Mathematik I für Studierende der Informatik und Wirtschaftsinformatik

(Diskrete Mathematik)

THOMAS ANDREAE

Wintersemester 2011 / 2012

(Stand: 22. Dezember 2011)

Inhaltsverzeichnis

1 Mengen und Boolesche Algebra

1.1 Einige Begriffe und Notationen der Mengenlehre

In diesem Abschnitt stellen wir einige Begriffe, Schreib- und Sprechweisen zusammen, die wir von Anfang an benötigen, um mathematische Sachverhalte (wie üblich) in der Sprache der Mengenlehre ausdrücken zu können. Einiges hiervon wird später noch wesentlich genauer behandelt werden.

Unter einer *Menge* verstehen wir eine Zusammenfassung von bestimmten Objekten, welche die *Elemente der Menge* genannt werden, zu einem neuen Objekt. Zur Beschreibung von Mengen verwenden wir geschweifte Klammern. Eine Menge kann durch Aufzählen ihrer Elemente beschrieben werden (z.B.: $\{6, 7, 8, 9\}$). Darüber hinaus kann man eine Menge durch Angabe von Eigenschaften ihrer Elemente beschreiben, wobei genau festgelegt werden muss, welche Elemente zu der betreffenden Menge gehören (s.u. für eine derartige Beschreibung der Menge $\{6, 7, 8, 9\}$).

Beispiele für Mengen:

1. Die *Menge der natürlichen Zahlen*: Dies sind die Zahlen 1, 2, 3, ... Diese Menge bezeichnen wir mit $\mathbb{N}$.
2. Die Menge der natürlichen Zahlen, die größer als 5 und kleiner als 10 sind. Diese Menge können wir auch so schreiben:

   $$\Big\{n : n \text{ ist eine natürliche Zahl, für die } 5 < n < 10 \text{ gilt}\Big\}.$$

   Offenbar ist dies genau die Menge $\{6, 7, 8, 9\}$.
3. Die Menge der geordneten Paare von natürlichen Zahlen: Diese Menge bezeichnet man mit $\mathbb{N} \times \mathbb{N}$ oder $\mathbb{N}^2$. Es gilt also:

   $$\mathbb{N}^2 = \mathbb{N} \times \mathbb{N} = \Big\{(n, m) : n \text{ und } m \text{ sind natürliche Zahlen}\Big\}.$$

4. Die *Menge der ganzen Zahlen*: Dies sind die Zahlen 0, 1, 2, 3, ... sowie -1, -2, -3, ... Diese Menge bezeichnen wir mit $\mathbb{Z}$.

$x \in M$ bedeutet: „x ist ein Element von M“;

$x \notin M$ bedeutet: „x ist kein Element von M“.

Sind A und B Mengen, so nennt man A eine *Teilmenge* von B (Schreibweise: $A \subseteq B$), wenn jedes Element von A auch ein Element von B ist. Zwei Mengen heißen *gleich*, wenn sie dieselben Elemente besitzen. Das heißt insbesondere, dass es nicht darauf ankommt, in welcher Reihenfolge man die Elemente einer Menge aufschreibt.

Beispiel. $\{2, 3, 4\} = \{3, 4, 2\}$.

Ferner spielen Mehrfachnotierungen von Elementen keine Rolle:

$$\Big\{1, 2, 1, 1\Big\} = \Big\{1, 2\Big\}.$$

Die Menge, die keine Elemente enthält, heißt *leere Menge*. Sie wird mit $\emptyset$ bezeichnet. Die leere Menge ist Teilmenge jeder Menge, d.h., es gilt: $\emptyset \subseteq A$ für alle Mengen A.

Eine Menge A heißt *echte Teilmenge* von B (Zeichen: $A \subsetneq B$), wenn $A \subseteq B$ und $A \neq B$ gilt.

Ist M eine Menge, so bezeichnen wir (wie im obigen Beispiel) mit $M \times M$ oder M^2 die Menge aller geordneten Paare von Elementen aus M, d.h.:

$$M^2 = M \times M = \Big\{(a,b) : a,b \in M\Big\}.$$

Man nennt die Menge $M \times M$ *kartesisches Produkt* oder auch *Paarmenge*.

Beispiel. Es sei $M = \big\{1,2,3\big\}$. Es folgt

$$M^2 = M \times M = \Big\{(1,1),\ (1,2),\ (1,3),\ (2,1),\ (2,2),\ (2,3),\ (3,1),\ (3,2),\ (3,3)\Big\}.$$

Man beachte, dass die Paare $(1,2)$ und $(2,1)$ verschieden sind, da es wie gesagt sich um *geordnete Paare* handelt.

Analog definieren wir:

$$M^3 = M \times M \times M = \Big\{(a,b,c) : a,b,c \in M\Big\}.$$

M^3 ist also die Menge der *geordneten Tripel* von Elementen aus M. Ebenso: M^4 ist die Menge der *geordneten Quadrupel*, M^5 ist die Menge der *geordneten Quintupel*, ... Allgemein definiert man für $n \geq 2$:

$$M^n = \Big\{(a_1, a_2, \ldots, a_n) : a_i \in M \text{ für } i = 1, \ldots, n\Big\}.$$

Man bezeichnet mit M^1 die Menge M selbst, also $M^1 = M$. Die Elemente von M^n nennt man *n-Tupel von Elementen aus M*; die Menge M^n aller *n-Tupel von Elementen aus M* nennt man auch *n-stelliges kartesisches Produkt* von M ($n \geq 1$).

Beispiel. Es sei $B = \big\{0,1\big\}$. Dann ist

$$\begin{aligned}
B^1 &= \Big\{0,1\Big\} \\
B^2 &= \Big\{(0,0),\ (0,1),\ (1,0),\ (1,1)\Big\} \\
B^3 &= \Big\{(0,0,0),\ (0,0,1),\ (0,1,0),\ (0,1,1),\ (1,0,0),\ (1,0,1),\ (1,1,0),\ (1,1,1)\Big\}.
\end{aligned}$$

1.2 Grundlegendes über Abbildungen

Definition.
Sind A und B Mengen, so versteht man unter einer *Funktion* f von A nach B eine Vorschrift, durch die jedem Element $a \in A$ genau ein Element $b \in B$ zugeordnet wird.

Anstelle von Funktion sagt man auch *Abbildung*. Um zum Ausdruck zu bringen, dass f eine Funktion von A nach B ist, benutzt man die Schreibweise

$$f : A \to B.$$

Man nennt A den *Definitionsbereich* und B den *Wertebereich* der Funktion $f : A \to B$. Wird durch die Funktion $f : A \to B$ dem Element $a \in A$ das Element $b \in B$ zugeordnet, so sagt man „f bildet a auf b ab“ und bezeichnet b mit $f(a)$. Statt „f bildet a auf b ab“ kann man also kurz

$$f(a) = b$$

schreiben; außerdem verwendet man häufig die Schreibweise

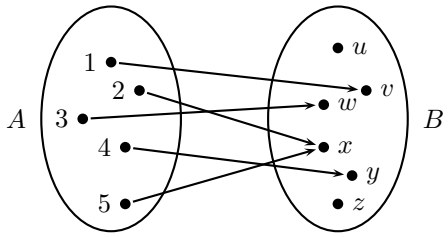
$$a \mapsto b.$$

Diese bringt ebenfalls zum Ausdruck, dass a auf b abgebildet wird. Gilt $f(a) = b$, so nennt man b den *Wert von f an der Stelle a*.

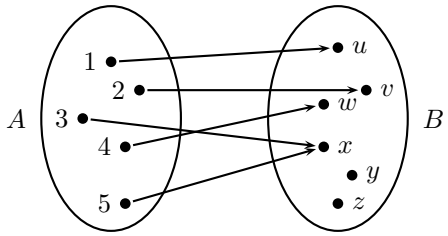
Beispiel. Es seien $A = \{1, 2, 3, 4, 5\}$ und $B = \{u, v, w, x, y, z\}$. Wir geben eine Funktion $f : A \to B$ in Form einer Tabelle an:

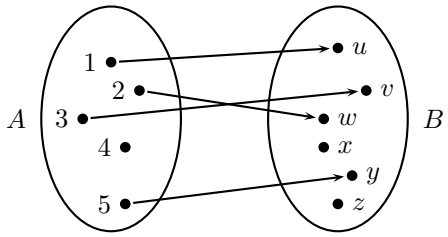
a	$f(a)$
1	v
2	x
3	w
4	y
5	x

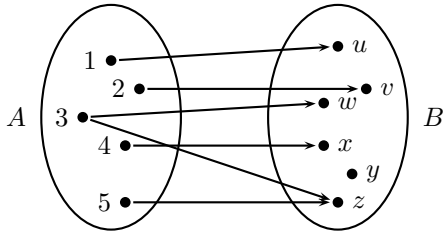
Für diese Funktion f gilt also beispielsweise $f(3) = w$ und $f(5) = x$. (Oder anders geschrieben: $3 \mapsto w$ und $5 \mapsto x$.) Die Funktion dieses Beispiels können wir auch durch ein Pfeildiagramm veranschaulichen:



Wir betrachten einige Pfeildiagramme (Statt Pfeildiagramm sagt man auch *bipartiter gerichteter Graph*; vergleiche Abschnitt 3.1):







Nur das erste dieser Pfeildiagramme stellt eine Funktion $f : A \to B$ dar! (Warum?)

Weitere **Beispiele** von Funktionen:

1. Eine Funktion $f : \mathbb{N} \to \mathbb{N}$ wird beispielsweise durch die Formel $f(n) = n + 1$ definiert. Durch diese Funktion wird jeder natürlichen Zahl ihr Nachfolger zugeordnet.
2. Durch die Formel $g(n) = 3n^4 + 2$ wird ebenfalls eine Funktion $g : \mathbb{N} \to \mathbb{N}$ definiert.
3. Durch $f\big((n, m)\big) = n + m$ wird eine Funktion $f : \mathbb{N}^2 \to \mathbb{N}$ definiert[1].
4. Ebenso: $f(n, m) = n \cdot m$.
5. Durch $f(n, m, k) = (n + k) \cdot m \cdot k + n$ wird eine Funktion $f : \mathbb{N}^3 \to \mathbb{N}$ definiert.
6. Eine Funktion $f : \big\{0, 1\big\} \to \big\{0, 1\big\}$ wird beispielsweise durch $f(0) = 1$ und $f(1) = 0$ definiert.

Hinweis zur Beschreibung von Abbildungen (in Anlehnung an Jänich: Lineare Algebra): Was schreibt man auf, wenn man eine Abbildung anzugeben hat? Als Beispiel benutzen wir die Abbildung von $\mathbb{N}$ nach $\mathbb{N}$, die jeder natürlichen Zahl ihr Quadrat zuordnet. Dann kann man beispielsweise schreiben:

$$\text{Sei } f : \mathbb{N} \to \mathbb{N} \text{ die durch } f(n) = n^2 \text{ (für } n \in \mathbb{N}) \text{ gegebene Abbildung.}$$

Oder etwas kürzer:

$$\text{Sei } f : \mathbb{N} \to \mathbb{N} \text{ die durch } n \mapsto n^2 \text{ gegebene Abbildung.}$$

Oder noch etwas kürzer:

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & n^2 \end{array}$$

Falls es nicht nötig ist, der Abbildung einen Namen zu geben, so kann man auch schreiben (besonders kompakte Schreibweise!):

$$\begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & n^2 \end{array}$$

Eine Abbildung muss aber nicht unbedingt durch eine Formel beschrieben werden; man kann eine Zuordnung auch in Worten beschreiben. (In unserem Beispiel: „Wir betrachten die Abbildung, die jeder natürlichen Zahl ihr Quadrat zuordnet“.)

Definition.

Eine Abbildung $f : A \to B$ heißt

(a) *injektiv*, falls für alle $x, y \in A$ gilt: Aus $x \neq y$ folgt $f(x) \neq f(y)$.

(b) *surjektiv*, falls es zu jedem $b \in B$ mindestens ein $a \in A$ gibt, für das $f(a) = b$ gilt.

(c) *bijektiv*, falls sie injektiv und surjektiv ist.

Beispiele:

1. Es sei $A = \big\{1, 2, 3\big\}$ und $B = \big\{1, 2, 3\big\}$. Die Funktion $f : A \to B$ sei definiert durch $f(1) = 1$, $f(2) = 1$ und $f(3) = 2$. Diese Funktion ist weder injektiv noch surjektiv.
2. Es sei $A = \big\{1, 2, 3\big\}$ und $B = \big\{1, 2, 3, 4\big\}$. Die Funktion $f : A \to B$ sei definiert durch $f(1) = 1$, $f(2) = 3$ und $f(3) = 4$. Diese Funktion ist injektiv, aber nicht surjektiv.
3. Es sei $A = \big\{1, 2, 3\big\}$ und $B = \big\{4, 5\big\}$. Die Funktion $f : A \to B$ sei definiert durch $f(1) = 4$, $f(2) = 5$ und $f(3) = 4$. Diese Funktion ist nicht injektiv, aber surjektiv.
4. Es sei $A = \big\{1, 2, 3\big\}$ und $B = \big\{3, 4, 5\big\}$. Die Funktion $f : A \to B$ sei definiert durch $f(1) = 4$, $f(2) = 5$ und $f(3) = 3$. Diese Funktion ist sowohl injektiv als auch surjektiv, also bijektiv.

[1] In diesem Beispiel und in vergleichbaren Fällen ist es auch üblich, anstelle von $f\big((n, m)\big)$ einfach $f(n, m)$ zu schreiben.

Anstelle von „f ist eine surjektive Abbildung von A nach B“ sagt man auch „f ist eine Abbildung von A *auf* B“; anstelle von injektiv sagt man auch *eineindeutig*; anstelle von bijektiv sagt man auch *umkehrbar eindeutig*. **Empfehlung**: Man veranschauliche sich die Begriffe „injektiv“, „surjektiv“ und „bijektiv“ mit Hilfe von Pfeildiagrammen.

Bemerkung zum Nachweis der Injektivität

Ist von einer Funktion $f : A \to B$ nachzuweisen, dass sie injektiv ist, so ist es meistens zweckmäßig, nach folgendem Schema vorzugehen („Widerspruchsbeweis“): Man wählt $x, y \in A$ beliebig und nimmt an, dass $x \neq y$ und $f(x) = f(y)$ gilt. Aus $f(x) = f(y)$ folgert man (beispielsweise durch Umformung der Gleichung $f(x) = f(y)$), dass $x = y$ gilt. Dies ist ein Widerspruch zur Annahme $x \neq y$, wodurch die Injektivität nachgewiesen ist. Wir erläutern diese Vorgehensweise anhand eines Beispiel.

Beispiel. Die Funktion $f : \mathbb{N} \to \mathbb{N}$ sei definiert durch $f(n) = 2n + 1$ für alle $n \in \mathbb{N}$.

Behauptung. f ist injektiv.

Beweis. Angenommen, für $n, m \in \mathbb{N}$ gelte $n \neq m$ und $f(n) = f(m)$. Nach Definition von f gilt also $2n + 1 = 2m + 1$. Durch Subtraktion von 1 auf beiden Seiten dieser Gleichung folgt $2n = 2m$. Hieraus folgt mittels Division durch 2, dass $n = m$ gilt – im Widerspruch zu $n \neq m$. Also ist f injektiv. □

Das Zeichen □ bedeutet, dass der Beweis abgeschlossen ist.

Wir weisen darüber hinaus nach, dass f nicht surjektiv ist. Hierzu genügt es, ein $m \in \mathbb{N}$ anzugeben, für das gilt: Es gibt kein $n \in \mathbb{N}$ mit $f(n) = m$. Wir weisen nach, dass dies für $m = 2$ der Fall ist: Angenommen, es gebe ein $n \in \mathbb{N}$ mit $f(n) = 2$. Nach Definition von f würde $2n + 1 = 2$ gelten, woraus durch Subtraktion von 1 und anschließender Division durch 2 folgen würde, dass $n = \frac{1}{2}$ gilt. Dies widerspricht der Annahme $n \in \mathbb{N}$. Also ist f nicht surjektiv.

Beim Beweis der Surjektivität im vorangegangenen Absatz handelt es sich ebenfalls um einen Beweis durch Widerspruch; in Abschnitt 2.2 finden sich weitere Bemerkungen zu Thema Widerspruchsbeweis.

Definition.

Unter einer *n-stelligen Verknüpfung* auf einer Menge M versteht man eine Abbildung $f : M^n \to M$ (für $n \in \mathbb{N}$). Statt n-stellige Verknüpfung sagt man auch *n-stellige Operation*.

Ein besonders wichtiger Spezialfall ist der Fall $n = 2$; in diesem Fall spricht man auch von einer *binären Verknüpfung* (bzw. *Operation*). Beispiele binärer Verknüpfungen sind die Addition und die Multiplikation natürlicher Zahlen. Siehe Beispiel 3 und 4 in Abschnitt 1.2 (vor dem Hinweis zur Beschreibung von Abbildungen).

Weitere Grundbegriffe, die im Zusammenhang mit Abbildungen stehen (wie beispielsweise Bild, Urbild oder Komposition von Abbildungen) werden in Abschnitt 3.5 behandelt.

1.3 Operationen für Mengen und Boolesche Algebra

Im Folgenden seien mit großen lateinischen Buchstaben immer Mengen bezeichnet. Mit $A \cap B$ bezeichnet man die *Schnittmenge* von A und B (auch *Durchschnitt* genannt), mit $A \cup B$ die *Vereinigungsmenge* von A und B (auch *Vereinigung* genannt). Diese werden definiert durch[2]:

$$A \cap B := \Big\{x : x \in A \textbf{ und } x \in B\Big\}$$
$$A \cup B := \Big\{x : x \in A \textbf{ oder } x \in B\Big\}$$

[2] „:=“ ist hier das *definitorische Gleichheitszeichen*; links von „:=“ steht immer der zu definierende Ausdruck.

Unter Verwendung der üblichen Verknüpfungszeichen für Aussagen hätten wir auch schreiben können:

$$\begin{aligned} A \cap B &:= \Big\{x : x \in A \wedge x \in B\Big\} \\ A \cup B &:= \Big\{x : x \in A \vee x \in B\Big\}. \end{aligned}$$

Zwei Mengen A und B heißen *disjunkt* (oder *elementfremd*), falls $A \cap B = \emptyset$ gilt.

