disk. Math. 1 wurde das Assoziativgesetz $(A \Delta B) \Delta C = A \Delta (B \Delta C)$ für alle Mengen A, B, C gezeigt.

(a) Geben Sie für $M := \{0, 1\}$ die Verknüpfungstafel von (G, Δ) an.

(b) Zeigen Sie, dass (G, Δ) eine kommutative Gruppe ist.

Aufgaben

Lösung zu Aufgabe 1

Sei $x \in \mathbb{Q}\backslash\{1\}$. Auflösen $x \circ x^{-1} = 0$ nach x^{-1} führt auf:

$$x \circ x^{-1} = 0 \quad \Leftrightarrow \quad x + x^{-1} - xx^{-1} = 0 \Leftrightarrow \; -x = (1-x)x^{-1} \Leftrightarrow x^{-1} = \frac{x}{x-1}.$$

Setze also $x^{-1} := \frac{x}{x-1}$. Dann ist $x^{-1} \in G$, denn

$$x^{-1} = 1 \Leftrightarrow \frac{x}{x-1} = 1 \Leftrightarrow x = x - 1 \Leftrightarrow 0 = -1,$$

also gilt $x^{-1} \neq 1$, und es gilt

$$x^{-1} \circ x = \frac{x}{x-1} + x - \frac{x^2}{x-1} = \frac{x + x(x-1) - x^2}{x-1} = 0.$$

Aufgaben

Lösung zu Aufgabe 2

(a) Es ist $M := \{0, 1\}$ und $G := P(M) = \{\emptyset, \{0\}, \{1\}, M\}$.

Δ	$\emptyset$	$\{0\}$	$\{1\}$	M
$\emptyset$	$\emptyset$	$\{0\}$	$\{1\}$	M
$\{0\}$	$\{0\}$	$\emptyset$	M	$\{1\}$
$\{1\}$	$\{1\}$	M	$\emptyset$	$\{0\}$
M	M	$\{1\}$	$\{0\}$	$\emptyset$

(b) (G1) Es gilt: $A \Delta B = (A \cup B) \setminus (A \cap B) \subseteq M$ für alle $A, B \subseteq M$. Also gilt: $A \Delta B \in G$ für alle $A, B \in G$.

(G2) Disk. Math. 1.

(G3) $\emptyset$ ist das neutrale Element, denn:
$\emptyset \Delta A = (A \backslash \emptyset) \cup (\emptyset \backslash A) = A$ für alle $A \in G$.

(G4) Zu $A \in G$ ist das inverse Element $A^{-1} = A$, denn:
$A \Delta A = (A \backslash A) \cup (A \backslash A) = \emptyset$.
Kommutativgesetz: Nach Disk. Math. 1 gilt:
$A \Delta B = (A \backslash B) \cup (B \backslash A) = (B \backslash A) \cup (A \backslash B) = B \Delta A$.

Überblick

Restklassenmultiplikation

- Bisher: Restklassengruppe $(\mathbb{Z}_m, \oplus)$ mit **Addition**
- In diesem Abschnitt: $(\mathbb{Z}_m, \otimes)$ mit **Multiplikation**
- Kandidat für neutrales Element bzgl. Multiplikation: $[1]_m$
- Problem: $[0]_m$ kann kein inverses Element besitzen
  $\rightsquigarrow$ bzgl. Multiplikation betrachten wir nur die Menge $\mathbb{Z}_m \setminus \{[0]_m\}$

Zum besseren allgemeinen Verständnis betrachten wir zunächst zwei Beispiele, die alle möglichen Phänomene aufweisen.

Restklassenmultiplikation

Beispiel $\left(\text{Restklassenmultiplikation in } \mathbb{Z}_5 \setminus \{[0]_5\}\right)$

Wir notieren der Übersichtlichkeit halber statt der Restklasse $[a]_5$ in der Verknüpfungstafel nur den kanonischen Repräsentanten a.

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Man kann an der Verknüpfungstafel erkennen, dass die Existenzforderung eines linksneutralen Elements und linksinverser Elemente aus der Definition „Gruppe“ erfüllt sind. Es handelt sich also um eine Gruppe.

Hinweis: In den ganzen Zahlen $(\mathbb{Z}, \cdot)$ gibt es zu der Zahl 3 kein inverses Element, denn $\frac{1}{3}$ ist keine ganze Zahl. Wenn man jedoch modulo 5 rechnet, findet man, dass $[2]_5$ multiplikatives Inverses zu $[3]_5$ ist, denn $[2]_5 \otimes [3]_5 = [1]_5$. Tatsächlich zeigt die Verknüpfungstafel, dass jede Zahl $1, 2, 3, 4$ ein multiplikativ Inverses modulo 5 besitzt.

Restklassenmultiplikation

Beispiel $\left(\text{Restklassenmultiplikation in } \mathbb{Z}_6 \setminus \{[0]_6\}\right)$

Wir notieren der Übersichtlichkeit halber statt der Restklasse $[a]_6$ in der Verknüpfungstafel nur den kanonischen Repräsentanten a.

$\otimes$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Man kann an der Verknüpfungstafel erkennen, dass nicht einmal eine algebraische Struktur vorliegt, denn das Verknüpfungsergebnis von $[2]_6$ und $[3]_6$ liegt nicht in der Menge $\mathbb{Z}_6 \setminus \{[0]_6\}$.

Bemerkung

Wir werden sehen, dass die Gruppeneigenschaft damit zu tun haben wird, dass der Modulus m eine Primzahl ist.

Größter gemeinsamer Teiler

Als nächstes soll beantwortet werden, wann eine Restklasse modulo m ein multiplikatives Inverses besitzt.

Aus der Schule ist für natürliche Zahlen $a, b \in \mathbb{N}$ der größte gemeinsame Teiler $\mathrm{ggT}(a, b)$ bekannt. Man lernt, den ggT zweier Zahlen durch Primfaktorzerlegung zu ermitteln:

Beispiel (ggT durch Primfaktorzerlegung)

Es ist der $\mathrm{ggT}(240, 420)$ zu bestimmen. Dazu zerlegt man die Zahlen in Primfaktoren:

$$240 = 2^4 \cdot 3 \cdot 5,$$

$$420 = 2^2 \cdot 3 \cdot 5 \cdot 7.$$

Der ggT wird durch die gemeinsamen Primfaktoren bestimmt:

$$\mathrm{ggT}(240, 420) = 2^2 \cdot 3 \cdot 5 = 60.$$

Hinweis: Primfaktorzerlegung und ggT können mit dem NAK-TR berechnet werden (FACT, GCD).

Größter gemeinsamer Teiler

- Leider ist aus algorithmischer Sicht die Primfaktorzerlegung ein sehr schwieriges Problem.
  - → Werden die Zahlen größer, ist es sehr schwer, Primfaktoren zu finden.
- Kryptographische Verfahren beruhen darauf, dass es praktisch unmöglich ist (also viel zu lange dauert), eine große Zahl in ihre Primfaktoren zu zerlegen, wenn diese Primfaktoren selbst große Zahlen sind.
- Zum Glück gibt es zur Primfaktorzerlegung Alternativen zur Berechnung des größten gemeinsamen Teiler, die algorithmisch sogar sehr leicht umzusetzen sind.
  - → Euklidischer Algorithmus.

Größter gemeinsamer Teiler

Wir starten mit der formalen Definition des größten gemeinsamen Teilers.

Definition (größter gemeinsamer Teiler)

Seien $a, b \in \mathbb{Z}$ nicht beide gleich 0 und sei $g \in \mathbb{N}$. Dann heißt g größter gemeinsamer Teiler von a und b (Notation: $g = \mathrm{ggT}(a, b)$) genau dann, wenn

1. $g \mid a \wedge g \mid b$, und
2. $\forall c \in \mathbb{Z} : \big(c \mid a \wedge c \mid b\big) \Rightarrow c \mid g$.

Satz (größter gemeinsamer Teiler)

Seien $a, b \in \mathbb{Z}$ nicht beide gleich 0. Dann besitzen a, b genau einen größten gemeinsamen Teiler.

Existenzbeweis (ohne Primfaktorzerlegung): später auf Folie 203.

Bemerkung (größter gemeinsamer Teiler)

Seien $a, b \in \mathbb{Z}$ nicht beide gleich 0. Dann ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|) = \inf\{|a|, |b|\}$ bzgl. der Ordnungsrelation „$|$“ auf $\mathbb{N}_0$.

Größter gemeinsamer Teiler

Grundlage des euklidischen Algorithmus ist der folgende Satz.

Satz (Invarianz größter gemeinsamer Teiler)

Es seien $a, b \in \mathbb{Z}$ nicht beide gleich 0 und $k \in \mathbb{Z}$, dann gilt

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a, b + ka).$$

Folgerung

Es seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Durch Teilen mit Rest finden wir eindeutig bestimmte $q, r \in \mathbb{Z}$ mit

$$a = q \cdot b + r \quad \text{und} \quad 0 \leq r < |b|.$$

Dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.

Notation (Rest nach ganzzahliger Division)

In der obigen Situation verwenden wir für den Rest nach ganzzahliger Division die Notation $a \mod b := r$. Es gilt also $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a \mod b)$

Euklidischer Algorithmus

Idee des euklidischen Algorithmus zum Finden des ggT:

- Man startet mit zwei Zahlen $a, b \in \mathbb{N}$, wobei wir die Bezeichnung so wählen, dass a die größere Zahl ist.
- Nun führt man eine Division mit Rest durch und erhält $a = q \cdot b + r$.
- Nach der Folgerung (F.197) ist der gesuchte ggT der Zahlen a, b gleich dem ggT der Zahlen b, r, wobei $b < a$ und $r < b$ ist.
- Dieses Verfahren kann man iterieren, wobei der Rest in jedem Schritt echt kleiner wird.
- Schließlich erhält man in einem letzten Schritt den Rest 0.
  Die kleinere der beiden zuletzt verwendeten Zahlen ist dann der gesuchte ggT.

Euklidischer Algorithmus

Bevor wir den Algorithmus formal notieren, betrachten wir ein Beispiel.

Beispiel (Euklids Algorithmus)

Wir wollen den $\mathrm{ggT}(1547, 560)$ bestimmen. Dazu rechnen wir:

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ 560 &= 1 \cdot 427 + 133 \\ 427 &= 3 \cdot 133 + 28 \\ 133 &= 4 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7 \\ 21 &= 3 \cdot 7 + 0. \end{aligned}$$

Damit ist klar: $\mathrm{ggT}(1547, 560) = \mathrm{ggT}(21, 7) = 7$.

Euklidischer Algorithmus

Der euklidische Algorithmus

Start: Zahlen $a, b \in \mathbb{N}$ mit $a > b$. Setze $a_1 := a$ und $b_1 := b$ und $i := 1$.

i-ter Schritt: Führe Division mit Rest durch:

$$a_i = q_i \cdot b_i + r_i.$$

- Falls $r_i = 0$. $\rightsquigarrow$ Abbruch: $\mathrm{ggT}(a, b) = b_i$.
- Falls $r_i \neq 0$. Setze $a_{i+1} := b_i$, $b_{i+1} := r_i$ und führe nächste Iteration mit $i + 1$ durch.

Nach Konstruktion gilt in jedem Schritt

$$\mathrm{ggT}(a_{i+1}, b_{i+1}) = \mathrm{ggT}(b_i, a_i - qb_i) = \mathrm{ggT}(a_i, b_i),$$

induktiv folgt also $\mathrm{ggT}(a_i, b_i) = \mathrm{ggT}(a, b)$ in jedem Schritt i, was die Korrektheit des Algorithmus zeigt. Außerdem werden die Zahlen a_i, b_i, r_i in jedem Schritt echt kleiner, was zeigt, dass der Algorithmus nach endlicher Zeit terminiert.

Euklidischer Algorithmus

Tabellarische Notation des euklidischen Algorithmus

Wir zeigen anhand eines Beispiels die typische tabellarische Notation zur Bestimmung des ggT:

Gesucht ist der ggT von $a := 130$ und $b := 35$.

a	b	q
130	35	3
35	25	1
25	10	2
10	5	2
5	0	

Damit erhalten wir $\mathrm{ggT}(130, 35) = 5$.

Euklidischer Algorithmus

Aufgabe

Bestimmen Sie $\mathrm{ggT}(420, 595)$ und $\mathrm{ggT}(420, 594)$ mithilfe des Euklidischen Algorithmus.

Lösung

a	b	q
595	420	1
420	175	2
175	70	2
70	35	2
35	0	

Es gilt also $\mathrm{ggT}(420, 595) = 35$.

a	b	q
594	420	1
420	174	2
174	72	2
72	30	2
30	12	2
12	6	2
6	0	

Es gilt also $\mathrm{ggT}(420, 594) = 6$.

Restklassen

Der nächste Satz enthält genau die Aussage, die erforderlich ist, um in multiplikativen Restklassenstrukturen zu invertieren.