Die *Differenz von Mengen* definiert man durch

$$A \setminus B := \Big\{x : x \in A \text{ und } x \notin B\Big\}.$$

Die *symmetrische Differenz*, für die wir das Zeichen $\oplus$ benutzen, wird definiert durch

$$A \oplus B := \Big(A \setminus B\Big) \cup \Big(B \setminus A\Big).$$

Die *Potenzmenge* $\mathcal{P}(M)$ einer Menge M ist die Menge aller Teilmengen von M.

Beispiele:

1. Es sei $M = \Big\{a, b, c\Big\}$. Dann gilt $\mathcal{P}(M) = \Big\{\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{a, b\},\ \{a, c\},\ \{b, c\},\ \{a, b, c\}\Big\}$.

2. Es sei $M = \Big\{a, b\Big\}$. Dann gilt $\mathcal{P}(M) = \Big\{\emptyset,\ \{a\},\ \{b\},\ \{a, b\}\Big\}$.

3. Es sei $M = \Big\{a\Big\}$. Dann gilt $\mathcal{P}(M) = \Big\{\emptyset,\ \{a\}\Big\}$.

4. Es sei $M = \emptyset$. Dann gilt $\mathcal{P}(M) = \Big\{\emptyset\Big\}$.

5. Es sei $M = \Big\{a, \{b, c\}\Big\}$. Dann gilt $\mathcal{P}(M) = \Big\{\emptyset,\ \{a\},\ \{\{b, c\}\},\ \{a, \{b, c\}\}\Big\}$.

Auch von Potenzmengen können Potenzmengen gebildet werden:

$$\begin{aligned} M &= \Big\{a\Big\} \\ \mathcal{P}(M) &= \Big\{\emptyset,\ \{a\}\Big\} \\ \mathcal{P}\big(\mathcal{P}(M)\big) &= \Big\{\emptyset,\ \{\emptyset\},\ \{\{a\}\},\ \{\emptyset,\ \{a\}\}\Big\}. \end{aligned}$$

Es sei eine Menge M fest gegeben. Für $A \subseteq M$ definiert man das *Komplement* $\overline{A}$ von A (in M) durch

$$\overline{A} := \Big\{x : x \in M \setminus A\Big\}.$$

Verwendet man das Zeichen $\overline{A}$, so muss aus dem Zusammenhang hervorgehen, auf welche Grundmenge M man sich bezieht.

Es sei nun M fest gegeben. A, B und C seien Teilmengen von M. Für das Rechnen mit den Operationen $\cap$, $\cup$ und $^-$ gelten die folgenden Regeln:

(1) Assoziativgesetze:

- $A \cap \big(B \cap C\big) = \big(A \cap B\big) \cap C$
- $A \cup \big(B \cup C\big) = \big(A \cup B\big) \cup C$

(2) Kommutativgesetze:

- $A \cap B = B \cap A$
- $A \cup B = B \cup A$

(3) Absorptionsgesetze:

- $A \cap \big(A \cup B\big) = A$
- $A \cup \big(A \cap B\big) = A$

(4) Distributivgesetze:
- $A \cap \big(B \cup C\big) = \big(A \cap B\big) \cup \big(A \cap C\big)$
- $A \cup \big(B \cap C\big) = \big(A \cup B\big) \cap \big(A \cup C\big)$

(5) 0 - 1 - Gesetze:
- $A \cap M = A$
- $A \cap \emptyset = \emptyset$
- $A \cup M = M$
- $A \cup \emptyset = A$

(6) Komplementgesetze:
- $A \cap \overline{A} = \emptyset$
- $A \cup \overline{A} = M$

(7) Idempotenzgesetze:
- $A \cap A = A$
- $A \cup A = A$

(8) Negation der Negation:
- $\overline{\overline{A}} = A$

(9) De Morgansche Regeln:
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Beweisen lassen sich diese Regeln mit Hilfe von Wahrheitstafeln; wir demonstrieren dies für das erste der beiden Distributivgesetze:

A	B	C	$B \cup C$	$A \cap \big(B \cup C\big)$	$A \cap B$	$A \cap C$	$\big(A \cap B\big) \cup \big(A \cap C\big)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

Der Eintrag „1“ bedeutet, dass die betreffende Aussage wahr ist, d.h.: $x \in A$, $x \in B$, ...

Der Eintrag „0“ bedeutet, dass die betreffende Aussage falsch ist, d.h.: $x \notin A$, $x \notin B$, ...

Da die Spalten für $A \cap (B \cup C)$ und $(A \cap B) \cup (A \cap C)$ übereinstimmen, haben wir das erste Distributivgesetz bewiesen. □

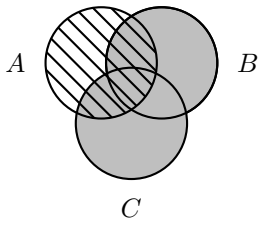
Aufgrund der Assoziativgesetze kann man bei der Durchschnittsbildung von mehreren Mengen auf eine Klammerung verzichten, gleiches gilt für die Vereinigung.

Durchschnitt und Vereinigung für Mengen A_i ($i \in I$, I ist eine sog. *Indexmenge*) definiert man durch

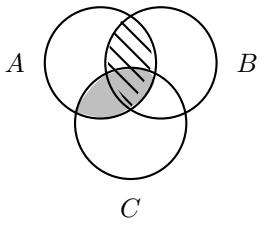
$$\begin{aligned} \bigcap_{i \in I} A_i &:= \Big\{x : x \in A_i \text{ für alle } i \in I\Big\} \\ \bigcup_{i \in I} A_i &:= \Big\{x : \text{ Es gibt ein } i \in I \text{ mit } x \in A_i\Big\}. \end{aligned}$$

Beispiel. Es sei $I = \{1, 2, \ldots, n\}$. Statt $\bigcap_{i \in I} A_i$ bzw. $\bigcup_{i \in I} A_i$ schreibt man dann auch $\bigcap_{i=1}^{n} A_i$ bzw. $\bigcup_{i=1}^{n} A_i$ oder auch $A_1 \cap A_2 \cap \ldots \cap A_n$ bzw. $A_1 \cup A_2 \cup \ldots \cup A_n$.

Man kann sich die Regeln (1) - (9) durch sogenannte *Venn-Diagramme* veranschaulichen:



Schraffiert: A
Grau: $B \cup C$
Grau und schraffiert: $A \cap (B \cup C)$



Schraffiert: $A \cap B$
Grau: $A \cap C$
Grau oder schraffiert: $(A \cap B) \cup (A \cap C)$

Unter einer Booleschen Algebra versteht man Folgendes:

Definition.

Gegeben sei eine Menge B zusammen mit zwei binären Verknüpfungen auf B, die mit $\sqcap$ und $\sqcup$ bezeichnet seien (d.h., jedem geordneten Paar (a, b) mit $a, b \in B$ seien zwei Elemente aus B zugeordnet, die mit $a \sqcap b$ bzw. $a \sqcup b$ bezeichnet seien). Man nennt B (zusammen mit den Verknüpfungen $\sqcap$ und $\sqcup$) eine *Boolesche Algebra*, falls folgende Aussagen für alle $a, b, c \in B$ gelten:

(A1) Assoziativgesetze:
- $a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c$
- $a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c$

(A2) Kommutativgesetze:
- $a \sqcap b = b \sqcap a$
- $a \sqcup b = b \sqcup a$

(A3) Distributivgesetze:
- $a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$
- $a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c)$

(A4) Existenz von Null und Eins:

Es gibt in B zwei Elemente, genannt 0 und 1, für die gilt:
- $a \sqcap 1 = a$
- $a \sqcup 0 = a$

(A5) Existenz eines Komplements:

Zu jedem $a \in B$ gibt es ein Element $\overline{a} \in B$ derart, dass gilt:
- $a \sqcap \overline{a} = 0$
- $a \sqcup \overline{a} = 1$

Man nennt die Aussagen (A1) - (A5) *Axiome* einer Booleschen Algebra. Wir wollen jetzt exemplarisch vorführen, wie man aus diesen Axiomen *Folgerungen* herleitet. Solche Folgerungen nennt man *Sätze* über Boolesche Algebren. Mit B sei jetzt immer eine Boolesche Algebra bezeichnet.

Satz 1.

Für alle $a \in B$ gilt: $a \sqcap a = a$ und $a \sqcup a = a$.

Beweis. Es gilt

$$a \sqcap a \overset{(A4)}{=} (a \sqcap a) \sqcup 0 \overset{(A5)}{=} (a \sqcap a) \sqcup (a \sqcap \overline{a}) \overset{(A3)}{=} a \sqcap (a \sqcup \overline{a}) \overset{(A5)}{=} a \sqcap 1 \overset{(A4)}{=} a.$$

Damit ist $a \sqcap a = a$ gezeigt. Ganz entsprechend weist man $a \sqcup a = a$ nach:

$$a \sqcup a \overset{(A4)}{=} (a \sqcup a) \sqcap 1 \overset{(A5)}{=} (a \sqcup a) \sqcap (a \sqcup \overline{a}) \overset{(A3)}{=} a \sqcup (a \sqcap \overline{a}) \overset{(A5)}{=} a \sqcup 0 \overset{(A4)}{=} a. \square$$

Über dem Gleichheitszeichen ist notiert, weshalb diese Gleichheit besteht. Man beachte, dass wir zur Herleitung nur die Axiome benutzt haben. Auffällig ist ferner, dass der Beweis der beiden Teilaussagen nach genau demselben Schema abgelaufen ist. Dies ist nicht verwunderlich: Jedes Axiom besteht aus einem Paar von Aussagen, die durch Vertauschen von $\sqcap$ und $\sqcup$ sowie durch Vertauschen von 0 und 1 auseinander hervorgegangen sind. Alle Schlüsse in einem Beweis kann man daher ebenso gut mit vertauschten Rollen von $\sqcap$ und $\sqcup$ bzw. 0 und 1 machen. Daher gehört zu jeder gültigen Folgerung aus den Axiomen immer zugleich noch eine weitere gültige Folgerung, die man auch als „duale Aussage“ bezeichnet. Wir halten dies noch einmal explizit als *Dualitätsprinzip* fest.

Dualitätsprinzip für Boolesche Algebren.

Jede Aussage, die eine Folgerung aus den Axiomen (A1) - (A5) ist, geht in eine gültige Aussage über, wenn man in ihr überall $\sqcap$ und $\sqcup$ sowie 0 und 1 vertauscht.

Satz 2.

Für alle $a \in B$ gilt $a \sqcap 0 = 0$ und $a \sqcup 1 = 1$.

Beweis. Es gilt:

$$a \sqcap 0 \overset{(A5)}{=} a \sqcap \big(a \sqcap \overline{a}\big) \overset{(A1)}{=} \big(a \sqcap a\big) \sqcap \overline{a} \overset{\text{Satz 1}}{=} a \sqcap \overline{a} \overset{(A5)}{=} 0.$$

Die Behauptung $a \sqcup 1 = 1$ folgt aus $a \sqcap 0 = 0$ nach dem Dualitätsprinzip. $\square$

Zum Beweis von Satz 2 haben wir nur die Axiome und den bereits bewiesenen Satz 1 benutzt. In ähnlicher Weise könnten wir fortfahren und eine ganze Reihe von gültigen Sätzen für Boolesche Algebren beweisen und dadurch die mathematische Theorie der Booleschen Algebren aufbauen[3].

Die Vorgehensweise, an den Anfang einer Theorie einige Aussagen als Axiome zu stellen, um dann aus ihnen durch *Deduktion* (logisches Schließen) eine mathematische Theorie zu entwickeln, ist typisch für die gesamte Mathematik. Man spricht von der *axiomatischen Methode* (oder auch *axiomatisch deduktiven Methode*). Beispiele für diese Vorgehensweise werden uns noch häufig begegnen.

[3] Wir können und wollen dies hier nicht durchführen. Uns geht es hier in erster Linie um die Darlegung der *axiomatischen Methode*. Deshalb begnügen wir uns mit den Herleitungen der beiden Sätze 1 und 2. Ausführliche Darstellungen findet man beispielsweise in:

- J. E. Whitesitt: Boolesche Algebra und ihre Anwendungen, Vieweg, Braunschweig (1968)
- R. Lidl, G. Pilz: Angewandte abstrakte Algebra II. B.I.-Wissenschaftsverlag, Mannheim (1982)
- M. Rueff, M. Jeger: Sets and Boolean Algebra, George Allen and Unwin Ltd., London (1970)
- W. Dörfler: Mathematik für Informatiker, Band 1, Hanser, München (1977)

Beispiele für Boolesche Algebren

1. Die Mengenalgebra

Hier ist B die Potenzmenge $\mathcal{P}(M)$ einer Menge M (also: $B = \mathcal{P}(M)$), die beiden binären Verknüpfungen sind Durchschnitt und Vereinigung von Mengen, das Nullelement ist die leere Menge und das Einselement ist die Menge M.

2. Die Schaltalgebra

Bei dieser Booleschen Algebra ist die zugrundeliegende Menge B die Menge $\{0, 1\}$ (also: $B = \{0, 1\}$); die Elemente 0 und 1 nennt man in diesem Zusammenhang *Wahrheitswerte*. Die beiden binären Verknüpfungen sind die bekannten Operationen $\wedge$ und $\vee$ (Konjunktion und Disjunktion), die sich durch die folgenden Verknüpfungstafeln definieren lassen:

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

$\vee$	0	1
0	0	1
1	1	1

Die Komplementbildung entspricht der Negation: $\overline{0} = 1$, $\overline{1} = 0$.

2 Elementare Zahlentheorie und Kombinatorik

2.1 Natürliche Zahlen und vollständige Induktion

Obwohl uns die natürlichen Zahlen 1, 2, 3, ... vertraut sind, wollen wir sie doch etwas genauer studieren; vor allem soll die *Methode der vollständigen Induktion* behandelt werden. Zunächst wollen wir jedoch einige einfache Eigenschaften der Addition und Multiplikation natürlicher Zahlen festhalten:

(1) Assoziativgesetze:
- $a + \big(b + c\big) = \big(a + b\big) + c$
- $a \cdot \big(b \cdot c\big) = \big(a \cdot b\big) \cdot c$

(2) Kommutativgesetze:
- $a + b = b + a$
- $a \cdot b = b \cdot a$

(3) Distributivgesetz:
- $a \cdot \big(b + c\big) = a \cdot b + a \cdot c$

(4) Existenz eines neutralen Elements der Multiplikation:
- $a \cdot 1 = a$

Vollständige Induktion ist eine häufig angewandte Methode, sowohl in der Mathematik als auch in der Informatik. Sie dient

- zum Nachweis der Richtigkeit von Behauptungen oder Vermutungen (vollständige Induktion als Beweismethode);
- zur Definition von Objekten oder Operationen (vollständige Induktion als Definitionsmethode); mit dieser Methode gewonnene Definitionen werden auch *rekursive Definitionen* genannt.

Vollständige Induktion als Beweismethode wird bei Problemen der folgenden Art angewandt: Für jede natürliche Zahl n sei $A(n)$ eine Aussage. Es soll bewiesen werden, dass $A(n)$ für alle natürlichen Zahlen n gilt, d.h., es soll die Gültigkeit der unendlich vielen Aussagen $A(1)$, $A(2)$, $A(3)$, ... nachgewiesen werden. Hierzu ist es häufig günstig, vollständige Induktion einzusetzen.

Beweismethode der vollständigen Induktion.
Um eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ zu beweisen, genügt es, Folgendes zu zeigen:

(I) *Induktionsanfang*
$A(1)$ ist richtig.

(II) *Induktionsschritt*
Für jedes $n \in \mathbb{N}$ gilt: Falls $A(n)$ richtig ist, so ist auch $A(n+1)$ richtig.

Wir erläutern die **Idee**, die dieser Methode zugrunde liegt. Zu beweisen sind die unendlich vielen Aussagen $A(1)$, $A(2)$, $A(3)$, ... Wieso hat man das erledigt, wenn man (I) und (II) nachweist? Das ist einfach zu erkennen: Hat man (I) und (II) nachgewiesen, so gilt aufgrund von (I) zunächst einmal $A(1)$. Hieraus folgt, wenn man (II) für den Fall $n = 1$ anwendet, dass auch $A(2)$ richtig ist. Wendet man nun (II) für den Fall $n = 2$ an, so folgt aus der Richtigkeit von $A(2)$, dass auch $A(3)$ richtig ist. Aus der Richtigkeit von $A(3)$ ergibt sich durch Anwendung von (II), dass auch $A(4)$ richtig ist. Analog erhält man Schritt

für Schritt die Richtigkeit von $A(5)$, $A(6)$ usw. Schematisch lässt sich das so zusammenfassen:

$$\underbrace{A(1)}_{\text{richtig wegen (I)}} \overset{(II)}{\Rightarrow} A(2) \overset{(II)}{\Rightarrow} A(3) \overset{(II)}{\Rightarrow} A(4) \overset{(II)}{\Rightarrow} \dots$$

Wir wollen nun die Anwendung von vollständiger Induktion an einem **Beispiel** vorführen. Hierzu betrachten wir die folgende Aussage $A(n)$:

Die Summe der ersten n natürlichen Zahlen (d.h. $1+2+\ldots+n$) ist gleich $\dfrac{n(n+1)}{2}$.

Als Gleichung geschrieben lautet diese Aussage:

$$A(n): \quad 1+2+\ldots+n = \frac{n(n+1)}{2}\ .$$

Dass dies für einzelne nicht allzu große natürliche Zahlen n richtig ist, lässt sich leicht feststellen: Man setzt einfach für n die betreffende Zahl ein, rechnet den Wert der linken und rechten Seite der Gleichung aus und vergleicht die Ergebnisse. Auf diese Art kann man beispielsweise nachweisen, dass $A(n)$ für $n = 1, 2, 3, 4$ richtig ist:

$$\begin{aligned}
A(1): \quad & 1 &&= 1 &&= \frac{1\cdot(1+1)}{2}\\
A(2): \quad & 1+2 &&= 3 &&= \frac{2\cdot(2+1)}{2}\\
A(3): \quad & 1+2+3 &&= 6 &&= \frac{3\cdot(3+1)}{2}\\
A(4): \quad & 1+2+3+4 &&= 10 &&= \frac{4\cdot(4+1)}{2}
\end{aligned}$$

Mit vollständiger Induktion lässt sich zeigen, dass $A(n)$ nicht nur für bestimmte $n \in \mathbb{N}$, sondern *für alle* $n \in \mathbb{N}$ gilt:

(I) *Induktionsanfang*

$A(1)$ ist richtig, da $1 = \frac{1\cdot(1+1)}{2}$ gilt (wie oben bereits festgestellt).