Satz von Bézout

Seien $a, b \in \mathbb{Z}$ nicht beide gleich 0. Dann gibt es $s, t \in \mathbb{Z}$ mit

$$\mathrm{ggT}(a, b) = s \cdot a + t \cdot b.$$

Insbesondere existiert der $\mathrm{ggT}(a, b)$.

Beispiel (Satz von Bézout)

Wir wissen, dass $\mathrm{ggT}(1547, 560) = 7$ ist. Der Satz von Bézout sagt, dass sich 7 in der Form $s \cdot 1547 + t \cdot 560$ schreiben lässt. $\rightsquigarrow$ Wie findet man s und t?

Man rechnet den euklidischen Algorithmus rückwärts!

$$\begin{aligned}
7 &= 28 - 1 \cdot 21 &&= 28 - 1 \cdot (133 - 4 \cdot 28) \\
&= 5 \cdot 28 - 1 \cdot 133 &&= 5 \cdot (427 - 3 \cdot 133) - 1 \cdot 133 \\
&= 5 \cdot 427 - 16 \cdot 133 &&= 5 \cdot 427 - 16 \cdot (560 - 1 \cdot 427) \\
&= 21 \cdot 427 - 16 \cdot 560 &&= 21 \cdot (1547 - 2 \cdot 560) - 16 \cdot 560 \\
&= 21 \cdot 1547 - 58 \cdot 560.
\end{aligned}$$

Erweiterter Euklidischer Algorithmus

Übersichtlicher lässt sich dies mit dem sogenannten erweiterten euklidischen Algorithmus in einer Tabelle bewerkstelligen:

1. Im ersten Schritt wird der euklidische Algorithmus bis zum Abbruchkriterium (Rest $= 0$) in einer Tabelle ausgeführt.
2. Anschließend wird die Tabelle um die Spalten „s“ und „t“ erweitert, und in die letzte Zeile wird $s = 1$ und $t = 0$ eingetragen.
3. Nun werden schrittweise in jeder Zeile die Werte s und t aus den „alten“ s und t der Zeile darunter berechnet gemäß:

$$s_{\text{neu}} := t_{\text{alt}} \quad \text{und} \quad t_{\text{neu}} := s_{\text{alt}} - q_{\text{neu}} \cdot t_{\text{alt}}.$$

   In jeder Zeile gilt dann: $\operatorname{ggT}(a, b) = s \cdot a + t \cdot b$.
4. Ist man schließlich wieder in der ersten Zeile angekommen, so erhält man wie gewünscht s, t mit $\operatorname{ggT}(a, b) = s \cdot a + t \cdot b$ für die anfänglichen Werte von a und b.

Erweiterter Euklidischer Algorithmus

Vorgehen:

1. Letzte Zeile $s = 1$ und $t = 0$ eintragen.
2. Dann iterativ $s_{\text{neu}} := t_{\text{alt}}$ und $t_{\text{neu}} := s_{\text{alt}} - q_{\text{neu}} \cdot t_{\text{alt}}$ für jede Zeile.
3. In jeder Zeile gilt dann: $\text{ggT}(a, b) = s \cdot a + t \cdot b$.

Weiter im Beispiel von Folie 201:

a	b	q	s	t
130	35	3		
35	25	1		
25	10	2		
10	5	2		
5	0			

Euklidischer Algorithmus

Aufgabe (Fortsetzung von Folie 202)

Bestimmen Sie jeweils Zahlen $s, t \in \mathbb{Z}$ mit

1. $\mathrm{ggT}(595, 420) = s \cdot 595 + t \cdot 420$,
2. $\mathrm{ggT}(594, 420) = s \cdot 594 + t \cdot 420$.

Lösung

a	b	q	s	t
595	420	1	**5**	**-7**
420	175	2	-2	5
175	70	2	1	-2
70	35	2	0	1
35	0		1	0

$$\begin{aligned} 35 &= \mathrm{ggT}(420, 595) \\ &= 5 \cdot 595 - 7 \cdot 420 \end{aligned}$$

a	b	q	s	t
594	420	1	**29**	**-41**
420	174	2	-12	29
174	72	2	5	-12
72	30	2	-2	5
30	12	2	1	-2
12	6	2	0	1
6	0		1	0

$$\begin{aligned} 6 &= \mathrm{ggT}(420, 594) \\ &= 29 \cdot 594 - 41 \cdot 420 \end{aligned}$$

Multiplikativ Inverse in $\mathbb{Z}_m$

Mit dem Satz von Bézout kann man nun prüfen, ob das inverse Element einer Restklasse modulo m existiert:

Satz (Existenzsatz multiplikative inverse Restklassen)

Sei $m \in \mathbb{N}$ ein fester Modulus und $a \in \mathbb{Z}$. Die Restklasse $[a]_m$ hat genau dann ein multiplikativ inverses Element, wenn $\mathrm{ggT}(m, a) = 1$.

Wenn der Modulus eine Primzahl ist, ist der ggT immer dann 1, wenn a nicht Vielfaches von m ist, es gilt also:

Satz (Multiplikative Restklassengruppe 1)

Sei $p \in \mathbb{P}$ eine Primzahl. Dann ist $\left(\mathbb{Z}_p \setminus \left\{[0]_p\right\}, \otimes\right)$ eine Gruppe.

Dieser Satz folgt aus dem folgenden allgemeineren Satz:

Satz (Multiplikative Restklassengruppe 2)

Sei $m \in \mathbb{N}$ ein fester Modulus. Setze $\mathbb{Z}_m^\times := \left\{[a]_m \mid a \in \mathbb{Z}, \mathrm{ggT}(m, a) = 1\right\}$. Dann ist $\left(\mathbb{Z}_m^\times, \otimes\right)$ eine Gruppe. $\mathbb{Z}_m^\times$ heißt die multiplikative Gruppe von $\mathbb{Z}_m$.

Multiplikativ Inverse in $\mathbb{Z}_m$

Im Fall $\mathrm{ggT}(m, a) = 1$ ist folglich jede (multiplikative) Gleichung mit Operand $[a]_m$ in $\mathbb{Z}_m$ eindeutig lösbar. Dies formulieren wir im folgenden Satz:

Satz (Existenz- und Eindeutigkeitssatz Restklassengleichungen)

Sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(m, a) = 1$. Dann besitzt die Gleichung

$$[a]_m \otimes x = [b]_m$$

für jedes $b \in \mathbb{Z}$ genau eine Lösung $x \in \mathbb{Z}_m$, und diese ist gegeben durch

$$x = [a]_m^{-1} \otimes [b]_m.$$

Bemerkung (Berechnung des multiplikativ Inversen)

Zur Berechnung von $[a]_m^{-1}$ bestimmt man mit Hilfe des erweiterten euklidischen Algorithmus $s, t \in \mathbb{Z}$ mit $1 = \mathrm{ggT}(m, a) = s \cdot m + t \cdot a$. Dann folgt $[t]_m \otimes [a]_m = [t \cdot a]_m = [1]_m$, also $[a]_m^{-1} = [t]_m$.