(II) *Induktionsschritt*

Es sei $n \in \mathbb{N}$ eine beliebig gewählte natürliche Zahl; wir setzen voraus, dass $A(n)$ für dieses n richtig ist, d.h., es gelte für dieses n:

$$1+2+\ldots+n = \frac{n\big(n+1\big)}{2}\ . \tag{2.1}$$

Wir haben zu zeigen, dass unter dieser Voraussetzung auch $A(n+1)$ richtig ist, d.h., wir müssen nachweisen, dass

$$1+2+\ldots+n+\big(n+1\big) = \frac{\big(n+1\big)\big((n+1)+1\big)}{2} \tag{2.2}$$

gilt. Dies ergibt sich durch folgende Rechnung:

$$\begin{aligned}
1+2+\ldots+n+\big(n+1\big) &\overset{(2.1)}{=} \frac{n\big(n+1\big)}{2}+\big(n+1\big)\\
&\overset{\text{Zusammenfassen}}{=} \frac{n\big(n+1\big)+2\big(n+1\big)}{2}\\
&\overset{(n+1)\text{ ausklammern}}{=} \frac{\big(n+1\big)\big(n+2\big)}{2}\\
&= \frac{\big(n+1\big)\big((n+1)+1\big)}{2}
\end{aligned}$$

Damit sind (I) und (II) gezeigt; nach dem Induktionsprinzip[1] gilt $A(n)$ also für alle $n \in \mathbb{N}$. □

Im Induktionsschritt geht man also wie folgt vor: Man wählt sich ein beliebiges $n \in \mathbb{N}$ und nimmt *für dieses fest gewählte* n an, dass $A(n)$ richtig ist. Dies nennt man die *Induktionsannahme*. (In unserem obigen Beispiel war (2.1) die Induktionsannahme.) Sodann weist man die Richtigkeit von $A(n+1)$ nach; im Laufe dieses Nachweises (nicht notwendigerweise am Anfang!) wird man die Induktionsannahme ein- oder auch mehrmals benutzen.

Wir wollen unser Ergebnis noch ausdrücklich als Satz festhalten.

Satz 1.
Für alle natürlichen Zahlen n gilt:

$$1 + 2 + \ldots + n \quad = \quad \frac{n\big(n+1\big)}{2} \; .$$

Wegen der Wichtigkeit des Induktionsprinzips wollen wir uns seine Anwendung noch an zwei weiteren Beispielen anschauen.

Satz 2.
Für alle natürlichen Zahlen n gilt:

$$1^2 + 2^2 + \ldots + n^2 \quad = \quad \frac{n\big(n+1\big)\big(2n+1\big)}{6} \; .$$

Beweis. Die Gleichung $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$ sei mit $A(n)$ bezeichnet. Wir zeigen mit vollständiger Induktion, dass $A(n)$ für alle $n \in \mathbb{N}$ gilt.

(I) *Induktionsanfang*

Die Gleichung $A(1)$ ist richtig, wie man durch Einsetzen leicht sieht:

$$1^2 = 1 \quad \text{und} \quad \frac{1\big(1+1\big)\big(2\cdot 1+1\big)}{6} = 1.$$

(II) *Induktionsschritt*

Es sei $n \in \mathbb{N}$ beliebig gewählt; wir setzen voraus (Induktionsannahme), dass die Gleichung $A(n)$ für dieses fest gewählte n richtig ist, d.h., es gelte für dieses n:

$$1^2 + 2^2 + \ldots + n^2 \quad = \quad \frac{n\big(n+1\big)\big(2n+1\big)}{6} \tag{2.3}$$

Wir zeigen nun, dass (unter der Voraussetzung (2.3)) auch die Gleichung $A(n+1)$ gilt, d.h., wir weisen Folgendes nach:

$$1^2 + 2^2 + \ldots + n^2 + \big(n+1\big)^2 \quad = \quad \frac{\big(n+1\big)\big((n+1)+1\big)\big(2(n+1)+1\big)}{6}$$

Dies ergibt sich so:

$$\begin{aligned}
1^2 + 2^2 + \ldots + n^2 + \big(n+1\big)^2 \quad &\overset{(2.3)}{=} \quad \frac{n\big(n+1\big)\big(2n+1\big)}{6} + \big(n+1\big)^2 \\
&\overset{\text{Zusammenfassen}}{=} \quad \frac{n\big(n+1\big)\big(2n+1\big) + 6\big(n+1\big)^2}{6} \\
&\overset{(n+1)\text{ ausklammern}}{=} \quad \frac{\big(n+1\big)\big(n(2n+1) + 6(n+1)\big)}{6} \\
&= \quad \frac{\big(n+1\big)\big((n+1)+1\big)\big(2(n+1)+1\big)}{6}
\end{aligned}$$

[1] Statt Beweismethode der vollständigen Induktion sagt man auch *Induktionsprinzip*.

Die letzte Gleichheit gilt, da $n(2n+1)+6(n+1) = \big((n+1)+1\big)\big(2(n+1)+1\big)$ gilt, wie man durch „einfaches Ausrechnen“ bestätigt:

$$\begin{aligned} n(2n+1)+6(n+1) &= 2n^2+n+6n+6 \\ &= 2n^2+7n+6 \end{aligned}$$

$$\begin{aligned} \big((n+1)+1\big)\big(2(n+1)+1\big) &= \big(n+2\big)\big(2n+3\big) \\ &= 2n^2+3n+4n+6 \\ &= 2n^2+7n+6 \end{aligned}$$

Aus (I) und (II) folgt nach dem Induktionsprinzip die Behauptung von Satz 2. □

Im nächsten Beispiel benutzen wir die folgenden einfachen Regeln für das Rechnen mit Ungleichungen. Eine ausführlichere Behandlung des Rechnens mit Ungleichungen erfolgt in Abschnitt 2.2. Der Doppelpfeil $\Rightarrow$ bezeichnet wie üblich die Implikation; $A \Rightarrow B$ bedeutet: „Aus A folgt B“ (für Aussagen A und B).

(5) $a \le b \wedge b \le c \Rightarrow a \le c$ (für $a, b, c \in \mathbb{N}$)

(6) $a \le b \Rightarrow a + c \le b + c$ (für $a, b, c \in \mathbb{N}$)

Behauptung: Für alle $n \in \mathbb{N}$ gilt $2n \le 2^n$.

Beweis.

Mit $A(n)$ sei die Aussage $2n \le 2^n$ bezeichnet.

(I) *Induktionsanfang*

$A(1)$ ist richtig, da $2 \cdot 1 \le 2^1$ gilt.

(II) *Induktionsschritt*

Es sei $n \in \mathbb{N}$ beliebig gewählt. Wir setzen voraus, dass $A(n)$ für dieses n gilt, d.h., es gelte $2n \le 2^n$ (Induktionsannahme). Wir wollen zeigen, dass dann auch $A(n+1)$ gilt, d.h., wir haben $2(n+1) \le 2^{n+1}$ zu zeigen. Wir starten den Nachweis dieser Ungleichung, indem wir die linke Seite ausmultiplizieren:

$$2(n+1) = 2n + 2.$$

Auf den Term $2n$ können wir die Induktionsannahme anwenden und erhalten

$$2(n+1) = 2n + 2 \le 2^n + 2.$$

Wegen $2 \le 2^n$ folgt

$$2(n+1) \le 2^n + 2 \le 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$$

womit $A(n+1)$ gezeigt ist.

Aus (I) und (II) folgt nach dem Induktionsprinzip die Behauptung. □

Beweismethode der vollständigen Induktion (2. Fassung).

Häufig verwendet man auch folgende *Variante des Induktionsprinzips*: Um eine Aussage $A(n)$ für alle natürlichen Zahlen n zu beweisen, genügt es, Folgendes zu zeigen:

(I) *Induktionsanfang*

$A(1)$ ist richtig.

(II) *Induktionsschritt*

Für jedes $n \in \mathbb{N}$ gilt: Falls alle Aussagen $A(1), \ldots, A(n)$ richtig sind, so ist auch $A(n+1)$ richtig.

In dieser 2. Fassung, die wie gesagt ebenfalls häufig verwendet wird, wird die Voraussetzung, dass $A(1), \ldots, A(n)$ richtig sind, als Induktionsannahme bezeichnet.

Weitere Varianten ergeben sich, wenn man in einer der beiden Fassungen anstelle von $n = 1$ einen anderen „Anfangswert“ n_0 wählt. Wir geben diese Variante explizit für die erste Fassung des Induktionsprinzips an.

Beweismethode der vollständigen Induktion (1. Fassung mit beliebigem „Anfangswert“ n_0).

Es sei $n_0 \in \mathbb{N}$ oder $n_0 = 0$. Um eine Aussage $A(n)$ für alle ganzen Zahlen $n \geq n_0$ zu beweisen, genügt es, Folgendes zu zeigen:

(I) *Induktionsanfang*

$A(n_0)$ ist richtig.

(II) *Induktionsschritt*

Für jedes $n \geq n_0$ gilt: Falls $A(n)$ richtig ist, so ist auch $A(n+1)$ richtig.

Diese Varianten lassen sich auf die ursprüngliche Version zurückführen, d.h., ihre Richtigkeit lässt sich mit Hilfe der ursprünglichen Version beweisen.

Wir kommen nun zum Begriff der *rekursiven Definition* (auch *Definition durch vollständige Induktion* genannt).

Betrachten wir ein **Beispiel**. Wir definieren eine unendliche Folge von natürlichen Zahlen a_1, a_2, a_3, ... durch die folgenden beiden Bedingungen:

(I) $a_1 = 1$

(II) $a_{n+1} = 2 \cdot a_n + 1$ für alle $n \in \mathbb{N}$.

Wir wollen die ersten vier Glieder a_1, a_2, a_3 und a_4 berechnen.

Nach (I) gilt zunächst einmal

$$a_1 = 1.$$

Wenden wir (II) auf den Fall $n = 1$ an, so folgt

$$a_2 = 2 \cdot a_1 + 1 = 2 \cdot 1 + 1 = 3.$$

Wenden wir nun (II) auf den Fall $n = 2$ an, so folgt

$$a_3 = 2 \cdot a_2 + 1 = 2 \cdot 3 + 1 = 7.$$

Durch Anwendung von (II) auf den Fall $n = 3$ folgt

$$a_4 = 2 \cdot a_3 + 1 = 2 \cdot 7 + 1 = 15.$$

In obiger Definition wird die Zahl a_{n+1} also dadurch definiert, dass man die bereits definierte Zahl a_n verdoppelt und anschließend 1 addiert. Definitionen dieser Art, in denen eine Folge von Objekten a_1, a_2, a_3, ... dadurch definiert wird, dass man zur Definition des Objektes a_{n+1} alle oder einen Teil der bereits definierten Objekte a_1, ..., a_n heranzieht, nennt man *rekursive*[2] *Definitionen*.

Drei weitere **typische Beispiele** für rekursive Definitionen:

1. Die Folge f_0, f_1, f_2, ... der *Fibonacci-Zahlen* wird rekursiv definiert durch

(I) $f_0 = 0$, $f_1 = 1$

(II) $f_n = f_{n-1} + f_{n-2}$ für $n \geq 2$

Hier werden durch die Anfangsbedingungen (I) die ersten beiden Folgenglieder f_0 und f_1 direkt festgelegt; die n-te Fibonacci-Zahl f_n ergibt sich für $n \geq 2$ aus den bereits definierten Zahlen f_{n-1}

[2] von lat. recurrere = zurücklaufen

und f_{n-2}, indem man ihre Summe bildet. Die ersten zehn dieser Zahlen:

$$\begin{array}{lllllll}
f_0 & = & 0 & & & & \\
f_1 & = & 1 & & & & \\
f_2 & = & f_1 + f_0 & = & 1+0 & = & 1 \\
f_3 & = & f_2 + f_1 & = & 1+1 & = & 2 \\
f_4 & = & f_3 + f_2 & = & 2+1 & = & 3 \\
f_5 & = & f_4 + f_3 & = & 3+2 & = & 5 \\
f_6 & = & f_5 + f_4 & = & 5+3 & = & 8 \\
f_7 & = & f_6 + f_5 & = & 8+5 & = & 13 \\
f_8 & = & f_7 + f_6 & = & 13+8 & = & 21 \\
f_9 & = & f_8 + f_7 & = & 21+13 & = & 34
\end{array}$$

2. Die n-te Potenz einer Zahl a ($n \in \mathbb{N}$) lässt sich folgendermaßen rekursiv definieren:

(I) $a^1 := a$

(II) $a^{n+1} := a^n \cdot a$

Das definitorische Gleichheitszeichen := dient hierbei nur zur Verdeutlichung der Tatsache, dass es sich bei diesen Gleichungen um Definitionsgleichungen handelt.

3. Wir definieren Zeichenreihen, die aus den beiden Zeichen □ und ⋆ gebildet werden.

(I) Die erste Zeichenreihe sei □ ⋆.

(II) Die $(n+1)$-te Zeichenreihe entstehe aus der n-ten Zeichenreihe, indem man die n-te Zeichenreihe in umgekehrter Reihenfolge aufschreibt und danach rechts erst □ und dann ⋆ anfügt.

Es ergibt sich:

□ ⋆

⋆ □ □ ⋆

⋆ □ □ ⋆ □ ⋆

⋆ □ ⋆ □ □ ⋆ □ ⋆

⋆ □ ⋆ □ □ ⋆ □ ⋆ □ ⋆

⋆ □ ⋆ □ ⋆ □ □ ⋆ □ ⋆ □ ⋆

Bemerkung zur axiomatischen Einführung der natürlichen Zahlen

Wir haben uns in diesem Abschnitt auf den Standpunkt gestellt, dass wir wissen, was die natürlichen Zahlen 1, 2, 3, ... sind und wie man mit ihnen rechnet (siehe Regeln (1) - (4) am Anfang dieses Abschnitts sowie Regeln (5) und (6) für das Rechnen mit $\leq$).

Eine andere Vorgehensweise ist, zunächst einmal so zu tun, als wüssten wir noch nichts über die natürlichen Zahlen; nicht, wie man mit ihnen rechnet, und nicht einmal, dass es sich bei den natürlichen Zahlen um die uns vertrauten Objekte 1, 2, 3, ... handelt. Man nimmt diesen Standpunkt ein, wenn man daran interessiert ist, die Grundlagen, auf denen der Umgang mit natürlichen Zahlen beruht, genau zu klären. Man führt dann die natürlichen Zahlen durch Axiome ein. Das bekannteste Axiomensystem für natürliche Zahlen sind die *Peano-Axiome*[3].

[3] nach G. Peano (1858-1932), italienischer Mathematiker.

Peano-Axiome.

1. 1 ist eine natürliche Zahl.
2. Jeder natürlichen Zahl n ist eine, und zwar genau eine, natürliche Zahl n' zugeordnet, die der Nachfolger von n genannt wird.
3. 1 ist kein Nachfolger.
4. Sind die natürlichen Zahlen n und m verschieden, so sind auch ihre Nachfolger n' und m' verschieden.
5. Enthält eine Menge M natürlicher Zahlen die Zahl 1 und folgt aus $n \in M$ stets $n' \in M$, so besteht M aus allen natürlichen Zahlen.

Ausgehend von diesen Axiomen kann man nun die Operationen + und · sowie die Relation $\leq$ für natürliche Zahlen geeignet einführen[4]. In diesem Rahmen beweist man dann beispielsweise die Regeln (1) - (6). Das fünfte Peano-Axiom wird auch *Induktionsaxiom* genannt, weil es sowohl die Grundlage für den Beweis durch vollständige Induktion ist als auch für die Möglichkeit, rekursiv zu definieren.

Anmerkung zur Sprechweise: Anstelle von *vollständiger Induktion* sagt man häufig auch einfach nur *Induktion* oder auch *mathematische Induktion*.

2.2 Ganze und rationale Zahlen

Ähnlich wie wir im letzten Abschnitt die Menge $\mathbb{N}$ der natürlichen Zahlen (zusammen mit den auf $\mathbb{N}$ erklärten Operationen + und · sowie der Kleiner-Gleich-Beziehung $\leq$) als bekannt vorausgesetzt haben, wollen wir in diesem Abschnitt (ebenfalls zusammen mit den Operationen + und · und der Kleiner-Gleich-Beziehung $\leq$) als bekannt voraussetzen:

- Die Menge $\mathbb{Z}$ der ganzen Zahlen. Dies ist die Menge aller natürlichen Zahlen erweitert um 0 und um die Zahlen -1, -2, -3, ...; also:
$$\mathbb{Z} = \Big\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\Big\}.$$
- Die Menge $\mathbb{Q}$ der rationalen Zahlen, d.h. die Menge aller Zahlen, die sich als Brüche $\frac{m}{n}$ mit $m, n \in \mathbb{Z}$ und $n \neq 0$ darstellen lassen.

Wir wollen uns im Folgenden die Addition und Multiplikation ganzer und rationaler Zahlen etwas genauer anschauen; dies wird auf die Feststellung hinauslaufen, dass die rationalen Zahlen $\mathbb{Q}$ zusammen mit den Operationen + und · ein Beispiel für die *algebraische Struktur eines Körpers* sind, während die ganzen Zahlen $\mathbb{Z}$ zusammen mit + und · die (schwächere) *algebraische Struktur eines Rings* besitzen. (Die Begriffe *Körper* und *Ring* werden später noch wesentlich ausführlicher behandelt werden.)

Wir weisen zunächst darauf hin, dass $\mathbb{Z} \subseteq \mathbb{Q}$ gilt. (Man beachte, dass sich jede ganze Zahl m als Bruch darstellen lässt: $m = \frac{m}{1}$.) Der Vollständigkeit halber erinnern wir daran, wie man Brüche addiert und multipliziert:

$$\begin{aligned} \frac{m}{n} + \frac{m'}{n'} &= \frac{m \cdot n' + m' \cdot n}{n \cdot n'} \\ \frac{m}{n} \cdot \frac{m'}{n'} &= \frac{m \cdot m'}{n \cdot n'} \end{aligned}$$

Für die Addition und Multiplikation rationaler Zahlen gelten folgende Regeln ($a, b, c \in \mathbb{Q}$):

(1) Assoziativgesetze:

[4] Wir verzichten hier auf die Einzelheiten. Genaueres findet man etwa in: A. Oberschelp: Aufbau des Zahlensystems, Vandenhoeck und Ruprecht, Göttingen 1972.

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

(2) Kommutativgesetze:

- $a + b = b + a$
- $a \cdot b = b \cdot a$

(3) Distributivgesetz:

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

(4) Existenz neutraler Elemente:

Es gibt in $\mathbb{Q}$ zwei verschiedene Elemente 0 und 1, welche die Eigenschaft haben, dass für jedes $a \in \mathbb{Q}$ gilt:

- $a + 0 = a$
- $a \cdot 1 = a$

(5) Existenz inverser Elemente:

Zu jedem $a \in \mathbb{Q}$ gibt es ein Element $-a \in \mathbb{Q}$ und zu jedem $a \in \mathbb{Q}$, $a \neq 0$, ein Element $a^{-1} \in \mathbb{Q}$, für die gilt:

- $a + (-a) = 0$
- $a \cdot a^{-1} = 1$

(Sei $a = \frac{m}{n} \in \mathbb{Q} \setminus \{0\}$. Dann gilt für das inverse Element der Multiplikation a^{-1} natürlich $a^{-1} = \frac{n}{m}$.)

Definition.
K sei eine Menge, auf der zwei binäre Operationen + („Addition“) und $\cdot$ („Multiplikation“) erklärt sind. K heißt ein *Körper*, falls Folgendes erfüllt ist $(a, b, c \in K)$:

(K1) Assoziativgesetze:

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

(K2) Kommutativgesetze:

- $a + b = b + a$
- $a \cdot b = b \cdot a$

(K3) Distributivgesetz:

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

(K4) Existenz neutraler Elemente:

Es gibt in K zwei verschiedene Elemente 0 und 1, welche die Eigenschaft haben, dass für jedes $a \in K$ gilt:

- $a + 0 = a$
- $a \cdot 1 = a$

(K5) Existenz inverser Elemente:

Zu jedem $a \in K$ gibt es ein Element $-a \in K$ und zu jedem $a \in K$, $a \neq 0$, ein Element $a^{-1} \in K$, für die gilt:

- $a + (-a) = 0$
- $a \cdot a^{-1} = 1$

Man nennt (K1) - (K5) die *Körperaxiome*. Für die rationalen Zahlen $\mathbb{Q}$ zusammen mit der üblichen Addition und Multiplikation sind, wie wir oben gesehen haben, (K1) - (K5) erfüllt. Daher spricht man vom *Körper $\mathbb{Q}$ der rationalen Zahlen*.

Die ganzen Zahlen $\mathbb{Z}$ bilden *keinen* Körper: Es sind zwar (K1) - (K4) auch für $\mathbb{Z}$ erfüllt; ferner ist der erste Teil von (K5) erfüllt; aber der zweite Teil ist nicht erfüllt: Beispielsweise gibt es zu 2 innerhalb von $\mathbb{Z}$ kein inverses Element der Multiplikation (d.h., es gibt keine ganze Zahl z, für die $2z = 1$ gilt). Daher können wir nur feststellen: Die ganzen Zahlen bilden einen Ring, genannt *Ring der ganzen Zahlen*. (Die genaue Definition der algebraischen Struktur eines Ringes wird später gegeben werden, wenn wir noch andere Beispiele für Ringe kennen gelernt haben.)

Neben der algebraischen Struktur eines Körpers besitzen die rationalen Zahlen eine weitere wichtige Eigenschaft: Die rationalen Zahlen sind *angeordnet* durch die Kleiner-Beziehung $<$. Für je zwei verschiedene rationale Zahlen a und b gilt stets entweder $a < b$ oder $b < a$. Für das Rechnen mit Ungleichungen gelten folgende Regeln:

1. $a < b \wedge b < c \Rightarrow a < c$

2. $a < b \Rightarrow a + c < b + c$

3. $a < b \Rightarrow a \cdot c < b \cdot c$, falls $c > 0$

4. $a < b \Rightarrow a \cdot c > b \cdot c$, falls $c < 0$

Das Zeichen $a \leq b$ bedeutet, dass $a < b$ oder $a = b$ gilt. Für das Rechnen mit $\leq$ gelten ähnliche Regeln wie für das Rechnen mit $<$:

1. $a \leq b \wedge b \leq c \Rightarrow a \leq c$

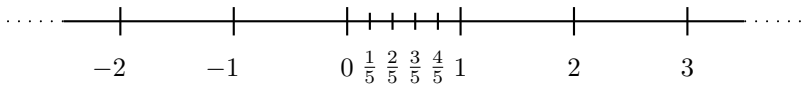
2. $a \leq b \Rightarrow a + c \leq b + c$

3. $a \leq b \Rightarrow a \cdot c \leq b \cdot c$, falls $c \geq 0$

4. $a \leq b \Rightarrow a \cdot c \geq b \cdot c$, falls $c \leq 0$

Veranschaulichung der Zahlen auf der Zahlengeraden

Man veranschaulicht Zahlen durch Punkte auf einer Geraden, die *Zahlengerade* genannt wird, indem man einen beliebigen Punkt auf dieser Geraden als Nullpunkt 0 festsetzt und einen anderen, rechts von 0 gelegenen Punkt als den Punkt 1. Dadurch legt man den Maßstab der Darstellung fest. Die Punkte 2, 3, ... findet man, indem man 2-mal, 3-mal, ... die Strecke $\overline{01}$ vom Nullpunkt aus nach rechts abträgt. Die negativen Zahlen -1, -2, ... werden entsprechend vom Nullpunkt aus nach links abgetragen. Ähnlich wie die ganzen Zahlen veranschaulicht man die rationalen Zahlen als Punkte auf der Zahlengeraden. Beispielsweise findet man die Punkte, die den Zahlen $\frac{1}{5}$, $\frac{2}{5}$, $\frac{3}{5}$ und $\frac{4}{5}$ entsprechen, indem man die Strecke $\overline{01}$ in fünf gleichgroße Teile teilt:



Wählt man zwei verschiedene Punkte A und B auf der Zahlengeraden, so kann man immer eine rationale Zahl finden, deren zugehöriger Punkt auf der Zahlengeraden zwischen A und B liegt. Man sagt hierzu auch: Die rationalen Zahlen sind *dicht* auf der Zahlengeraden. Trotzdem füllen die rationalen Zahlen die Zahlengerade *nicht vollständig* aus, wie wir im nächsten Abschnitt sehen werden.

2.3 Die reellen Zahlen

Mit $\sqrt{2}$ bezeichnet man bekanntlich die positive Lösung der Gleichung $x^2 = 2$.

Frage: Ist $\sqrt{2}$ eine rationale Zahl?

Die **Antwort** lautet nein, wie der folgende Satz zeigt.

Satz.
Es gibt keine rationale Zahl a, für die $a^2 = 2$ gilt.

Der Beweis dieses Satzes ist ein Beispiel für eine wichtige Beweismethode, die Methode des *Widerspruchsbeweises*. Bevor wir den Beweis durchführen, sei an Folgendes erinnert: Eine ganze Zahl m heißt *gerade*, wenn sie durch 2 teilbar ist; oder anders gesagt: m ist gerade, wenn $m = 2k$ für ein $k \in \mathbb{Z}$ gilt. Andernfalls heißt m *ungerade*; m ist also ungerade, wenn $m = 2k + 1$ für ein $k \in \mathbb{Z}$ gilt. Das Quadrat m^2 einer Zahl m ist genau dann gerade, wenn m gerade ist, wie man an den folgenden beiden Gleichungen sehen kann:

$$\begin{aligned} (2k)^2 &= 4 \cdot k^2 = 2(2k^2) \\ (2k+1)^2 &= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \end{aligned}$$

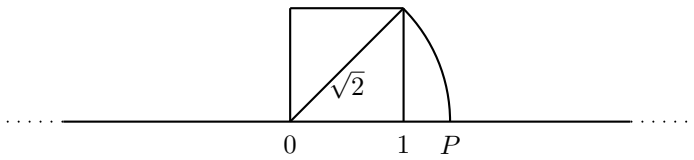
Beweis des Satzes. Wir wollen annehmen, dass die Aussage des Satzes falsch sei, d.h., wir nehmen an, dass es ein $a \in \mathbb{Q}$ gibt, für das $a^2 = 2$ gilt. Diese Annahme führen wir zum Widerspruch, woraus folgt, dass der Satz richtig ist.

Da $a \in \mathbb{Q}$ gilt, lässt sich a als ein Bruch darstellen, d.h., $a = \frac{m}{n}$ für $m, n \in \mathbb{Z}$ mit $n \neq 0$. Wir können voraussetzen, dass der Bruch $\frac{m}{n}$ in gekürzter Form vorliegt. Aus $a^2 = 2$ und $a = \frac{m}{n}$ folgt $\left(\frac{m}{n}\right)^2 = 2$, woraus folgt:

$$m^2 = 2n^2 \tag{2.4}$$

Also ist m^2 eine gerade Zahl. Dann ist aber auch m eine gerade Zahl (wie oben bemerkt), d.h., $m = 2k$ für ein $k \in \mathbb{Z}$. Setzt man dies in (2.4) ein, so folgt $4k^2 = 2n^2$, woraus $2k^2 = n^2$ folgt. Also ist n^2 eine gerade Zahl, woraus folgt, dass auch n gerade ist. Demnach gilt $n = 2k'$ für ein $k' \in \mathbb{Z}$. Wir haben also $m = 2k$ und $n = 2k'$ gezeigt. Dies ist ein Widerspruch zur Voraussetzung, dass $\frac{m}{n}$ in gekürzter Form vorliegt. Die Annahme, unser Satz sei falsch, ist also zum Widerspruch geführt worden, womit der Satz bewiesen ist. □

Veranschaulicht man Zahlen, wie im letzten Abschnitt vorgeführt, durch Punkte auf der Zahlengeraden, so entspricht der Zahl $\sqrt{2}$ ein wohlbestimmter Punkt: Man konstruiert über der Strecke $\overline{01}$ ein Quadrat mit Seitenlänge 1 (siehe Zeichnung); die Diagonale hat dann die Länge $\sqrt{2}$ (nach dem Satz des Pythagoras); klappt man nun diese Diagonale herunter auf die Zahlengerade, so erhält man den Punkt P, der der Zahl $\sqrt{2}$ entspricht.



Wir haben gesehen:

1. Es ist innerhalb der rationalen Zahlen $\mathbb{Q}$ nicht möglich, eine so einfache Gleichung wie $x^2 = 2$ zu lösen (da $\sqrt{2} \notin \mathbb{Q}$).
2. Es gibt Punkte auf der Zahlengeraden, denen keine rationale Zahl entspricht.

Ähnlich dem obigen Beispiel $\sqrt{2}$ gibt es viele Zahlen, denen ein Punkt auf der Zahlengeraden entspricht, die aber nicht in $\mathbb{Q}$ liegen: beispielsweise Wurzelausdrücke (wie $\sqrt{3}$, $\sqrt[3]{2}$, $\sqrt{5}$ oder $\sqrt[5]{11}$), die Kreiszahl π oder die Eulersche Zahl e. Man kann diese Beobachtungen als Begründung dafür ansehen, warum man die Menge $\mathbb{Q}$ noch einmal erweitert, nämlich zur *Menge $\mathbb{R}$ der reellen Zahlen*. Wie man diese Erweiterung durchführt, wollen wir an dieser Stelle nicht diskutieren, da eine genaue Durchführung zu aufwändig wäre. Wir begnügen uns damit, die folgenden Tatsachen über die reellen Zahlen festzuhalten:

1. Die Erweiterung von $\mathbb{Q}$ zu $\mathbb{R}$ führt dazu, dass jedem Punkt der Zahlengeraden genau eine reelle Zahl entspricht, und dass auch umgekehrt zu jeder reellen Zahl genau ein solcher Punkt gehört.
2. Auf $\mathbb{R}$ sind binäre Operationen $+$ und $\cdot$ sowie eine Kleiner-Beziehung $<$ erklärt. Ebenso wie die rationalen Zahlen $\mathbb{Q}$ (vgl. Abschnitt 2.2) bilden die reellen Zahlen einen Körper. Man spricht dementsprechend auch vom *Körper der reellen Zahlen*. Die Regeln über das Rechnen mit Ungleichungen (vgl. Abschnitt 2.2) gelten ebenso für $\mathbb{R}$.
3. Man kann die reellen Zahlen auch beschreiben als die Menge der Zahlen, die durch einen endlichen oder unendlichen Dezimalbruch darstellbar sind. Den endlichen und periodischen Dezimalbrüchen entsprechen genau die rationalen Zahlen $\mathbb{Q}$, während den nicht-periodischen Dezimalbrüchen die Zahlen aus $\mathbb{R} \setminus \mathbb{Q}$ entsprechen.

2.4 Teilbarkeit, Primzahlen und Euklidischer Algorithmus

In diesem Abschnitt seien mit kleinen lateinischen Buchstaben stets ganze Zahlen bezeichnet.

Definition 1.
Man nennt b einen *Teiler* von a, falls es ein c gibt, für das $a = b \cdot c$ gilt (für $a, b, c \in \mathbb{Z}$).

Ist b ein Teiler von a, so sagt man „b *teilt* a“ und nennt a ein *Vielfaches* von b.

Schreibweisen:

- $b \mid a$ bedeutet: „b ist ein Teiler von a“.
- $b \nmid a$ bedeutet: „b ist kein Teiler von a“.

Einige Eigenschaften der Teilbarkeitsbeziehung $|$:

(1) Gilt $c \mid b$ und $b \mid a$, dann gilt auch $c \mid a$.

(2) Aus $b_1 \mid a_1$ und $b_2 \mid a_2$ folgt $b_1 \cdot b_2 \mid a_1 \cdot a_2$.

(3) Aus $c \cdot b \mid c \cdot a$ (für $c \neq 0$) folgt $b \mid a$.

(4) Aus $b \mid a_1$ und $b \mid a_2$ folgt $b \mid c_1 \cdot a_1 + c_2 \cdot a_2$ für beliebige ganze Zahlen c_1 und c_2.

Von der Richtigkeit der Aussagen (1) - (4) kann man sich leicht überzeugen; (1) sieht man beispielsweise so ein: $c \mid b$ bedeutet, dass $b = c \cdot d$ für ein $d \in \mathbb{Z}$ gilt; $b \mid a$ bedeutet, dass $a = b \cdot e$ für ein $e \in \mathbb{Z}$ gilt. Durch Einsetzen erhält man $a = c \cdot d \cdot e$; also gilt $c \mid a$.

Teiler jeder ganzen Zahl a sind 1 und -1 sowie a und $-a$. Dies sind die sogenannten *trivialen Teiler* von a.

Definition 2.
Eine natürliche Zahl $n \geq 2$ heißt *Primzahl*, wenn n nur die trivialen Teiler besitzt, d.h., n ist nur durch 1, -1, n und $-n$ teilbar.

Die ersten zwölf Primzahlen sind 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 und 37.

Ist $n \geq 2$ eine natürliche Zahl und ist p eine Primzahl, für die $p \mid n$ gilt, so nennt man p einen *Primteiler* von n. Jede natürliche Zahl $n \geq 2$ besitzt mindestens einen Primteiler, da die kleinste natürliche Zahl $p \geq 2$, die n teilt, ein Primteiler ist.

Satz 1 (Satz von Euklid).
Es gibt unendlich viele Primzahlen.

Beweis. Wir nehmen an, dass es nur endlich viele Primzahlen p_1, p_2, …, p_n gibt und führen diese Annahme zum Widerspruch. Es sei $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Die Zahl $a + 1$ hat (wie jede natürliche Zahl ≥ 2) einen Primteiler p. Da p_1, p_2, …, p_n nach unserer Annahme die einzigen Primzahlen sind, muss $p = p_i$ für ein i gelten, d.h., $p_i \mid (a + 1)$. Wegen $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ gilt $p_i | a$. Wir haben also erhalten, dass p_i sowohl $a + 1$ als auch a teilt. Nach (4) teilt p_i dann auch $(a + 1) - a$, d.h., p_i teilt 1, was wegen

$p_i \geq 2$ unmöglich ist. Damit haben wir aus unserer Annahme, es gebe nur endlich viele Primzahlen, einen Widerspruch hergeleitet. Es folgt Satz 1. □

Ohne Beweis geben wir den folgenden grundlegenden Satz an (Existenz und Eindeutigkeit der Primfaktorzerlegung).

Satz 2.

Jede natürliche Zahl $n \geq 2$ ist als Produkt von Primzahlen darstellbar:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_m \quad (m \geq 1). \tag{2.5}$$

Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig. Ist n eine Primzahl, so besteht das „Produkt“ lediglich aus einem Faktor.

In der obigen Darstellung sind die Primfaktoren p_1, p_2, …, p_m im Allgemeinen nicht alle verschieden.

Beispiele:

1. $6600 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11$

2. $126 = 2 \cdot 3 \cdot 3 \cdot 7$

Um eine übersichtlichere Darstellung zu bekommen, fasst man daher meistens gleiche Faktoren zusammen:

1. $6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11$

2. $126 = 2 \cdot 3^2 \cdot 7$

Überträgt man dies auf den allgemeinen Fall der Primfaktordarstellung (2.5), so kann man n auch wie folgt darstellen.

Satz 2'.

Jede natürliche Zahl $n \geq 2$ ist als Produkt wie folgt darstellbar:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m} \quad (m \geq 1 \text{ und } \alpha_1, \ldots, \alpha_m \in \mathbb{N}). \tag{2.6}$$

Die p_i sind dabei *paarweise verschiedene* Primzahlen. Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.

Eine wichtige Eigenschaft von Primzahlen, die man als Folgerung aus Satz 2 erhalten kann, ist die folgende: Für jede Primzahl p gilt:

$$p \mid ab \wedge p \nmid a \Rightarrow p \mid b\ . \tag{$\star$}$$

Man mache sich klar, dass die Aussage ($\star$) im Allgemeinen nicht richtig ist, wenn p keine Primzahl ist (Beispiel: $p = 6$, $a = 4$ und $b = 3$). Aus Satz 2 kann man auch die folgende Aussage ($\star\star$) erhalten, die etwas allgemeiner als ($\star$) ist: Für jede Primzahl p und $\alpha \in \mathbb{N}$ gilt:

$$p^\alpha \mid ab \wedge p \nmid a \Rightarrow p^\alpha \mid b\ . \tag{$\star\star$}$$

Größter gemeinsamer Teiler (ggT) und kleinstes gemeinsames Vielfaches (kgV)

Gilt $c \mid a$ und $c \mid b$, so nennt man c einen *gemeinsamen Teiler* von a und b. Als eine Folgerung aus Satz 2 lässt sich Folgendes zeigen: Zu je zwei ganzen Zahlen a und b, die nicht beide gleich Null sind, gibt es immer einen gemeinsamen Teiler $t \in \mathbb{N}$, so dass für jeden gemeinsamen Teiler d von a und b gilt: $d \mid t$. Man nennt t den *größten gemeinsamen Teiler* von a und b (Zeichen: $\mathrm{ggT}\,(a, b)$).