Multiplikativ Inverse in $\mathbb{Z}_m$

Beispiel

- Betrachte $m = 15$ und $a = 8$.
  Dann ist $\mathrm{ggT}(m, a) = 1$, also ist $[8]_{15}$ invertierbar.
- Es gilt $[8]_{15}^{-1} = [2]_{15}$, denn $[8]_{15} \otimes [2]_{15} = [16]_{15} = [1]_{15}$.
- Folglich ist die Gleichung

$$[8]_{15} \otimes x = [b]_{15}$$

  für jedes $b \in \mathbb{Z}$ eindeutig lösbar.
- Betrachte konkret z.B. die Gleichung $[8]_{15} \otimes x = [12]_{15}$:
  Die eindeutige Lösung ist gegeben durch

$$x = [8]_{15}^{-1} \otimes [12]_{15} = [2]_{15} \otimes [12]_{15} = [24]_{15} = [9]_{15}.$$

Multiplikativ Inverse in $\mathbb{Z}_m$

Aufgaben

1. Geben Sie die multiplikative Gruppe von $\mathbb{Z}_{15}$ an, und geben Sie zu jedem $[a]_{15} \in \mathbb{Z}_{15}^{\times}$ ein $b \in \mathbb{Z}$ mit $[a]_{15}^{-1} = [b]_{15}$ an.
2. Berechnen Sie das multiplikativ Inverse von $[19]_{42}$ in $\mathbb{Z}_{42}$ mithilfe des erweiterten euklidischen Algorithmus.
3. Lösen Sie die Gleichung $[19]_{42} \otimes x = [5]_{42}$.

Multiplikativ Inverse in $\mathbb{Z}_m$

Lösung

1. Es gilt: $\mathbb{Z}_{15}^{\times} = \{[a]_{15} \mid \mathrm{ggT}(a,15) = 1\}$
$= \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}$

g	$[1]_{15}$	$[2]_{15}$	$[4]_{15}$	$[7]_{15}$	$[8]_{15}$	$[11]_{15}$	$[13]_{15}$	$[14]_{15}$
g^{-1}	$[1]_{15}$	$[8]_{15}$	$[4]_{15}$	$[13]_{15}$	$[2]_{15}$	$[11]_{15}$	$[7]_{15}$	$[14]_{15}$

2. Erweiterter Euklid. Alg. mit $a = 42$ und $b = 19$:

a	b	q	s	t
42	19	2	5	**-11**
19	4	4	-1	5
4	3	1	1	-1
3	1	3	0	1
1	0		1	0

$\rightsquigarrow 1 = \mathrm{ggT}(42,19) = 5 \cdot 42 + (-11) \cdot 19$,
also $[-11]_{42} \otimes [19]_{42} = [1]_{42}$,
also $[19]_{42}^{-1} = [-11]_{42} = [31]_{42}$.

3. $x = [19]_{42}^{-1} \otimes [5]_{42} = [-11]_{42} \otimes [5]_{42} = [-55]_{42} = [29]_{42}$.

Restklassengleichungen

Eine Verallgemeinerung des Satzes „Existenz- und Eindeutigkeitssatz Restklassengleichungen“ (Folie 208) ist der folgende Satz:

Satz (Existenzsatz Restklassengleichungen)

Sei $m \in \mathbb{N}$ ein fester Modulus. Dann hat für gegebene $a, b \in \mathbb{Z}$ die Restklassengleichung

$$[a]_m \otimes x = [b]_m$$

genau dann eine Lösung, wenn $\mathrm{ggT}(m, a) \mid b$.

Bemerkung (Lösung Restklassengleichung bestimmen)

Der Beweis des Satzes liefert ein Verfahren zum Bestimmen einer Lösung der Gleichung $[a]_m \otimes x = [b]_m$ im Fall $g := \mathrm{ggT}(m, a) \mid b$:

1. Setze $n := \frac{b}{g}$, dann gilt $n \in \mathbb{Z}$ und $b = n \cdot g$.
2. Bestimme $s, t \in \mathbb{Z}$ mit $\mathrm{ggT}(m, a) = s \cdot m + t \cdot a$ (s, t können mithilfe des erweiterten euklidischen Algorithmus berechnet werden).
3. Eine Lösung ist dann gegeben durch $x = [n \cdot t]_m$.

Restklassengleichungen

Beispiel

Wir wollen die folgende Gleichung lösen:

$$[15]_{24} \otimes x = [12]_{24}.$$

- Es gilt $\mathrm{ggT}(24, 15) = 3 \mid 12$, also ist die Gleichung lösbar.
- Es gilt $12 = 4 \cdot 3$ (also $n = 4$), und wir erhalten

$$3 = \mathrm{ggT}(15, 24) = 2 \cdot 24 + (-3) \cdot 15 \quad (\text{also } t = -3).$$

- Eine Lösung erhalten wir damit als

$$x = [n \cdot t]_{24} = [4 \cdot (-3)]_{24} = [-12]_{24} = [12]_{24}.$$

Restklassengleichungen

Abschließend wollen wir die Frage klären, wie man **alle** Lösungen der Gleichung

$$[a]_m \otimes x = [b]_m$$

im Fall $1 \neq \mathrm{ggT}(m, a) \mid b$ erhält.

Satz (Gesamtheit Lösungen Restklassengleichung)

Sei $m \in \mathbb{N}$ ein fester Modulus, und seien $a, b \in \mathbb{Z}$ mit $g := \mathrm{ggT}(m, a) \mid b$.
Ist $x_0 = [c]_m$ eine Lösung der Gleichung

$$[a]_m \otimes x = [b]_m,$$

so ist jede Lösung von der Gestalt

$$x_j = [c + j \cdot q]_m, \quad \text{für alle } j = 0, \ldots, g-1, \qquad \text{mit } \; q := \frac{m}{g},$$

und die Menge aller Lösungen ist gegeben durch $\{x_0, x_1, \ldots, x_{g-1}\}$.
Insbesondere gibt es insgesamt g Lösungen.