Ist für a und b ($b \geq 2$) die Primfaktorzerlegung von a und b gegeben, so kann man $\mathrm{ggT}\,(a, b)$ leicht bestimmen.

Beispiel.

$$\begin{aligned} a &= 2^4 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13^4 \\ b &= 2^2 \cdot 5 \cdot 7^2 \cdot 13^3 \cdot 17 \cdot 23 \\ \mathrm{ggT}\,(a,b) &= 2^2 \cdot 5 \cdot 7 \cdot 13^3 \end{aligned}$$

Gilt $a \mid c$ und $b \mid c$, so nennt man c ein *gemeinsames Vielfaches* von a und b. Ebenfalls als Folgerung aus Satz 2 erhält man: Zu je zwei ganzen Zahlen a und b gibt es immer ein gemeinsames Vielfaches $v \in \mathbb{N}$, so dass für jedes andere gemeinsame Vielfache w von a und b gilt: $v \mid w$. Man nennt v das *kleinste gemeinsame Vielfache* von a und b (Zeichen: $\mathrm{kgV}\,(a,b)$).

Beispiel.

$$\begin{aligned} a &= 2^4 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13^4 \\ b &= 2^2 \cdot 5 \cdot 7^2 \cdot 13^3 \cdot 17 \cdot 23 \\ \mathrm{kgV}\,(a,b) &= 2^4 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 13^4 \cdot 17 \cdot 23 \end{aligned}$$

Für $a, b \in \mathbb{N}$ gilt allgemein:

$$\mathrm{ggT}\,(a,b) \cdot \mathrm{kgV}\,(a,b) = a \cdot b. \tag{2.7}$$

Sind a und b gegeben (etwa $a = 816$ und $b = 294$), so genügt es, $\mathrm{ggT}\,(a,b)$ zu berechnen; $\mathrm{kgV}\,(a,b)$ kann dann mittels (2.7) bestimmt werden.

Wir kommen nun zum *Euklidischen Algorithmus*, mit dem man für $m, n \in \mathbb{N}$ den größten gemeinsamen Teiler von m und n berechnet. Hierzu benötigen wir die folgende Feststellung über die *Division mit Rest*.

$$\begin{gathered} \text{Zu } m \in \mathbb{Z} \text{ und } n \in \mathbb{N} \text{ gibt es immer eindeutig bestimmte ganze Zahlen} \\ q \text{ und } r \text{ mit } 0 \le r < n, \text{ so dass } m = q \cdot n + r \text{ gilt.} \\ \text{Man nennt in dieser Darstellung } q \text{ den } \textit{Quotienten} \text{ und } r \text{ den } \textit{Rest}. \end{gathered} \tag{2.8}$$

Beispiele zur Division mit Rest[5]:

1. $m = 27$, $n = 12$; dann gilt $27 = 2 \cdot 12 + 3$; es folgt $q = 2$ und $r = 3$.

2. $m = -10$, $n = 3$; dann gilt $-10 = (-4) \cdot 3 + 2$; es folgt $q = -4$ und $r = 2$.

Dem Euklidischen Algorithmus liegt die folgende einfache Beobachtung zugrunde:

$$\text{Gilt } m = q \cdot n + r \quad (0 \le r < n), \text{ so folgt } \quad \mathrm{ggT}\,(m,n) = \mathrm{ggT}\,(n,r). \tag{2.9}$$

Beweis von (2.9). Es gelte $m = q \cdot n + r$. Ist t ein gemeinsamer Teiler von n und r, so ist t auch ein gemeinsamer Teiler von m und n (vgl. (2.4)). Ist umgekehrt t ein gemeinsamer Teiler von m und n, so ist t auch ein gemeinsamer Teiler von n und r (aufgrund von (2.4) und wegen $r = m - q \cdot n$). Die Menge der gemeinsamen Teiler von n und r ist also gleich der Menge der gemeinsamen Teiler von m und n; insbesondere gilt also $\mathrm{ggT}\,(n,r) = \mathrm{ggT}\,(m,n)$. □

Euklidischer Algorithmus

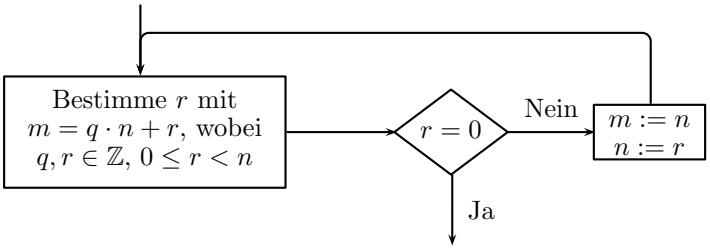
Der Algorithmus liefert zu gegebenen $m, n \in \mathbb{N}$ (mit $m > n$), den größten gemeinsamen Teiler.

1. Man teilt m durch n und bestimmt den Rest r derart, dass $m = q \cdot n + r$ gilt (mit $q, r \in \mathbb{Z}$ und $0 \le r < n$).

2. Falls $r = 0$ gilt, ist man fertig, und das Ergebnis ist der Wert von n.

3. Andernfalls setzt man $m := n$ und $n := r$ und geht zurück zu 1.

[5] Man spricht auch von „Zerlegung mit kleinstem nicht negativen Rest“ oder einfach von „Zerlegung mit Rest“.



Beispiel. Es seien $m = 816$ und $n = 294$.

$$\begin{aligned} 816 &= 2 \cdot 294 + 228 \\ 294 &= 1 \cdot 228 + 66 \\ 228 &= 3 \cdot 66 + 30 \\ 66 &= 2 \cdot 30 + 6 \\ 30 &= 5 \cdot 6 + 0 \qquad \Rightarrow \operatorname{ggT}(816, 294) = 6 \end{aligned}$$

Der Algorithmus endet nach endlich vielen Schritten, da bei jeder Ausführung der Anweisung $n := r$ der Wert von n verkleinert wird.

Dass der Euklidische Algorithmus tatsächlich $\operatorname{ggT}(m, n)$ berechnet, lässt sich wie folgt einsehen: Ist $r > 0$, so wird in 3. die Anweisung $m := n$, $n := r$ ausgeführt und anschließend nach 1. gegangen. Dies bedeutet, dass man die Aufgabe, den $\operatorname{ggT}(m, n)$ zu berechnen, durch die Aufgabe, den $\operatorname{ggT}(n, r)$ zu berechnen, ersetzt hat; wegen (2.9) gilt aber $\operatorname{ggT}(m, n) = \operatorname{ggT}(n, r)$. Ist $r = 0$, so gilt $m = q \cdot n$, d.h., n ist ein Teiler von m; also ist in diesem Fall n der größte gemeinsame Teiler von m und n.

Im Folgenden werden wir den Begriff der *Kongruenz* ganzer Zahlen betrachten.

Definition.
Es sei $m \in \mathbb{N}$. Zwei ganze Zahlen a und b heißen *kongruent modulo* m, wenn $a - b$ durch m teilbar ist. Man sagt auch: „a ist kongruent zu b modulo m“ und schreibt $a \equiv b \pmod{m}$.

Beispiele:

1. $27 \equiv 12 \pmod{5}$, da $27 - 12 = 15$ und $5 \mid 15$.

2. $-7 \equiv 2 \pmod{3}$, da $-7 - 2 = -9$ und $3 \mid -9$.

3. $8227 \not\equiv 11 \pmod{3}$, da $8227 - 11 = 8216$ und $3 \nmid 8216$.

Es sei $m \in \mathbb{N}$. Für die ganzen Zahlen a und b seien $a = q_1 \cdot m + r_1$
und $b = q_2 \cdot m + r_2$ die Zerlegungen mit Rest (d.h., $0 \leq r_1 < m$ und $0 \leq r_2 < m$). (2.10)
Behauptung: $a \equiv b \pmod{m}$ gilt genau dann, wenn $r_1 = r_2$ gilt.

Bevor wir dies beweisen, wollen wir uns den Inhalt von (2.10) an einem Beispiel verdeutlichen: Es sei $m = 3$. Wir teilen die ganzen Zahlen $\mathbb{Z}$ in drei Klassen $\mathcal{K}_0$, $\mathcal{K}_1$ und $\mathcal{K}_2$ ein:

$$\begin{aligned} \mathcal{K}_0 &= \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}, \\ \mathcal{K}_1 &= \{\ldots, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}, \\ \mathcal{K}_2 &= \{\ldots, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}. \end{aligned}$$

In $\mathcal{K}_0$ sind also diejenigen ganzen Zahlen, die durch 3 teilbar sind, in $\mathcal{K}_1$ sind diejenigen, die beim Teilen durch 3 den Rest 1 ergeben, und in $\mathcal{K}_2$ sind diejenigen, die den Rest 2 ergeben. Die Behauptung von (2.10) besagt für dieses Beispiel, dass $a \equiv b \pmod{3}$ genau dann gilt, wenn a und b in derselben Klasse $\mathcal{K}_i$ $(i = 0, 1, 2)$ liegen.

Beweis von (2.10). Es wird behauptet: $a \equiv b \pmod{m} \Leftrightarrow r_1 = r_2$. Um eine solche *Äquivalenz* zu beweisen, hat man zwei Dinge zu zeigen:

(1) $a \equiv b \pmod{m} \Rightarrow r_1 = r_2$

Es gelte $a \equiv b \pmod{m}$, d.h., $m \mid (a-b)$. Es gibt also ein $c \in \mathbb{Z}$, so dass $a - b = c \cdot m$ gilt.

Aus $a = q_1 \cdot m + r_1$ und $b = q_2 \cdot m + r_2$ folgt

$$a - b = c \cdot m = (q_1 - q_2) \cdot m + (r_1 - r_2).$$

Durch Umstellen ergibt sich:

$$r_1 - r_2 = (c - q_1 + q_2) \cdot m.$$

Also ist $r_1 - r_2$ ein Vielfaches von m. Aus $0 \leq r_1 < m$ und $0 \leq r_2 < m$ folgt

$$-m < r_1 - r_2 < m.$$

Das einzige Vielfache von m, das größer als $-m$ und kleiner als m ist, ist 0. Also gilt $r_1 - r_2 = 0$, woraus $r_1 = r_2$ folgt.

(2) $a \equiv b \pmod{m} \Leftarrow r_1 = r_2$

Es gelte $r_1 = r_2$. Aus $a = q_1 \cdot m + r_1$ und $b = q_2 \cdot m + r_2$ folgt demnach:

$$\begin{aligned} a - b &= (q_1 - q_2) \cdot m + (r_1 - r_2) \\ &= (q_1 - q_2) \cdot m. \end{aligned}$$

Also gilt $m \mid (a-b)$, d.h., $a \equiv b \pmod{m}$. □

Regeln für das Rechnen mit Kongruenzen.

1. $a \equiv a \pmod{m}$ für alle $a \in \mathbb{Z}$

2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

3. $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

4. $a_1 \equiv b_1 \pmod{m} \wedge a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$

$a_1 \equiv b_1 \pmod{m} \wedge a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$

5. $a_1 \equiv b_1 \pmod{m} \wedge a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$

6. Gilt $\mathrm{ggT}(k, m) = 1$, so folgt aus $k \cdot a \equiv k \cdot b \pmod{m}$, dass $a \equiv b \pmod{m}$ ist.

Man erhält diese Regeln durch direktes Zurückführen auf die Definition von $a \equiv b \pmod{m}$ oder durch Verwenden der gleichwertigen Bedingung $r_1 = r_2$ aus (2.10). Empfehlung: Man beweise zum Einüben des Umgangs mit Kongruenzen die Regeln 1 bis 6.

Wir geben ein Beispiel dafür, dass man in Regel 6 für das Rechnen mit Kongruenzen die Voraussetzung $\mathrm{ggT}(k, m) = 1$ nicht einfach weglassen darf: Es sei $k = 8$ und $m = 6$; dann gilt $8 \cdot 3 \equiv 8 \cdot 6 \pmod{6}$, allerdings gilt $3 \not\equiv 6 \pmod{6}$.

Eine häufig verwendete Schreibweise: Ist r eine reelle Zahl, so bezeichnet $\lceil r \rceil$ die kleinste ganze Zahl a, für die $a \geq r$ gilt. Ähnlich wird $\lfloor r \rfloor$ als die größte ganze Zahl b definiert mit $b \leq r$. Es gilt $\lfloor r \rfloor \leq r \leq \lceil r \rceil$.

Man nennt $\lfloor\ \rfloor$ *untere* und $\lceil\ \rceil$ *obere Gaußklammer*.

Beispiele:

$$\begin{aligned} \lceil 3.14 \rceil &= 4 & \lfloor 3.14 \rfloor &= 3 \\ \lceil \sqrt{2} \rceil &= 2 & \lfloor \sqrt{2} \rfloor &= 1 \\ \lceil 5 \rceil &= 5 & \lfloor 5 \rfloor &= 5 \\ \lceil -1.2 \rceil &= -1 & \lfloor -1.2 \rfloor &= -2 \end{aligned}$$

2.5 Rechnen mit dem Summenzeichen

In diesem Abschnitt sind mit a_i ($i \in \mathbb{Z}$) immer reelle Zahlen bezeichnet. Wir erklären die Bedeutung des Summenzeichens $\sum$ zunächst an **Beispielen**:

1. Für $n \in \mathbb{N}$ ist $\sum\limits_{i=1}^{n} a_i$ ein anderer Ausdruck für $a_1 + a_2 + \ldots + a_n$.

Statt $\sum\limits_{i=1}^{n} a_i$ kann man auch $\sum\limits_{1 \le i \le n} a_i$ schreiben. Es gilt also beispielsweise:

$$\sum_{i=1}^{5} a_i = \sum_{1 \le i \le 5} a_i = a_1 + a_2 + a_3 + a_4 + a_5 \ .$$

2. Eine Variante dieser Schreibweise:

$$\sum_{5 \le i \le 8} a_i = a_5 + a_6 + a_7 + a_8 \ .$$

3. Weitere Beispiele:

$$\begin{aligned}
\sum_{0 \le k \le 3} a_k &= a_0 + a_1 + a_2 + a_3 \\
\sum_{-1 \le s \le 3} b_s &= b_{-1} + b_0 + b_1 + b_2 + b_3 \\
\sum_{\substack{1 \le j \le 10 \\ j \text{ gerade}}} a_j &= a_2 + a_4 + a_6 + a_8 + a_{10} \\
\sum_{\substack{0 \le j \le 10 \\ j \text{ ungerade}}} 2^j &= 2^1 + 2^3 + 2^5 + 2^7 + 2^9 \\
\sum_{\substack{1 \le j \le 12 \\ j \text{ Primzahl}}} s_j &= s_2 + s_3 + s_5 + s_7 + s_{11} \\
\sum_{\substack{1 \le k \le 50 \\ k \text{ Quadratzahl}}} a_k &= a_1 + a_4 + a_9 + a_{16} + a_{25} + a_{36} + a_{49}
\end{aligned}$$

In allen diesen Beispielen ist die *Indexvariable*[6] i (bzw. j, k oder s) eine ganze Zahl. Unter dem Summenzeichen steht eine Bedingung $B(i)$, die von endlich vielen ganzen Zahlen i erfüllt wird. Summiert wird über diejenigen i, die die Bedingung $B(i)$ erfüllen. (Entsprechendes gilt natürlich auch, wenn die Indexvariable mit j, k, ... bezeichnet ist; die Bedingung wird dann mit $B(j)$, $B(k)$, ... bezeichnet.) Dies führt zur folgenden allgemeinen Schreibweise:

$\sum\limits_{B(i)} a_i$ bezeichnet die Summe aller a_i, die die Bedingung $B(i)$ erfüllen.

Dabei wird vorausgesetzt, dass dies nur für endlich viele i der Fall ist. Erfüllt kein $i \in \mathbb{Z}$ die Bedingung $B(i)$, so ist die Summe gleich 0.

Beispiele:

1. $\sum\limits_{\substack{50 \le i \le 60 \\ i \text{ Quadratzahl}}} a_i = 0$

2. $\sum\limits_{1 \le i \le n} a_i = 0$ für $n = 0$

Im Folgenden werden vier Operationen mit dem Summenzeichen besprochen.

[6] Statt Indexvariable sagt man auch *Summationsindex*.

2.5.1 Das allgemeine Distributivgesetz

$$\left(\sum_{B(i)} a_i\right)\left(\sum_{C(j)} b_j\right) = \sum_{B(i)}\left(\sum_{C(j)} a_i b_j\right) \tag{2.11}$$

Bemerkung: Die Klammern auf der rechten Seite von (2.11) wurden nur der Deutlichkeit halber gesetzt. Es ist möglich (und üblich), diese Klammer wegzulassen.

Beispiel.

$$\begin{aligned}\left(\sum_{i=1}^{2} a_i\right)\left(\sum_{j=1}^{3} b_j\right) &= \big(a_1+a_2\big)\big(b_1+b_2+b_3\big)\\ &= \big(a_1b_1+a_1b_2+a_1b_3\big)+\big(a_2b_1+a_2b_2+a_2b_3\big)\\ &= \sum_{i=1}^{2}\sum_{j=1}^{3} a_i b_j\end{aligned}$$

2.5.2 Indextransformation

Zunächst schauen wir uns typische Beispiele an. Es gilt offenbar (für $n \in \mathbb{N}$):

$$\begin{aligned}\sum_{i=1}^{n} a_i &= \sum_{i=0}^{n-1} a_{i+1}\\ \sum_{i=1}^{n} a_i &= \sum_{i=2}^{n+1} a_{i-1}\end{aligned}$$

Oder etwas allgemeiner (für $m, n \in \mathbb{Z}$ und $m \le n$):

$$\begin{aligned}\sum_{i=m}^{n} a_i &= \sum_{i=m-1}^{n-1} a_{i+1}\\ \sum_{i=m}^{n} a_i &= \sum_{i=m+1}^{n+1} a_{i-1}\end{aligned}$$

Oder noch etwas allgemeiner (für $m, n \in \mathbb{Z}$, $m \le n$ und $h \in \mathbb{N}$):

$$\sum_{i=m}^{n} a_i = \sum_{i=m-h}^{n-h} a_{i+h} \tag{2.12}$$

$$\sum_{i=m}^{n} a_i = \sum_{i=m+h}^{n+h} a_{i-h} \tag{2.13}$$

Bezeichnen wir in der Summe $\sum_{i=m}^{n} a_i$ die Zahlen m und n als Summationsgrenzen, so können wir die Formeln (2.12) und (2.13) so beschreiben: *Erhöht man den Summationsindex um h, so muss man gleichzeitig die Summationsgrenzen um h erniedrigen; und umgekehrt.*

Ein weiteres typisches Beispiel einer Indextransformation (für $n \in \mathbb{N}$):

$$\sum_{i=0}^{n} a_i = \sum_{i=0}^{n} a_{n-i}$$

Oder etwas allgemeiner (für $m, n \in \mathbb{Z}$ und $m \leq n$):

$$\sum_{i=m}^{n} a_i = \sum_{i=0}^{n-m} a_{n-i} \tag{2.14}$$

Nachdem wir typische Beispiele gesehen haben, wollen wir nun den allgemeinen Fall behandeln. Unter einer *Indextransformation* verstehen wir eine injektive Abbildung

$$\begin{array}{rcl} \tau : \mathbb{Z} & \to & \mathbb{Z} \\ i & \mapsto & \tau(i) \end{array}$$

Die oben in (2.12), (2.13) und (2.14) betrachteten Indextransformationen waren die Abbildungen $\tau : \mathbb{Z} \to \mathbb{Z}$ mit $\tau(i) = i + h$ bzw. $\tau(i) = i - h$ bzw. $\tau(i) = n - i$ (für festes h bzw. n).

Sei nun $\tau : \mathbb{Z} \to \mathbb{Z}$ eine beliebige Indextransformation. Wir betrachten die Summe

$$\sum_{B(i)} a_i$$

und bezeichnen mit S die Menge derjenigen $i \in \mathbb{Z}$, die $B(i)$ erfüllen; wir setzen $T = \big\{i \in \mathbb{Z} : \tau(i) \in S\big\}$. Dann gilt

$$\sum_{B(i)} a_i = \sum_{i \in S} a_i = \sum_{i \in T} a_{\tau(i)}.$$

Ist nun $C(i)$ entweder die Bedingung „$i \in T$“ selbst oder eine zu „$i \in T$“ gleichwertige Bedingung (d.h., $C(i)$ gilt genau dann, wenn $i \in T$ gilt), so erhalten wir

$$\sum_{i \in T} a_{\tau(i)} = \sum_{C(i)} a_{\tau(i)}.$$

Mit dieser Bedeutung von $C(i)$ ergibt sich die folgende Formel für eine beliebige Indextransformation τ:

$$\sum_{B(i)} a_i = \sum_{C(i)} a_{\tau(i)}. \tag{2.15}$$

2.5.3 Änderung der Summationsreihenfolge

Wir betrachten jetzt Summanden der Form a_{ij}, d.h. Summanden, die mit zwei Indexvariablen i und j versehen sind. Die Idee, die der Regel über die Änderung der Summationsreihenfolge zugrunde liegt, ist sehr einfach: Addiert man die Zahlen in einer Matrix „zeilenweise“, so erhält man selbstverständlich dasselbe Ergebnis wie bei „spaltenweiser“ Addition.

Beispiel. Wir betrachten die folgende Matrix:

$$\begin{pmatrix} 1 & 3 & 7 & 11 \\ 4 & -6 & 9 & 8 \\ 3 & 3 & 1 & 2 \end{pmatrix}$$

Zeilenweise Addition: $(1 + 3 + 7 + 11) + (4 - 6 + 9 + 8) + (3 + 3 + 1 + 2) = 46$

Spaltenweise Addition: $(1 + 4 + 3) + (3 - 6 + 3) + (7 + 9 + 1) + (11 + 8 + 2) = 46$

Die Regel über die Änderung der Summationsreihenfolge lautet

$$\sum_{B(i)} \sum_{C(j)} a_{ij} = \sum_{C(j)} \sum_{B(i)} a_{ij}. \tag{2.16}$$

Ein Spezialfall: Wir betrachten die folgenden beiden Summen:

$$\begin{aligned}\sum_{B(i)}\sum_{j=1}^{2} a_{ij} &= \sum_{B(i)} (a_{i1}+a_{i2})\\ \sum_{j=1}^{2}\sum_{B(i)} a_{ij} &= \sum_{B(i)} a_{i1} + \sum_{B(i)} a_{i2}.\end{aligned}$$

Nach (2.16) sind diese beiden Summen gleich. Schreibt man b_i für a_{i1} und c_i für a_{i2}, so ergibt sich als Spezialfall von (2.16):

$$\sum_{B(i)} (b_i + c_i) = \sum_{B(i)} b_i + \sum_{B(i)} c_i. \tag{2.16.1}$$

Oftmals reicht die Regel (2.16) nicht aus; es tritt nämlich häufig der Fall auf, dass die Bedingung $C(j)$, die unter dem inneren Summenzeichen steht, von i abhängt. Mit anderen Worten: Für jedes i, das $B(i)$ erfüllt, tritt in der Summe eine Bedingung $C_i(j)$ auf, die von i abhängt. Eine solche Summe hat dann die Form

$$\sum_{B(i)}\sum_{C_i(j)} a_{ij}.$$

Beispiel.

$$\begin{aligned}\sum_{i=1}^{3}\sum_{j=1}^{i} a_{ij} &= \sum_{j=1}^{1} a_{1j} + \sum_{j=1}^{2} a_{2j} + \sum_{j=1}^{3} a_{3j}\\ &= a_{11} + \big(a_{21}+a_{22}\big) + \big(a_{31}+a_{32}+a_{33}\big)\end{aligned}$$

Hier gibt es zu jedem i eine eigene Bedingung $C_i(j)$, nämlich die Bedingung $1 \le j \le i$.

Im Falle einer Summe $\sum\limits_{B(i)}\sum\limits_{C_i(j)} a_{ij}$ kann man (ähnlich wie in (2.16)) eine Umformung vornehmen, wenn man sich die Zahlen a_{ij} in einer Matrix angeordnet vorstellt. Der Unterschied zu (2.16) besteht allerdings darin, dass wir es hier sozusagen mit einer „unvollständigen“ Matrix zu tun haben, d.h., nicht an jeder Stelle der Matrix befindet sich ein Eintrag. Wir wollen nicht die allgemeine Formel hierfür behandeln, sondern dies an einem typischen Beispiel erklären.

Beispiel. Die Matrix, die zur Summe $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{i} a_{ij}$ gehört, hat die folgende „Dreiecksgestalt“:

$$\begin{pmatrix} a_{11} & \star & \star & \dots & \star\\ a_{21} & a_{22} & \star & \dots & \star\\ a_{31} & a_{32} & a_{33} & \dots & \star\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn}\end{pmatrix} \qquad (\star \text{ bedeutet, es besteht kein Eintrag}).$$

Summiert man erst „zeilenweise“ und dann „spaltenweise“, so erhält man:

$$\sum_{i=1}^{n}\sum_{j=1}^{i} a_{ij} = \sum_{j=1}^{n}\sum_{i=j}^{n} a_{ij}. \tag{2.16.2}$$

Wir kommen nun zur vierten Operation mit dem Summenzeichen.

2.5.4 Vereinigungs- und Aufspaltungsregel

$$\sum_{B(i)} a_i + \sum_{C(i)} a_i = \sum_{B(i)\vee C(i)} a_i + \sum_{B(i)\wedge C(i)} a_i \tag{2.17}$$

Typisches **Beispiel**:

$$\sum_{i=1}^{m} a_i + \sum_{i=m}^{n} a_i = \left(\sum_{i=1}^{n} a_i\right) + a_m.$$

Wir werden im Folgenden die Verwendung der obigen Umformungsoperationen an einem Beispiel vorführen; und zwar wollen wir die oft gebrauchte *geometrische Summenformel* herleiten.

Herleitung der geometrischen Summenformel

Es sei $q \in \mathbb{R}$ $(q \neq 1)$ und $n \in \mathbb{N} \cup \{0\}$. Wir betrachten die Summe

$$\sum_{i=0}^{n} q^i = 1 + q + q^2 + q^3 + \ldots + q^n.$$

Unser Ziel ist es, für diese Summe einen einfachen, kurzen Ausdruck zu gewinnen, in dem insbesondere das Summenzeichen nicht mehr vorkommt. Hierzu formen wir die Summe mit Hilfe unserer Umformungsoperationen um:

$$\begin{aligned}
\sum_{i=0}^{n} q^i &\overset{(2.17)}{=} 1 + \sum_{i=1}^{n} q^i \\
&\overset{(2.11)}{=} 1 + q \sum_{i=1}^{n} q^{i-1} \\
&\overset{(2.12)}{=} 1 + q \sum_{i=0}^{n-1} q^i \\
&= 1 + q \sum_{i=0}^{n-1} q^i + q^{n+1} - q^{n+1} \\
&= 1 + q \left(\sum_{i=0}^{n-1} q^i + q^n\right) - q^{n+1} \\
&\overset{(2.17)}{=} 1 + q \sum_{i=0}^{n} q^i - q^{n+1}
\end{aligned}$$

Vergleicht man die linke Seite mit der rechten, so erhält man durch Umstellung der Gleichung

$$(1-q) \sum_{i=0}^{n} q^i = 1 - q^{n+1}.$$

Hieraus folgt, wenn wir durch $(1-q)$ teilen (das ist wegen $q \neq 1$ möglich):

Geometrische Summenformel

$$\sum_{i=0}^{n} q^i = \frac{1 - q^{n+1}}{1 - q}$$

Dadurch, dass wir die Summe $\sum_{i=0}^{n} q^i$ mit Hilfe der Operationen (2.11), (2.12) und (2.17) umgeformt haben, haben wir also einen einfachen Ausdruck für diese Summe gewonnen.

Hat man einmal eine gesuchte Formel gefunden, so ist es häufig sehr einfach, diese Formel im Nachhinein durch vollständige Induktion zu bestätigen.

Um dies zu verdeutlichen, führen wir noch einen zweiten Beweis der geometrischen Summenformel vor, bei dem wir vollständige Induktion verwenden:

Beweis der geometrischen Summenformel durch vollständige Induktion

(I) *Induktionsanfang*

Für $n = 0$ ist die geometrische Summenformel richtig, denn für $n = 0$ gilt:

$$\sum_{i=0}^{0} q^i = q^0 = 1 \quad \text{und} \quad \frac{1 - q^{0+1}}{1 - q} = \frac{1 - q}{1 - q} = 1.$$

(II) *Induktionsschritt*

Für ein festes $n \geq 0$ gelte die geometrische Summenformel (Induktionsannahme). Dann gilt sie auch für $n + 1$:

$$\begin{aligned} \sum_{i=0}^{n+1} q^i &= \sum_{i=0}^{n} q^i + q^{n+1} \\ &\overset{(\star)}{=} \frac{1 - q^{n+1}}{1 - q} + q^{n+1} \\ &= \frac{1 - q^{n+1}}{1 - q} + \frac{q^{n+1}(1 - q)}{1 - q} \\ &= \frac{1 - q^{n+2}}{1 - q} \end{aligned}$$

An der mit $(\star)$ bezeichneten Stelle wurde die Induktionsannahme benutzt. □

Man erkennt an diesem Beispiel im Übrigen recht gut, was die Methode der vollständigen Induktion leistet und was sie nicht leistet: Vollständige Induktion ist ein Mittel, um die Richtigkeit eines Ergebnisses (oder einer Vermutung) zu *beweisen*; geht es aber darum, ein Ergebnis oder eine Vermutung zu *finden*, so hilft die Methode der vollständigen Induktion nicht weiter.

Abschließend erwähnen wir noch das *Produktzeichen*, das (für $n \in \mathbb{N}$) folgendermaßen definiert wird:

$$\prod_{i=1}^{n} a_i := a_1 \cdot a_2 \cdot \ldots \cdot a_n$$

2.6 Elementare Kombinatorik

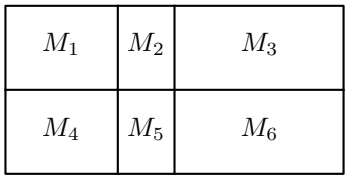
Ist M eine endliche Menge, so bezeichnet man die Anzahl der Elemente von M mit $|M|$. Wir beginnen mit drei ebenso einleuchtenden wie nützlichen Regeln: der Additionsregel, der Multiplikationsregel und der Gleichheitsregel.

Additionsregel.

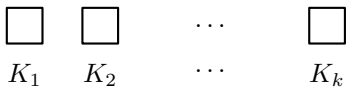
Es sei M eine endliche Menge, die in k paarweise disjunkte Teilmengen M_1, ..., M_k ($k \in \mathbb{N}$) eingeteilt sei, d.h., $M = M_1 \cup \ldots \cup M_k$, $M_i \cap M_j = \emptyset$ für alle $i \neq j$ (siehe Zeichnung). Dann gilt:

$$|M| = \sum_{i=1}^{k} |M_i|.$$

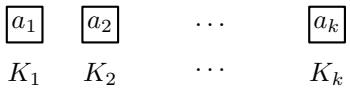
Zur Illustration der Additionsregel: Die Menge M ist in der folgenden Zeichnung in sechs paarweise disjunkte Teilmengen M_1, ..., M_6 eingeteilt.



Um die Multiplikationsregel formulieren zu können, betrachten wir k Kästchen K_1, ..., K_k ($k \in \mathbb{N}$):



Legen wir in K_1 ein Objekt a_1, dann in K_2 ein Objekt a_2 usw., so erhalten wir eine *Belegung* der Kästchen:



Multiplikationsregel.

Gegeben seien (wie oben) k Kästchen K_1, ..., K_k, die nacheinander belegt werden sollen: Erst K_1, dann K_2 usw. Wir nehmen an, dass man n_1 Möglichkeiten hat, das Kästchen K_1 zu belegen; nach vorgenommener Belegung von K_1 hat man n_2 Möglichkeiten, K_2 zu belegen; nachdem K_1 und K_2 belegt wurden, hat man n_3 Möglichkeiten, K_3 zu belegen usw. Dann ist die Anzahl der möglichen Belegungen der Kästchen gleich:

$$n_1 \cdot n_2 \cdot \ldots \cdot n_k.$$

Die Multiplikationsregel ist gültig für alle ganzen Zahlen $n_i \geq 0$; bewiesen werden kann sie mit vollständiger Induktion.

Gleichheitsregel.

A und B seien endliche Mengen. Wir möchten die Anzahl der Elemente von A bestimmen und nehmen an, dass wir für die Menge B die Anzahl ihrer Elemente bereits kennen, etwa $|B| = m$. Gelingt es uns nachzuweisen, dass es eine bijektive Abbildung $f : A \to B$ gibt, so gilt $|A| = |B| = m$, d.h., wir haben die Anzahl der Elemente von A bestimmt.

Beispiele:

1. Eine Kennziffer bestehe aus drei Buchstaben und vier darauffolgenden Ziffern (z.B.: $FAB3447$ oder $ARR5510$).

(a) Wie viele derartige Kennziffern gibt es?

Nach der Multiplikationsregel ergibt sich:

$$26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 26^3 \cdot 10^4 = 175760000.$$

(b) Wie viele Kennziffern gibt es, bei denen kein Zeichen doppelt vorkommt?

Nach der Multiplikationsregel ergibt sich:

$$26 \cdot 25 \cdot 24 \cdot 10 \cdot 9 \cdot 8 \cdot 7 = 78624000.$$

2. Gegeben seien 15 unterschiedliche Bücher, von denen 8 in englischer Sprache, 3 in deutscher und 4 in russischer Sprache sind. Auf wie viele Arten kann man zwei Bücher in unterschiedlichen Sprachen wählen?

Nach der Additions- und Multiplikationsregel ergibt sich:

$$8 \cdot 3 + 8 \cdot 4 + 3 \cdot 4 = 68.$$

Im Folgenden werden wir fünf Fragestellungen behandeln, die wir als „Grundaufgaben“ bezeichnen wollen, da es sich bei ihnen um grundlegende kombinatorische Aufgaben handelt, denen man, oft in versteckter Form, innerhalb und außerhalb der Mathematik immer wieder begegnet.

Zunächst nehmen wir jedoch eine Ergänzung zum Begriff „k-Tupel“ vor. Für $k \geq 1$ hatten wir bereits früher definiert, was ein k-Tupel ist; dabei hatten wir mit M^k die Menge der k-Tupel von Elementen aus M bezeichnet. Nun beziehen wir zusätzlich den Fall $k = 0$ mit ein, indem wir die folgende Definition vornehmen.

Definition.

Unter einem 0-*Tupel* von Elementen einer Menge M wollen wir nichts anderes als die leere Menge $\emptyset$ verstehen. Zu jeder Menge M gibt es also genau ein 0-Tupel von Elementen von M, nämlich $\emptyset$. Mit M^0 bezeichnet man die Menge der 0-Tupel von Elementen von M; es gilt also:

$$M^0 = \Big\{\emptyset\Big\}.$$

Grundaufgabe 1

Frage: Es sei $k \geq 0$ sowie $n \geq 0$. Wie viele k-Tupel kann man aus einer n-elementigen Menge M bilden?

Antwort: n^k

Begründung: Für $k \geq 1$ gilt dies aufgrund der Multiplikationsregel; für den Fall $k = 0$ ist die Antwort ebenfalls richtig, da sowohl $|M^0| = 1$ als auch $n^0 = 1$ gilt.

Beispiele:

1. Es sei $M = \big\{a, b\big\}$ und $k = 3$. Es gibt insgesamt 2^3 k-Tupel:

$$\begin{array}{llll} (a,a,a) & (a,a,b) & (a,b,a) & (a,b,b) \\ (b,a,a) & (b,a,b) & (b,b,a) & (b,b,b) \end{array}$$

2. Es sei $M = \big\{a, b, c, d, e, f, g\big\}$ und $k = 3$. Es gibt 7^3 k-Tupel.

Grundaufgabe 2

Zur Vorbereitung von Grundaufgabe 2 führen wir zunächst eine Bezeichnung ein.

Definition.

Für $k, n \in \mathbb{N} \cup \big\{0\big\}$ sei $n^{\underline{k}}$ wie folgt definiert:

$$n^{\underline{k}} := \begin{cases} n \cdot \big(n-1\big) \cdot \ldots \cdot \big(n-k+1\big) & \text{, falls } k \geq 1 \\ 1 & \text{, falls } k = 0 \end{cases}$$

Beispiele:

1. $7^{\underline{3}} = 7 \cdot 6 \cdot 5 = 210$

2. $7^{\underline{2}} = 7 \cdot 6 = 42$

3. $7^{\underline{1}} = 7$

4. $7^{\underline{0}} = 1$

Frage: Es sei $k \geq 0$ sowie $n \geq 0$: Wie viele k-Tupel, in denen kein Element mehrfach auftritt, kann man aus einer n-elementigen Menge M bilden?