Restklassengleichungen

Beispiel von Folie 213

Wir betrachten wieder die Gleichung

$$[15]_{24} \otimes x = [12]_{24}.$$

- Wir haben bereits eine Lösung berechnet, nämlich $x_0 := [12]_{24}$.
- Es ist $q := \frac{m}{g} = \frac{24}{3} = 8$. Wir erhalten insgesamt die $g = 3$ Lösungen $x_j = [12 + j \cdot 8]_{24}, j = 0, 1, 2$:
  1. $x_0 = [12]_{24}$,
  2. $x_1 = [12 + 8]_{24} = [20]_{24}$,
  3. $x_2 = [12 + 2 \cdot 8]_{24} = [28]_{24} = [4]_{24}$.

Restklassengleichungen

Aufgabe

Welche der folgenden Restklassengleichungen besitzt eine Lösung? Geben Sie ggf. alle Lösungen an.

1. $[17]_{81} \otimes x = [7]_{81}$
2. $[45]_{81} \otimes x = [25]_{81}$
3. $[45]_{81} \otimes x = [27]_{81}$

Multiplikativ Inverse in $\mathbb{Z}_m$

Lösung

1. Hier ist $m = 81$ und $a = 17$, also $\mathrm{ggT}(m, a) = 1$
   $\rightsquigarrow$ es gibt **genau eine** Lösung.

   Bestimme $[17]_{81}^{-1}$ mit dem erweiterten Euklidischen Algorithmus:

m	a	q	s	t
81	17	4	4	**-19**
17	13	1	-3	4
13	4	3	1	-3
4	1	4	0	1
1	0		1	0

   $\rightsquigarrow [17]_{81}^{-1} = [-19]_{81} = [62]_{81}$,
   Lösung der Gleichung also:

$$\begin{aligned} x &= [17]_{81}^{-1} \otimes [7]_{81} = [-19 \cdot 7]_{81} \\ &= [-133]_{81} = [29]_{81}. \end{aligned}$$

2. Hier ist $m = 81$ und $a = 45$, also $g := \mathrm{ggT}(m, a) = 9$. Es gilt $g = 9 \nmid 25\,(= b)$, also besitzt die Gleichung **keine** Lösung.

Multiplikativ Inverse in $\mathbb{Z}_m$

Lösung

3. Hier ist $m = 81$ und $a = 45$, also $g := \mathrm{ggT}(m, a) = 9$, und es gilt $g = 9 \mid 27\,(= b)$.
Dabei ist $b = 27 = 3 \cdot 9$ und $m = 81 = 9 \cdot 9$, also $n = 3$ und $q = 9$.
Euklidischen Algorithmus:

m	a	q	s	t
81	45	1	-1	**2**
45	36	1	1	-1
36	9	4	0	1
9	0		1	0

$\rightsquigarrow 9 = -1 \cdot 81 + 2 \cdot 45.$

Eine Lösung der Gleichung ist also gegeben durch:
$x_0 = [n \cdot t]_{81} = [2 \cdot 3]_{81} = [6]_{81}.$

Es gib insgesamt $g = 9$ Lösungen, nämlich $x_j = [6 + 9 \cdot j]$, $j = 0, \ldots, 8$, also:

$$
\begin{aligned}
x_0 &= [6]_{81}, & x_1 &= [6+9]_{81} = [15]_{81},\\
x_2 &= [15+9]_{81} = [24]_{81}, & x_3 &= [24+9]_{81} = [33]_{81},\\
x_4 &= [33+9]_{81} = [42]_{81}, & x_5 &= [42+9]_{81} = [51]_{81},\\
x_6 &= [51+9]_{81} = [60]_{81}, & x_7 &= [60+9]_{81} = [69]_{81},\\
x_8 &= [69+9]_{81} = [78]_{81}.
\end{aligned}
$$

Überblick

Untergruppenkriterium

Definition (Untergruppe)

Sei $(G, \circ)$ eine Gruppe und $U \subseteq G$ eine nichtleere Teilmenge von G. U heißt Untergruppe von G, wenn U zusammen mit der eingeschränkten Verknüpfung $\circ_{|U \times U}$ selbst eine Gruppe ist.

Satz (Untergruppenkriterium)

Sei $(G, \circ)$ eine Gruppe und $U \subseteq G$, dann ist U genau dann eine Untergruppe, wenn gilt:

(U1) $U \neq \emptyset$,

(U2) $a \circ b \in U$ für alle $a, b \in U$,

(U3) $a^{-1} \in U$ für alle $a \in U$.

Untergruppen

Bemerkung

$\{e\}$ und G sind offensichtlich immer Untergruppen einer Gruppe G. Deshalb bezeichnet man sie als triviale Untergruppen.

Beispiel

Betrachte die Gruppe $(\mathbb{Z}, +)$. Sei $m \in \mathbb{N}$. Dann ist

$$m\mathbb{Z} = \{m \cdot a \mid a \in \mathbb{Z}\} = \{k \in \mathbb{Z} \mid \exists a \in \mathbb{Z} : k = m \cdot a\}$$

eine Untergruppe.

Beweis: [z.z.: $(m\mathbb{Z}, +) \subseteq (\mathbb{Z}, +)$ ist Untergruppe]

(U1) [z.z.: $m\mathbb{Z} \neq \emptyset$]
Es gilt: $0 = m \cdot 0 \in m\mathbb{Z}$, da $0 \in \mathbb{Z}$. Also ist $m\mathbb{Z} \neq \emptyset$.

(U2) [z.z.: $\forall a, b \in m\mathbb{Z} : a + b \in m\mathbb{Z}$]
Seien $a, b \in m\mathbb{Z}$. Es existiert $z, z' \in \mathbb{Z}$ mit $a = mz$ und $b = mz'$.
Es gilt: $a + b = mz + mz' = m(z + z') \in m\mathbb{Z}$, da $z + z' \in \mathbb{Z}$.

(U3) [z.z.: $\forall a \in m\mathbb{Z} : -a \in m\mathbb{Z}$]
Sei $a \in m\mathbb{Z}$. Es existiert $z \in \mathbb{Z}$ mit $a = mz$.
Es gilt: $-a = -mz = m(-z) \in m\mathbb{Z}$, da $-z \in \mathbb{Z}$.

Nichttriviale Untergruppen

Beispiele

1. Gruppe $(\mathbb{Z}_6, \oplus)$. Nichttriviale Untergruppen sind:
   - $U_1 = \{[0]_6, [3]_6\}$
   - $U_2 = \{[0]_6, [2]_6, [4]_6\}$
2. Gruppe $(\mathbb{Z}_5, \oplus)$. Es gibt keine nichttriviale Untergruppen!
3. Gruppe $\left(\mathbb{Z}_5 \setminus \{[0]_5\}, \otimes\right)$ hat eine nichttriviale Untergruppe:
   - $U_1 = \{[1]_5, [4]_5\}$

Untergruppen der S_3

Beispiel

Wir betrachten wieder die Gruppe S_3 der Bijektionen der Menge $\{1,2,3\}$ auf sich selbst.

$$\mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \tau_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_{13} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

In dieser Gruppe gibt es folgende nichttriviale Untergruppen:

- $U_1 = \{\mathrm{Id}, \tau_{12}\}$,
- $U_2 = \{\mathrm{Id}, \tau_{13}\}$,
- $U_3 = \{\mathrm{Id}, \tau_{23}\}$,
- $U_4 = \{\mathrm{Id}, \rho_1, \rho_2\}$.

Wiederholungen von Gruppenelementen

Zur einfacheren Notation definieren wir:

Definition (Wiederholungen von Gruppenelementen)

Sei $(G, \circ)$ eine Gruppe sowie $g \in G$ und $k \in \mathbb{Z}$.

$$g^k := \begin{cases} \underbrace{g \circ \ldots \circ g}_{k\text{-mal}}, & \text{falls } k > 0, \\ e, & \text{falls } k = 0, \\ \underbrace{g^{-1} \circ \ldots \circ g^{-1}}_{-k\text{-mal}}, & \text{falls } k < 0. \end{cases}$$

Satz (Potenzgesetze)

Sei $(G, \circ)$ eine Gruppe sowie $g \in G$ und $k, \ell \in \mathbb{Z}$. Dann gilt:

1. $g^k \circ g^\ell = g^{k+\ell}$,
2. $\left(g^k\right)^\ell = g^{k \cdot \ell}$.

Zyklische (Unter-)Gruppen

Satz und Definition (Von g erzeugte Untergruppe)

Sei $(G, \circ)$ eine Gruppe.

1. Für jedes $g \in G$ ist
$$\langle g \rangle := \{ g^k \mid k \in \mathbb{Z} \}$$
eine Untergruppe von G und wird die von g erzeugte Untergruppe genannt.
2. Falls es ein $g \in G$ gibt mit $G = \langle g \rangle$, so heißt die Gruppe G zyklisch und g ein erzeugendes Element von G.

Satz und Definition (Ordnung von g in endlichen Gruppen)

Sei $(G, \circ)$ eine **endliche** Gruppe und $g \in G$.

1. Dann gibt es ein $n \in \mathbb{N}$ mit $g^n = e$. Die kleinste solche Zahl n wird als Ordnung von g bezeichnet. Notation: $\mathrm{ord}(g) := n$.
2. Es gilt $\langle g \rangle = \{ g^k \mid k = 0, \ldots, \mathrm{ord}(g) - 1 \}$ und
$$\mathrm{ord}(g) = \mathrm{ord}(\langle g \rangle) = |\langle g \rangle|.$$

Ordnung von Elementen einer Gruppe

Beispiel

Wir betrachten wieder die Gruppe S_3.

$$\mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \tau_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_{13} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Die Elemente von S_3 haben folgende Ordnungen:

g	$\langle g \rangle$	$\mathrm{ord}(g)$
Id	$\{\mathrm{Id}\}$	1
τ_{23}	$\{\tau_{23}, \mathrm{Id}\}$	2
τ_{13}	$\{\tau_{13}, \mathrm{Id}\}$	2
τ_{12}	$\{\tau_{12}, \mathrm{Id}\}$	2
ρ_1	$\{\rho_1, \rho_2, \mathrm{Id}\}$	3
ρ_2	$\{\rho_2, \rho_1, \mathrm{Id}\}$	3

Beobachtung: Die S_3 ist nicht zyklisch.

Ordnung von Elementen einer Gruppe

Beispiel

Wir betrachten die Gruppe $(\mathbb{Z}_5, \oplus)$. Zur besseren Übersichtlichkeit notieren wir anstelle der Restklassen nur ihre kanonischen Repräsentanten.

g	$\langle g \rangle$	$\operatorname{ord}(g)$
0	$\{0\}$	1
1	$\{1, 2, 3, 4, 0\}$	5
2	$\{2, 4, 1, 3, 0\}$	5
3	$\{3, 1, 4, 2, 0\}$	5
4	$\{4, 3, 2, 1, 0\}$	5

Beobachtung: $(\mathbb{Z}_5, \oplus)$ ist zyklisch.
Alle Elemente $\neq 0$ sind erzeugende Elemente.

Ordnung von Elementen einer Gruppe

Beispiel

Wir betrachten die Gruppe $(\mathbb{Z}_6, \oplus)$. Zur besseren Übersichtlichkeit notieren wir anstelle der Restklassen nur ihre kanonischen Repräsentanten.

g	$\langle g \rangle$	$\operatorname{ord}(g)$
0	$\{0\}$	1
1	$\{1, 2, 3, 4, 5, 0\}$	6
2	$\{2, 4, 0\}$	3
3	$\{3, 0\}$	2
4	$\{4, 2, 0\}$	3
5	$\{5, 4, 3, 2, 1, 0\}$	6

Beobachtung: $(\mathbb{Z}_6, \oplus)$ ist zyklisch. Erzeugende Elemente sind $1, 5$.

Ordnung von Elementen einer Gruppe

Beispiel

Wir betrachten die Gruppe $\left(\mathbb{Z}_5 \setminus \{[0]_5\}, \otimes\right)$. Zur besseren Übersichtlichkeit notieren wir anstelle der Restklassen nur ihre kanonischen Repräsentanten.

g	$\langle g \rangle$	$\operatorname{ord}(g)$
1	$\{1\}$	1
2	$\{2, 4, 3, 1\}$	4
3	$\{3, 4, 2, 1\}$	4
4	$\{4, 1\}$	2

Beobachtung: $\left(\mathbb{Z}_5 \setminus \{[0]_5\}, \otimes\right)$ ist zyklisch.
Erzeugende Elemente sind $2, 3$.

Erzeugende Elemente in $\mathbb{Z}_m$ und $\mathbb{Z}_m^\times$

Bemerkung (Erzeugende Elemente in $\mathbb{Z}_m$ und $\mathbb{Z}_m^\times$)

Sei $m \in \mathbb{N}$ und $p \in \mathbb{P}$.

- Die Gruppe $(\mathbb{Z}_m, \oplus)$ ist zyklisch. Ein Element $[a]_m$ ist genau dann erzeugendes Element, wenn $\mathrm{ggT}(a, m) = 1$ ist.

  (Beweis: Übungsaufgabe in moodle)

- Die Gruppe $\left(\mathbb{Z}_m^\times, \otimes\right)$ ist im allgemeinen nicht zyklisch.