Antwort: $n^{\underline{k}}$

Begründung: Für $k \geq 1$ erhält man dies aufgrund der Multiplikationsregel; für $k = 0$ ist die Antwort wegen $n^{\underline{0}} = 1$ richtig.

Beispiel: Es sei $M = \{a, b, c, d, e, f, g\}$ (also $n = 7$) und $k = 4$. Ein k-Tupel, bei dem ein Element mehrfach auftritt, ist dann beispielsweise (b, f, b, a). Solche k-Tupel sind in Grundaufgabe 2 „verboten“. Die Antwort zur Grundaufgabe 2 lautet hier:

$$7^{\underline{4}} = 7 \cdot 6 \cdot 5 \cdot 4 = 840.$$

Definition.
Eine bijektive Abbildung einer Menge M auf sich selbst nennt man eine *Permutation von M*.

Beispiel. Es sei $M = \{a, b, c\}$. Eine Permutation π von M ist dann beispielsweise die Abbildung $\pi : M \to M$, die durch

$$\pi(a) = c, \qquad \pi(b) = a \qquad \text{und} \qquad \pi(c) = b$$

gegeben ist.

Ist M eine endliche Menge, etwa $M = \{m_1, \ldots, m_n\}$, so schreibt man Permutationen π von M gewöhnlich in der Form

$$\begin{pmatrix} m_1 & m_2 & \ldots & m_n \\ \pi(m_1) & \pi(m_2) & \ldots & \pi(m_n) \end{pmatrix}.$$

Die Permutation π des obigen Beispiels wird in dieser Schreibweise so dargestellt:

$$\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}.$$

Für den Spezialfall $n = k$ ergibt sich aus der Lösung von Grundaufgabe 2, dass die Anzahl der Permutationen einer n-elementigen Menge gleich

$$n^{\underline{n}} = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$$

ist. Anstelle von $n^{\underline{n}}$ schreibt man gewöhnlich $n!$ (sprich: n *Fakultät*). Es gilt also beispielsweise:

$$\begin{array}{rcccl} 0! & = & 0^{\underline{0}} & = & 1 \\ 1! & = & 1^{\underline{1}} & = & 1 \\ 2! & = & 2^{\underline{2}} & = & 2 \cdot 1 = 2 \\ 3! & = & 3^{\underline{3}} & = & 3 \cdot 2 \cdot 1 = 6 \\ 4! & = & 4^{\underline{4}} & = & 4 \cdot 3 \cdot 2 \cdot 1 = 24 \\ 5! & = & 5^{\underline{5}} & = & 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120 \\ 10! & = & 10^{\underline{10}} & = & 10 \cdot \ldots \cdot 2 \cdot 1 = 3628800 \end{array}$$

Beispiele:

1. Es sei $M = \{a, b, c\}$.

Es gibt insgesamt $3! = 6$ Permutationen von M:

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

2. Es sei $M = \{a, b, c, d, e, f, g\}$.

Es gibt insgesamt $7! = 5040$ Permutationen von M.

Grundaufgabe 3

Frage: Es sei $n \geq k \geq 0$. Wie viele k-elementige Teilmengen hat eine n-elementige Menge M?

Antwort: $\dfrac{n^{\underline{k}}}{k!}$.

Begründung: Um die gesuchte Anzahl t der k-elementigen Teilmengen einer n-elementigen Menge M zu bestimmen, können wir das Ergebnis von Grundaufgabe 2 verwenden; dort hatten wir k-Tupel von Elementen von M betrachtet, in denen kein Element mehrfach auftritt. Die k-elementigen Teilmengen von M unterscheiden sich von diesen k-Tupeln genau dadurch, dass bei den Mengen die Reihenfolge der Elemente keine Rolle spielt. Da jede k-elementige Teilmenge von M auf genau $k!$ Arten angeordnet werden kann und es nach Grundaufgabe 2 genau $n^{\underline{k}}$ derartige k-Tupel gibt, erhalten wir $t \cdot k! = n^{\underline{k}}$. Es folgt wie behauptet $t = \frac{n^{\underline{k}}}{k!}$. □

Für die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge schreibt man $\binom{n}{k}$; man nennt diese Zahlen *Binomialkoeffizienten*. Es gilt also

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!}.$$

Durch Erweitern mit $(n-k)!$ ergibt sich:

$$\frac{n^{\underline{k}}}{k!} = \frac{n^{\underline{k}} \cdot (n-k)!}{k! \cdot (n-k)!} = \frac{n!}{k! \cdot (n-k)!} \ .$$

Insgesamt hat sich also als Lösung von Grundaufgabe 3 Folgendes ergeben:

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n!}{k! \cdot (n-k)!} \ . \tag{2.18}$$

Für $k \geq 1$ kann man alternativ die obige Formel (2.18) auch so schreiben:

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!} = \frac{n!}{k! \cdot (n-k)!} \ . \tag{2.18'}$$

Ein **Beispiel** zu (2.18'): Wir fragen uns, wie viele 3-elementige Teilmengen eine 7-elementige Menge besitzt?

Antwort: Nach (2.18') ist die Anzahl der Teilmengen gleich:

$$\binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2 \cdot 1} = 35.$$

Pascalsches Dreieck

Für die Zahlen $\binom{n}{k}$ gilt folgende Identität:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \qquad (\text{für } n \geq 2 \text{ und } 1 \leq k \leq n-1) \tag{2.19}$$

Die Gleichung (2.19) kann man leicht nachprüfen, indem man

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}, \quad \binom{n-1}{k} = \frac{(n-1)!}{k! \cdot (n-1-k)!} \quad \text{sowie} \quad \binom{n-1}{k-1} = \frac{(n-1)!}{(k-1)! \cdot (n-k)!}$$

einsetzt (vgl. (2.18)) und anschließend durch geeignetes Umformen und Zusammenfassen die Gleichheit zeigt.

Mit Hilfe von (2.19) können die Binomialkoeffizienten rekursiv berechnet werden; dabei ordnet man die Binomialkoeffizienten im *Pascalschen Dreieck* an:

$$\begin{array}{ccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
\iddots & & & & & & \vdots & & & & & & \ddots
\end{array}$$

Nach (2.19) erhält man die Zahl $\binom{n}{k}$ für $n \geq 2$ und $1 \leq k \leq n-1$, indem man die beiden versetzt über $\binom{n}{k}$ stehenden Zahlen addiert:

$$\begin{array}{ccc}
\binom{n-1}{k-1} & & \binom{n-1}{k} \\
& \searrow \quad \swarrow & \\
& \binom{n}{k} &
\end{array}$$

Auf diese Weise kann man leicht die Werte in den ersten Zeilen des Pascalschen Dreiecks berechnen:

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
\iddots & & & & & & \vdots & & & & & & \ddots
\end{array}$$

Die Binomialkoeffizienten treten im *Binomischen Lehrsatz* auf ($a, b \in \mathbb{R}$).

Satz (Binomischer Lehrsatz).
Für alle $n \in \mathbb{N} \cup \{0\}$ gilt:

$$\begin{aligned}
(a+b)^n &= \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \\
&= a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \ldots + \binom{n}{n-1} a b^{n-1} + b^n
\end{aligned}$$

Als Koeffizienten tauchen im Binomischen Lehrsatz also immer die Zahlen auf, die in der entsprechenden Zeile des Pascalschen Dreiecks stehen.

Beispiele:

1. Für $n = 2$ ist der Binomische Lehrsatz nichts anderes als die bekannte Formel $(a+b)^2 = a^2 + 2ab + b^2$.

2. Für $n = 3$ gilt: $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.

3. Für $n = 4$ gilt: $(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$.

4. Für $n = 5$ gilt: $(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$.

Um die Richtigkeit des Binomischen Lehrsatzes einzusehen, schauen wir uns zunächst exemplarisch den Fall $n = 3$ an:

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

Wir berechnen dies durch Ausmultiplizieren:

$$\begin{aligned}(a+b)^3 &= (a+b)\cdot(a+b)\cdot(a+b)\\ &= (aa+ab+ba+bb)\cdot(a+b)\\ &= aaa+aab+aba+abb+baa+bab+bba+bbb\\ &= a^3+a^2b+a^2b+ab^2+a^2b+ab^2+ab^2+b^3\\ &= a^3+3a^2b+3ab^2+b^3\end{aligned}$$

Ebenso gehen wir jetzt im allgemeinen Fall vor: Es ist

$$(a+b)^n = \underbrace{(a+b)\cdot(a+b)\cdot\ldots\cdot(a+b)}_{n \text{ Faktoren}}.$$

Wir wollen die n Faktoren $(a+b)$ mit F_1, F_2, …, F_n bezeichnen, also:

$$F_1 = F_2 = \ldots = F_n = (a+b).$$

Folglich gilt:

$$\begin{aligned}(a+b)^n &= (a+b)\cdot(a+b)\cdot\ldots\cdot(a+b)\\ &= F_1\cdot F_2\cdot\ldots\cdot F_n\end{aligned}$$

Wir berechnen dieses Produkt durch das übliche Ausmultiplizieren: Wir wählen aus $F_1 = (a+b)$ entweder a oder b aus, wir wählen sodann aus $F_2 = (a+b)$ entweder a oder b aus, …, und schließlich wählen wir aus $F_n = (a+b)$ entweder a oder b aus. Die so gewählten n Werte multiplizieren wir nun miteinander: Haben wir beispielsweise beim ersten, zweiten und beim letzten Mal b und sonst immer a ausgewählt, so erhalten wir das Produkt $b\cdot b\cdot a\cdot\ldots\cdot a\cdot b = a^{n-3}b^3$.

Derartige Produkte bilden wir für alle möglichen Auswahlen von a und b; so erhalten wir jedes Mal einen Summanden der Form $a^{n-i}b^i$, wobei $0\le i\le n$ gilt. Für jedes i fassen wir danach die Summanden $a^{n-i}b^i$ zusammen. Für festes i gibt es genau $\binom{n}{i}$ Summanden $a^{n-i}b^i$, da jedem solchen Summanden eine der $\binom{n}{i}$ Möglichkeiten entspricht, aus der Menge $\{F_1, F_2, \ldots, F_n\}$ die Teilmenge derjenigen i Faktoren zu bestimmen, aus denen beim Ausmultiplizieren b ausgewählt wird. □

Obiger Beweis des Binomischen Lehrsatzes gibt „die Idee, die hinter dem Binomischen Lehrsatz steckt“, wieder. Eine andere Möglichkeit: Man beweist unter Verwendung von (2.19) den Binomischen Lehrsatz durch vollständige Induktion (Übungsaufgabe!).

Setzt man im Binomischen Lehrsatz für a und b jeweils 1 ein, so erhält man:

$$\sum_{i=0}^{n}\binom{n}{i} = 2^n\ . \tag{2.20}$$

Dies bedeutet, dass die Anzahl der Teilmengen einer n-elementigen Menge 2^n ist.

Setzt man im Binomischen Lehrsatz $a=1$ und $b=-1$ ein, so erhält man für $n\ge 1$:

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i} = 0 \tag{2.21}$$

Deutung der Formel (2.21) am Pascalschen Dreieck:

$$\begin{array}{ccccccccccccccccccc}
 & & & & & & 1 & - & 1 & = & 0 & & & & & & & & \\
 & & & & & 1 & - & 2 & + & 1 & = & 0 & & & & & & & \\
 & & & & 1 & - & 3 & + & 3 & - & 1 & = & 0 & & & & & & \\
 & & & 1 & - & 4 & + & 6 & - & 4 & + & 1 & = & 0 & & & & & \\
 & & 1 & - & 5 & + & 10 & - & 10 & + & 5 & - & 1 & = & 0 & & & & \\
 & 1 & - & 6 & + & 15 & - & 20 & + & 15 & - & 6 & + & 1 & = & 0 & & & \\
\iddots & & & & & & & \vdots & & & & & & & & & \ddots & &
\end{array}$$

Etwas anders ausgedrückt besagt die Formel (2.21), dass für jede nichtleere endliche Menge M gilt: Es gibt ebenso viele Teilmengen von M mit einer geraden Anzahl von Elementen wie Teilmengen von M mit einer ungeraden Anzahl von Elementen.

Abschließend sei noch folgende häufig benutzte Formel aufgeführt, die sich unmittelbar aus (2.18) ergibt:

$$\binom{n}{k} = \binom{n}{n-k} . \tag{2.22}$$

Man beachte, dass auch Formel (2.22) eine anschauliche Deutung am Pascalschen Dreieck besitzt. (Nämlich welche?)

Grundaufgabe 4

Die 4. Grundaufgabe soll hier in einer anschaulichen Darstellungsform präsentiert werden: Zur Wahl (etwa eines Vorsitzenden) stellen sich n Personen P_1, P_2, ..., P_n ($n \geq 1$) und es gibt k Wähler, die in einer geheimen Abstimmung jeweils genau einen Kandidaten wählen ($k \geq 0$). **Frage**: Wie viele mögliche Wahlergebnisse gibt es? Ein Wahlergebnis ist eine Liste der folgenden Art:

P_1	P_2	P_3	...	P_n
$\surd\surd$		$\surd\surd\surd$	...	$\surd$

Immer wenn P_i eine Stimme bekommen hat, wird beim Auszählen ein Haken in die entsprechende Spalte eingetragen. Eine derartige Liste kann durch ein $(k+n-1)$-Tupel aus Nullen und Einsen beschrieben werden, wobei die Nullen den $n-1$ Trennstrichen und die Einsen den k Haken entsprechen. Im Beispiel der oben abgebildeten Liste sieht das zugehörige $(k+n-1)$-Tupel so aus: $(1,1,0,0,1,1,1,0,\ldots,0,1)$.

Die Anzahl der Möglichkeiten, in dem $(k+n-1)$-Tupel die k Plätze für die Einsen auszuwählen, ist

$$\binom{k+n-1}{k}$$

Also lautet die Lösung: Es gibt $\binom{k+n-1}{k}$ mögliche Wahlergebnisse.

Hinweis: Man beachte, dass auf Grund von (2.22) $\binom{k+n-1}{k} = \binom{k+n-1}{n-1}$ gilt. Also hätte man ebenso gut feststellen können: Es gibt $\binom{k+n-1}{n-1}$ mögliche Wahlergebnisse.

Grundaufgabe 5

Die fünfte Grundaufgabe soll zunächst an einem Beispiel illustriert werden.

Frage: Wie viele verschiedene (sinnvolle oder sinnlose) Wörter mit acht Buchstaben kann man durch Veränderung der Reihenfolge aus den Buchstaben des Wortes $ANAGRAMM$ bilden?

Antwort: $\dfrac{8!}{3! \cdot 2!} = 3360$.

Begründung: Wir stellen uns zunächst vor, die mehrfach auftretenden Buchstaben „A“ bzw. „M“ in dem Wort $ANAGRAMM$ seien unterscheidbar und bezeichnen sie dementsprechend mit A_1, A_2 und A_3 sowie M_1 und M_2. Wir unterscheiden also zunächst einmal beispielsweise zwischen $A_1NA_2GRA_3M_1M_2$ und $A_2NA_1GRA_3M_1M_2$. Unter dieser Voraussetzung kann man genau 8! unterschiedliche Buchstabenfolgen bilden. Diese 8! Buchstabenfolgen zerfallen in disjunkte Klassen von jeweils $3! \cdot 2! = 12$ Buchstabenfolgen, die in Wirklichkeit nicht unterscheidbar sind; beispielsweise bilden die folgenden 12 Buchstabenfolgen eine solche Klasse:

$A_1M_1M_2A_2GRA_3N$	$A_1M_1M_2A_3GRA_2N$	$A_2M_1M_2A_1GRA_3N$
$A_2M_1M_2A_3GRA_1N$	$A_3M_1M_2A_1GRA_2N$	$A_3M_1M_2A_2GRA_1N$
$A_1M_2M_1A_2GRA_3N$	$A_1M_2M_1A_3GRA_2N$	$A_2M_2M_1A_1GRA_3N$
$A_2M_2M_1A_3GRA_1N$	$A_3M_2M_1A_1GRA_2N$	$A_3M_2M_1A_2GRA_1N$

Man erhält also wie behauptet $\frac{8!}{3!\cdot 2!}$ verschiedene Wörter.

Die Verallgemeinerung dieses Beispiels führt zur allgemeinen Form von Grundaufgabe 5.

Frage: Gegeben seien r verschiedene Zeichen Z_1, ..., Z_r ($r \geq 1$). Wie viele verschiedene Zeichenfolgen der Länge n kann man aus den Zeichen Z_1, ..., Z_r unter den folgenden Bedingungen bilden?

$$\begin{array}{c} Z_1 \text{ kommt genau } n_1 \text{ mal vor;} \\ Z_2 \text{ kommt genau } n_2 \text{ mal vor;} \\ \vdots \\ Z_r \text{ kommt genau } n_r \text{ mal vor.} \end{array}$$

Hierbei gelte $\sum\limits_{i=1}^{r} n_i = n$ sowie $n_i \geq 0$ $(i = 1, \ldots, r)$.

Antwort: $\dfrac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_r!}$.

Man beachte, dass einige der Zahlen n_1, ..., n_r gleich 0 oder 1 sein können. Wegen $0! = 1! = 1$ kann man dann die entsprechenden Faktoren $n_i!$ im Nenner der Lösung weglassen. Im obigen Beispiel kamen etwa die Buchstaben G, R und N jeweils nur einmal vor; deshalb konnten wir anstelle von $\frac{8!}{3!\cdot 2!\cdot 1!\cdot 1!\cdot 1!}$ einfach $\frac{8!}{3!\cdot 2!}$ schreiben.

Die in der Antwort zu Grundaufgabe 5 auftretenden Zahlen nennt man *Multinomialkoeffizienten* und bezeichnet sie mit $\binom{n}{n_1,\ldots,n_r}$. Man definiert also für ganze Zahlen n_1, ..., n_r mit $n_i \geq 0$ $(i = 1, \ldots, r)$ und $\sum\limits_{i=1}^{r} n_i = n$:

$$\binom{n}{n_1, \ldots, n_r} = \frac{n!}{n_1! \cdot \ldots \cdot n_r!}.$$

Im *Spezialfall* $r = 2$ stimmen die Multinomialkoeffizienten mit den zuvor behandelten Binomialkoeffizienten überein; es gilt nämlich (wegen $n_1 + n_2 = n$):

$$\begin{aligned} \binom{n}{n_1, n_2} = \frac{n!}{n_1! \cdot n_2!} &= \frac{n!}{n_1! \cdot (n - n_1)!} = \binom{n}{n_1} \\ \binom{n}{n_1, n_2} = \frac{n!}{n_1! \cdot n_2!} &= \frac{n!}{n_2! \cdot (n - n_2)!} = \binom{n}{n_2} \end{aligned}$$

Der Vollständigkeit halber merken wir an, dass die Lösung von Grundaufgabe 5 auch den (sehr speziellen) Fall $n = n_1 = \ldots = n_r = 0$ abdeckt. Dann gilt:

$$\binom{n}{n_1, \ldots, n_r} = \frac{0!}{0! \cdot \ldots \cdot 0!} = 1 \ .$$

Andererseits gibt es auch genau eine Zeichenfolge der Länge 0, nämlich die *leere Zeichenfolge*, worunter nichts anderes als die leere Menge $\emptyset$ zu verstehen ist.