  Beispiel: $\mathbb{Z}_8^\times = \left\{[1]_8, [3]_8, [5]_8, [7]_8\right\}$.
  Es gilt $\mathrm{ord}\left([1]_8\right) = 1$ und $\mathrm{ord}\left([a]_8\right) = 2$ für $a = 3, 5, 7$.

- Die Gruppe $\left(\mathbb{Z}_p^\times, \otimes\right) = \left(\mathbb{Z}_p \setminus \left\{[0]_p\right\}, \otimes\right)$ ist zyklisch (hier ohne Beweis).

  Achtung: Das bedeutet, **es gibt** ein multiplikativ erzeugendes Element von $\left(\mathbb{Z}_p \setminus \left\{[0]_p\right\}, \otimes\right)$.

  Problem: Finden eines solchen erzeugenden Elements.

Satz von Lagrange

Wie man in den Beispielen sieht, ist die Ordnung einer Untergruppe immer ein Teiler der Ordnung der Gruppe. Das ist nicht nur in diesen Beispielen so, sondern allgemeingültig:

Satz von Lagrange

Sei $(G, \circ)$ eine endliche Gruppe und H eine Untergruppe. Dann gilt:

$$\text{ord}(H) \mid \text{ord}(G).$$

Folgerung

Da die Ordnung eines Gruppenelements g gleich der Ordnung der von g erzeugten Untergruppe $\langle g \rangle$ ist, folgt für alle $g \in G$:

$$\text{ord}(g) \mid \text{ord}(G).$$

Satz von Lagrange – Beweis

Der Beweis vom Satz von Lagrange beruht auf einer geschickt gewählten Äquivalenzrelation $\equiv_H$, die wir Kongruenz modulo H nennen.

Definition (Kongruenz modulo einer Untergruppe)

Sei $(G, \circ)$ eine Gruppe sowie H eine Untergruppe. Wir definieren für alle $g_1, g_2 \in G$:

$$g_1 \equiv_H g_2 :\Leftrightarrow g_1^{-1} \circ g_2 \in H.$$

Bemerkung

Dies stellt eine Verallgemeinerung der Kongruenz modulo m dar: Hier ist $G = (\mathbb{Z}, +)$ und $H = m\mathbb{Z}$, und die Kongruenz modulo H ist gegeben durch

$$a \equiv_H b \Leftrightarrow (-a) + b \in m\mathbb{Z} \Leftrightarrow b - a \in m\mathbb{Z} \Leftrightarrow m \mid b - a \Leftrightarrow a \equiv_m b.$$

Satz von Euler I

Satz (Kongruenz ist Äquivalenzrelation)

Sei $(G, \circ)$ eine Gruppe und H eine Untergruppe.

1. Dann ist $\equiv_H$ eine Äquivalenzrelation.
2. Sei $g \in G$. Dann gilt:

$$[g]_{\equiv_H} = \{g \circ h \mid h \in H\} =: gH.$$

Satz von Euler (Gruppentheoretische Variante)

Sei $(G, \circ)$ eine endliche Gruppe und $g \in G$. Dann gilt:

$$g^{\mathrm{ord}(G)} = e.$$

Satz von Euler II

Ursprünglich hat Euler diesen Satz nur für die multiplikative Gruppe $\left(\mathbb{Z}_m^\times, \otimes\right)$ bewiesen, und in dieser Fassung benötigen wir den Satz in den Anwendungen aus der Kryptologie. Für die entsprechende Formulierung definieren wir:

Definition (Eulersche φ-Funktion)

Sei $m \in \mathbb{N}$. Dann definieren wir

$$\varphi(m) := \left|\left\{a \in \mathbb{N} \mid a \leq m \text{ und } \operatorname{ggT}(a, m) = 1\right\}\right|,$$

dies ist also die Anzahl der zu m teilerfremden natürlichen Zahlen zwischen 1 und m. φ heißt die Eulersche φ-Funktion. Es gilt:

$$\varphi(m) = \operatorname{ord}\left(\mathbb{Z}_m^\times\right).$$

Satz von Euler (1760)

Seien $m, a \in \mathbb{N}$ mit $\operatorname{ggT}(m, a) = 1$. Dann gilt:

$$a^{\varphi(m)} \equiv_m 1.$$

Satz von Fermat

Der berühmte Mathematiker Pierre Fermat hat einen Spezialfall des Satzes von Euler bereits früher bewiesen:

Kleiner Satz von Fermat (1637)

Sei $p \in \mathbb{P}$ und $a \in \mathbb{N}$ mit $1 \leq a < p$. Dann gilt:

$$a^{p-1} \equiv_p 1.$$

Bemerkung

In der Notation der Restklassen bedeutet die Formel aus dem kleinen Satz von Fermat, dass für jede Primzahl p und jede Restklasse $[a]_p \neq [0]_p$ gilt:

$$[a]_p^{p-1} = [1]_p.$$

Berechnung der Eulerschen Phi-Funktion

Berechnung der Eulerschen Phi-Funktion

(1) Sei $p \in \mathbb{P}$. Dann gilt:

$$\varphi(p) = p - 1.$$

(2) Seien $p \in \mathbb{P}$ und $k \in \mathbb{N}$. Dann gilt:

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

(3) Seien $m, n \in \mathbb{N}$ und $\text{ggT}(m, n) = 1$. Dann gilt:

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

(4) Spezialfall: Seien $p, q \in \mathbb{P}$ mit $p \neq q$. Dann gilt:

$$\varphi(p \cdot q) = (p - 1) \cdot (q - 1).$$

(5) Sei $1 \neq n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} = \prod_{j=1}^{r} p_j^{k_j}$ mit $r \in \mathbb{N}$, paarweise verschiedenen $p_j \in \mathbb{P}$ und $k_j \in \mathbb{N}$ für alle $j = 1, \ldots, r$. Dann gilt:

$$\varphi(n) = n \cdot \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right).$$

Lemma von Euklid

Der Beweis von (3) erfordert einige Vorbereitungen. Zunächst formulieren wir das folgende grundlegende zahlentheoretische Ergebnis, welches auch die Grundlage für die Eindeutigkeit der Primfaktorzerlegung darstellt.

Lemma von Euklid

Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{Z}\backslash\{0\}$ mit $\mathrm{ggT}(m, a) = 1$. Dann gilt:

$$m \mid a \cdot b \Rightarrow m \mid b.$$

Folgerungen

1. Seien $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}$ mit $p \mid a \cdot b$. Dann folgt: $p \mid a$ oder $p \mid b$.
2. Seien $m, n, x \in \mathbb{Z}$ mit $\mathrm{ggT}(m, n) = 1$. Dann gilt:
$$m \cdot n \mid x \Leftrightarrow m \mid x \wedge n \mid x.$$
3. Seien $m, n \in \mathbb{Z}$ mit $\mathrm{ggT}(m, n) = 1$ und $a, b \in \mathbb{Z}$. Dann gilt:
$$[a]_{m \cdot n} = [b]_{m \cdot n} \Leftrightarrow [a]_m = [b]_m \wedge [a]_n = [b]_n.$$

Der chinesische Restsatz (ca. 3. Jhd.)

Einleitendes Beispiel

(a) Herr A. hat in diesem Jahr einen runden Geburtstag gefeiert. Gleichzeitig hat er auch ein volles Jahrsiebt vollendet. Wie alt ist Herr A. geworden?

(b) Herr B. dagegen hat das letzte volle Jahrsiebt vor 2 Jahren vollendet, und sein letzter runder Geburtstag liegt bereits 8 Jahre zurück. Wie alt ist Herr B.?

Mathematische Formulierung: Modulo-Gleichungssystem.

Der chinesische Restsatz

Seien $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$ und $a, b \in \mathbb{Z}$. Dann gibt es ein $x \in \mathbb{Z}$ mit

$$\begin{aligned} x &\equiv_m a, \\ x &\equiv_n b, \end{aligned}$$

und x ist eindeutig modulo $m \cdot n$.

$\text{ggT}(m,n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Beweisskizze für (3): $\text{ggT}(m,n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Der Beweis von (3) beruht auf der Tatsache, dass allgemein $\varphi(k) = \text{ord}\left(\mathbb{Z}_k^\times\right)$ ist.
Wir gehen folgendermaßen vor:

1. Wir zeigen, dass die Abbildung

$$\psi : \mathbb{Z}_{m\cdot n} \to \mathbb{Z}_m \times \mathbb{Z}_n, [x]_{m\cdot n} \mapsto \left([x]_m, [x]_n\right)$$

   wohldefiniert und bijektiv ist.

2. Anschließend zeigen wir, dass die Einschränkung von ψ auf die multiplikative Gruppe eine Bijektion zwischen $\mathbb{Z}_{m\cdot n}^\times$ und $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ ist, das heißt, wir zeigen, dass die Abbildung

$$\psi^* := \psi|_{\mathbb{Z}_{m\cdot n}^\times} : \mathbb{Z}_{m\cdot n}^\times \to \mathbb{Z}_m \times \mathbb{Z}_n,$$

   die folgende Identität erfüllt: $\text{Bild}(\psi^*) = \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$.

3. Hieraus folgt:

$$\varphi(m \cdot n) = |\mathbb{Z}_{m\cdot n}^\times| = |\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times| = |\mathbb{Z}_m^\times| \cdot |\mathbb{Z}_n^\times| = \varphi(m) \cdot \varphi(n).$$

Überblick

Algebraische Strukturen mit zwei Verknüpfungen

- Bisher haben wir algebraische Strukturen als Mengen mit einer Verknüpfung betrachtet.
- In der Algebra gibt es weitere Strukturen, die zwei (oder mehr) Verknüpfungen tragen.
- Dies ist bereits wohlbekannt:
  Die aus der Schule vertrauten Zahlenräume tragen als Verknüpfungen Addition und Multiplikation.
- Die additive und multiplikative Struktur werden dabei durch das Distributivgesetz verbunden.
- Wir wollen diese Strukuren – wie üblich – allgemein definieren und betrachten.

Ringe

Definition (Ring)

Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus eine Menge R und zwei Verknüpfungen $+$ und $\cdot$ auf R mit den folgenden Eigenschaften:

(R1) $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0.

(R2) $(R, \cdot)$ erfüllt das Assoziativgesetz.

(R3) Es gilt das Distributivgesetz: Für alle $a, b, c \in R$ gilt

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

- Erfüllt $(R, \cdot)$ auch das Kommutativgesetz, so nennt man $(R, +, \cdot)$ einen kommutativen Ring.
- Besitzt $(R, \cdot)$ ein neutrales Element, so nennt man $(R, +, \cdot)$ einen Ring mit Einselement oder kurz Ring mit Eins.

Beispiele Ringe und Rechenregeln

Beispiele

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit Eins.
- $(\mathbb{N}_0, +, \cdot)$ ist kein Ring.
- Für jedes $m \in \mathbb{N} \setminus \{1\}$ ist $(m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring ohne Eins.
- Für jedes $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, \oplus, \otimes)$ ein kommutativer Ring mit Eins.
- Sei X eine Menge und $R := P(X)$. Dann ist $(R, \Delta, \cap)$ ein Ring.

Rechenregeln in Ringen

Es sei $(R, +, \cdot)$ ein Ring.

(1) Für alle $a \in R$ gilt $0 \cdot a = 0 = a \cdot 0$.

(2) Für alle $a, b \in R$ gilt $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$.

Körper und Beispiele

Definition (Körper)

Ein Körper ist ein Tripel $(K, +, \cdot)$ bestehend aus eine Menge K und zwei Verknüpfungen $+$ und $\cdot$ auf K mit den folgenden Eigenschaften:

(K1) $(K, +)$ ist eine abelsche Gruppe mit neutralem Element 0.

(K2) $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1.

(K3) Es gilt das Distributivgesetz: Für alle $a, b, c \in K$ gilt

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

Beispiele

- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind Körper.
- $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- Für jedes $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, \oplus, \otimes)$ genau dann ein Körper, wenn m eine Primzahl ist.

Rechenregeln in Körpern

In einem Ring $(R, +, \cdot)$ kann es Elemente $a, b \neq 0$ geben, für die $a \cdot b = 0$ gilt (Beispiel?). Man bezeichnet solche Elemente a, b als Nullteiler. Eine wichtige Eigenschaft von Körpern besteht darin, dass es keine Nullteiler außer der 0 gibt.

Bemerkung (Nullteilerfreiheit von Körpern)

Es sei $(K, +, \cdot)$ ein Körper und es seien $a, b \in K$ mit $a \cdot b = 0$.
Dann gilt $a = 0$ oder $b = 0$.

Satz

Es sei $(K, +, \cdot)$ ein Körper und $a \in K$. Dann gilt:

$$a^2 = 1 \Leftrightarrow a = 1 \vee a = -1.$$

Folgerung

Sei $p \in \mathbb{P}$ und $a \in \{0, \ldots, p-1\}$ ein kanonischer Repräsentant. Es gilt:

$$[a]_p^2 = [1]_p \quad \Leftrightarrow \quad a = 1 \ \vee \ a = p - 1.$$

Vielen Dank für Ihre Aufmerksamkeit