2.7 Ergänzungen zur elementaren Kombinatorik

2.7.1 Ziehen von Elementen aus einer Menge

Die ersten vier Grundaufgaben lassen sich auch als Fragen zum Ziehen von Elementen aus einer Menge formulieren. Die *Grundfrage* lautet dabei:

Wie viele Möglichkeiten gibt es, k Elemente aus einer n-elementigen Menge zu ziehen?

Die Antwort auf diese Frage ist davon abhängig, welche „Spielregeln“ für das Ziehen gelten; man unterscheidet

- Ziehen mit Zurücklegen, geordnet
- Ziehen ohne Zurücklegen, geordnet
- Ziehen ohne Zurücklegen, ungeordnet
- Ziehen mit Zurücklegen, ungeordnet

Die Menge, aus der die Elemente gezogen werden, wird im Folgenden immer mit M bezeichnet; es gilt also immer

$$|M| = n.$$

Um etwas spitzfindige Diskussionen, die sich um die leere Menge drehen, zu vermeiden, setzen wir $n \geq 1$ und $k \geq 1$ voraus. Im Fall des Ziehens ohne Zurücklegen sei aus ähnlichen Gründen $n \geq k$ vorausgesetzt.

1) Ziehen mit Zurücklegen, geordnet

Wie viele Möglichkeiten gibt es, k Elemente aus M zu ziehen, wobei die gezogenen Elemente jeweils zurückgelegt werden und es auf die Reihenfolge, in der die Elemente gezogen werden, ankommen soll?

Unter diesen Bedingungen kann das Ergebnis des k-maligen Ziehens als ein k-Tupel ausgedrückt werden: Ist beispielsweise $M = \{a, b, c, d, e\}$ und wird bei 4-maligem Ziehen (d.h. $k = 4$) zunächst b, dann a und danach zweimal d gezogen, so lässt sich das Ergebnis durch das 4-Tupel (b, a, d, d) ausdrücken. Ergebnisse von Ziehungen und k-Tupel entsprechen sich also umkehrbar eindeutig. Es liegt demnach (in anderer Formulierung) Grundaufgabe 1 vor, und man erkennt, dass die Antwort

$$n^k$$

lautet.

2) Ziehen ohne Zurücklegen, geordnet

Wie in 1) soll es auf die Reihenfolge ankommen, aber gezogene Elemente sollen *nicht* wieder zurückgelegt werden. In diesem Fall liegt (in anderer Formulierung) Grundaufgabe 2 vor; die Antwort lautet also

$$n^{\underline{k}} = n \cdot (n-1) \cdot \ldots \cdot (n-k+1).$$

3) Ziehen ohne Zurücklegen, ungeordnet

Wie in 2) werden gezogene Elemente nicht wieder zurückgelegt, aber es soll diesmal nicht auf die Reihenfolge ankommen; wird beispielsweise im Fall $k = 3$ zunächst b, dann a und danach c gezogen, so soll jede beliebige andere Reihenfolge, in der die Elemente a, b, c gezogen werden, als das gleiche Ergebnis angesehen werden. Das Ergebnis einer Ziehung kann demnach eindeutig als k-elementige Teilmenge von M beschrieben werden. Es liegt also (in anderer Formulierung) Grundaufgabe 3 vor und wir erhalten, dass die Antwort im vorliegenden Fall lautet:

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!}$$

4) Ziehen mit Zurücklegen, ungeordnet

Wie viele Möglichkeiten gibt es, k Elemente aus M zu ziehen, wobei die gezogenen Elemente jeweils zurückgelegt werden und es auf die Reihenfolge, in der die Elemente gezogen werden, *nicht* ankommen soll?

Beispiel: $M = \{a, b, c, d, e\}, k = 4$. Wir betrachten zwei mögliche Abläufe:

a) Erst wird c gezogen, dann a und danach zweimal e,

b) erst wird e gezogen, dann a, danach c und am Schluss wieder e.

Da es nicht auf die Reihenfolge, in der die Elemente gezogen werden, ankommen soll, betrachten wir die Ergebnisse der beiden Ziehungen als gleich. Mit anderen Worten: Es kommt im vorliegenden Fall nur darauf an, *wie oft* jedes einzelne Element gezogen wurde, und deshalb können wir das Ergebnis der obigen Ziehung auch wie folgt in einer Liste notieren:

a	b	c	d	e
$\surd$		$\surd$		$\surd\surd$

Dabei wird, immer wenn ein Element gezogen wird, ein Haken in das entsprechende Kästchen gemacht.

Im allgemeinen Fall (d.h. für ein beliebiges n und k) geht man entsprechend vor. Man nummeriert zunächst die Elemente von M:

$$M = \{a_1, \ldots, a_n\}.$$

Dann entspricht jedem Ergebnis einer k-fachen Ziehung umkehrbar eindeutig eine Liste, in die wie beschrieben Haken eingetragen werden:

a_1	a_2	$\ldots$	a_n

Ein Vergleich mit Grundaufgabe 4 zeigt: Es liegt genau diese Grundaufgabe vor - nur in anderer Formulierung. Die Antwort lautet im vorliegenden Fall also, dass es genau

$$\binom{k+n-1}{k}$$

Möglichkeiten gibt.

Wir können unsere Ergebnisse in einer Tabelle zusammenfassen:

	geordnet	ungeordnet
mit Zurücklegen	n^k	$\binom{k+n-1}{k}$
ohne Zurücklegen	$n^{\underline{k}}$	$\binom{n}{k}$

Anzahl der Möglichkeiten, k Elemente aus einer n-elementigen Menge zu ziehen

2.7.2 Der Multinomialsatz

In ähnlicher Weise, wie die Binomialkoeffizienten im *Binomischen Lehrsatz* $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$ auftreten, treten die Multinomialkoeffizienten in folgendem Satz auf, den man *Multinomialsatz* nennt.

Multinomialsatz.
Für $r \geq 2$ und $n \geq 0$ gilt

$$(x_1 + x_2 + \ldots + x_r)^n = \sum \binom{n}{n_1, n_2, \ldots, n_r} x_1^{n_1} \cdot x_2^{n_2} \cdot \ldots \cdot x_r^{n_r},$$

wobei die Summe über alle r-Tupel $(n_1, n_2, \ldots, n_r)$ nichtnegativer ganzer Zahlen genommen wird, für die $n_1 + n_2 + \ldots + n_r = n$ gilt.

Man beachte, dass der Multinomialsatz für $r = 2$ dasselbe aussagt wie der Binomische Lehrsatz. Ganz ähnlich, wie wir den Binomischen Lehrsatz bewiesen haben (vgl. Seite 38/39), lässt sich auch der Multinomialsatz beweisen. Wir geben eine **Beweisskizze**: Berechnet man das Produkt

$$(x_1 + x_2 + \ldots + x_r)^n = \underbrace{(x_1 + x_2 + \ldots + x_r) \cdot \ldots \cdot (x_1 + x_2 + \ldots + x_r)}_{n \text{ Faktoren}}$$

durch das übliche Ausmultiplizieren, so erhält man eine Summe von Ausdrücken der Art

$$x_1^{n_1} \cdot x_2^{n_2} \cdot \ldots \cdot x_r^{n_r} \tag{2.23}$$

wobei $n_1, \ldots, n_r$ nichtnegative ganze Zahlen mit $n_1 + n_2 + \ldots + n_r = n$ sind.

Für den Rest der Beweisskizze betrachten wir nun ein *fest gewähltes r-Tupel* $(n_1, \ldots, n_r)$ nichtnegativer ganzer Zahlen mit $n_1 + n_2 + \ldots + n_r = n$. Beim Ausmultiplizieren tritt der Summand (2.23) genau dann auf, wenn

x_1 aus genau n_1 Faktoren gewählt wurde,

x_2 aus genau n_2 Faktoren gewählt wurde,

$\vdots$

x_r aus genau n_r Faktoren gewählt wurde.

Jeder derartigen Auswahl entspricht genau eine Zeichenfolge der Länge n, die aus den Zeichen $x_1, \ldots, x_r$ gebildet wird, wobei

x_1 genau n_1 mal vorkommt,

x_2 genau n_2 mal vorkommt,

$\vdots$

x_r genau n_r mal vorkommt.

Also gilt nach Grundaufgabe 5: Für ein festes n-Tupel $(n_1, \ldots, n_r)$ tritt der Summand (2.23) genau $\binom{n}{n_1, n_2, \ldots, n_r}$ mal auf. □

Beispiel. Zu berechnen ist der Koeffizient von $x^5y^3z^2$ in $(x + y + z)^{10}$. Lösung:

$$\binom{10}{5, 3, 2} = \frac{10!}{5! \cdot 3! \cdot 2!} = \frac{6 \cdot 7 \cdot 8 \cdot 9 \cdot 10}{3! \cdot 2!} = \frac{7 \cdot 8 \cdot 9 \cdot 10}{2} = 7 \cdot 4 \cdot 9 \cdot 10 = 2520.$$

2.7.3 Das Schubfachprinzip (pigeonhole principle)

Es seien $m, n \in \mathbb{N}$. Wir geben zunächst zwei äquivalente Formulierungen des Schubfachprinzips in seiner einfachsten Form an:

1. Wenn n Objekte auf m Fächer verteilt werden und es gilt $n > m$, dann gibt es mindestens ein Fach, in das mindestens zwei Objekte hineinkommen.

Zur Abkürzung schreiben wir $\mathbb{N}_m := \{1, \ldots, m\}$ und ebenso $\mathbb{N}_n := \{1, \ldots, n\}$.

2. Ist $f : \mathbb{N}_n \longrightarrow \mathbb{N}_m$ eine Funktion und gilt $n > m$, so ist f nicht injektiv.

Ein einfaches **Beispiel**: In jeder Menge von 13 oder mehr Menschen gibt es mindestens zwei, die im gleichen Monat Geburtstag haben.

Varianten bzw. Erweiterungen des Schubfachprinzips (für $\mathbf{n, m} \in \mathbb{N}$)

3. Wenn n Objekte auf m Fächer verteilt werden, dann gibt es mindestens ein Fach, in das mindestens

$$\left\lceil \frac{n}{m} \right\rceil$$

Objekte hineinkommen.

Einfache Beispiele:

(i) In einer Menge von 100 Menschen gibt es mindestens 9, die im gleichen Monat Geburtstag haben;

(ii) in einer Menge von 501 in den U.S.A. geborenen Menschen gibt es mindestens 11, die im gleichen Bundesstaat geboren wurden.

Beweis von 3. Angenommen, die Aussage wäre nicht wahr. Dann würde es in jedem Fach höchstens $\lceil \frac{n}{m} \rceil - 1$ Objekte geben; insgesamt hätten wir also höchstens $m\left(\lceil \frac{n}{m} \rceil - 1\right)$ Objekte, d.h. $n \leq m\left(\lceil \frac{n}{m} \rceil - 1\right)$. Durch Umformung erhält man hieraus

$$1 \leq \left\lceil \frac{n}{m} \right\rceil - \frac{n}{m},$$

was nicht sein kann, da der Abstand zwischen einer reellen Zahl a und $\lceil a \rceil$ immer kleiner als 1 ist. □

4. Wenn unendlich viele Objekte auf m Fächer verteilt werden (für $m \in \mathbb{N}$), dann gibt es mindestens ein Fach, in das unendlich viele Objekte hineinkommen.

   Dies kann auch wie folgt formuliert werden:

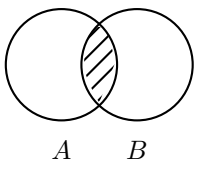
5. Ist $f : U \longrightarrow \mathbb{N}_m$ eine Funktion und ist U eine unendliche Menge, dann gibt es ein $j \in \mathbb{N}_m$, auf das unendlich viele $u \in U$ abgebildet werden.

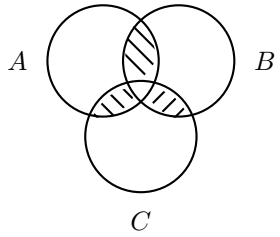
2.7.4 Das Prinzip der Inklusion und Exklusion (Siebformel)

Alle in diesem Abschnitt auftretende Mengen seien endlich. Unser Ziel ist es, eine Formel für die Anzahl der Elemente in der Vereinigung von n Mengen $A_1, \ldots, A_n$ herzuleiten. Mit anderen Worten: Wir suchen eine Formel für die Anzahl

$$|A_1 \cup A_2 \cup \ldots \cup A_n|.$$

Zur Orientierung betrachten wir zunächst den Fall zweier Mengen A, B und dann den Fall dreier Mengen A, B, C. Dabei ist es nützlich, die zugehörigen Venn-Diagramme vor Augen zu haben:





Die Formel $|A \cup B| = |A| + |B|$ für die Anzahl der Elemente der Vereinigung zweier endlicher Mengen ist nur dann gültig, wenn A und B disjunkt sind; ist dies nicht der Fall, so muss man, damit die Elemente aus $A \cap B$ nicht doppelt gezählt werden, noch zusätzlich $|A \cap B|$ abziehen. Die korrekte Formel lautet somit

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Im Fall dreier Mengen gehen wir ähnlich vor: Um Elemente aus den Durchschnitten $A \cap B$, $A \cap C$, $B \cap C$ nicht doppelt zu zählen, ziehen wir von $|A| + |B| + |C|$ die Ausdrücke $|A \cap B|$, $|A \cap C|$ und $|B \cap C|$ ab und gelangen zu $|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C|$. Dies ist aber noch nicht die korrekte Formel

für $|A \cup B \cup C|$, da wir die Elemente aus $A \cap B \cap C$ nicht berücksichtigt haben: Diese wurden in dem Ausdruck $|A| + |B| + |C|$ zunächst 3-fach gezählt, dann aber auch 3-mal wieder abgezogen. Die korrekte Formel lautet demnach: $|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$.

Für beliebiges n erhält man auf ganz ähnliche Art eine Formel für $|A_1 \cup A_2 \cup \ldots \cup A_n|$:

Zunächst addiert man alle Anzahlen $|A_1|, |A_2|, \ldots, |A_n|$; danach subtrahiert man die Anzahlen $|A_1 \cap A_2|, |A_1 \cap A_3|, \ldots, |A_{n-1} \cap A_n|$ aller möglichen Durchschnitte von jeweils zwei Mengen; danach betrachtet man sämtliche Möglichkeiten, Durchschnitte $A_i \cap A_j \cap A_k$ mit $i < j < k$ zu bilden, und addiert die zugehörigen Anzahlen $|A_i \cap A_j \cap A_k|$; danach werden alle möglichen Ausdrücke der Form $|A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{i_4}|$ $(i_1 < i_2 < i_3 < i_4)$ subtrahiert, etc.

Für $n = 4$ lautet die entsprechende Formel: $|A_1 \cup A_2 \cup A_3 \cup A_4| = |A_1| + |A_2| + |A_3| + |A_4| - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_4| + |A_2 \cap A_3| + |A_2 \cap A_4| + |A_3 \cap A_4|) + (|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4|) - |A_1 \cap A_2 \cap A_3 \cap A_4|$.

Für die allgemeine Formulierung der Formel ist es zweckmäßig, das Summenzeichen zu verwenden: Anstelle von $|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4|$ schreiben wir beispielsweise

$$\sum_{1 \le i_1 < i_2 < i_3 \le 4} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|.$$

Satz (Prinzip der Inklusion und Exklusion, Siebformel).
Für endliche Mengen $A_1, \ldots, A_n$ gilt

$$|A_1 \cup \ldots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{1 \le i_1 < \ldots < i_r \le n} |A_{i_1} \cap \ldots \cap A_{i_r}|.$$

Beweis. Es sei $a \in A_1 \cup \ldots \cup A_n$ beliebig. Auf der linken Seite, d.h. in dem Ausdruck $|A_1 \cup \ldots \cup A_n|$, wird das Element a genau einmal gezählt. Wir haben deshalb zu zeigen, dass a auch auf der rechten Seite genau einmal gezählt wird. Aus diesem Grunde richten wir unser Augenmerk auf diejenigen Mengen A_i, für die $a \in A_i$ gilt; es sei

$$k := |\{1 \le i \le n : a \in A_i\}|,$$

d.h. k gibt die Anzahl derjenigen Indices i an, für die $a \in A_i$ gilt. Es folgt, dass a in der Summe

$$\sum_{1 \le i_1 < \ldots < i_r \le n} |A_{i_1} \cap \ldots \cap A_{i_r}|$$

genau $\binom{k}{r}$ mal gezählt wird, falls $r \le k$ gilt, bzw. 0 mal, falls $r > k$ gilt. (Man beachte: a ist genau dann in $A_{i_1} \cap \ldots \cap A_{i_r}$ enthalten, wenn die Indices $i_1, \ldots, i_r$ alle aus der k-elementigen Menge $\{1 \le i \le n : a \in A_i\}$ stammen. Ist $r \le k$, so gibt es also $\binom{k}{r}$ Möglichkeiten, die Indices $i_1, \ldots, i_r$ aus der Menge $\{1 \le i \le n : a \in A_i\}$ auszuwählen; ist $r > k$, so ist eine derartige Auswahl unmöglich.)

Es folgt, dass das Element a auf der rechten Seite insgesamt genau

$$\sum_{r=1}^{k} (-1)^{r-1} \binom{k}{r}$$

mal gezählt wird. Aufgrund von Formel (2.21) (vgl. Seite 39) gilt für diese Summe

$$\sum_{r=1}^{k} (-1)^{r-1} \binom{k}{r} = \binom{k}{0} = 1,$$

d.h. a wird auf der rechten Seite genau einmal gezählt. □

Als Abkürzung für die in der Siebformel mit alternierendem Vorzeichen auftretenden Ausdrücke wollen wir α_r schreiben, d.h. wir setzen

$$\alpha_r := \sum_{1 \le i_1 < \ldots < i_r \le n} |A_{i_1} \cap \ldots \cap A_{i_r}| \ (r = 1, \ldots, n).$$

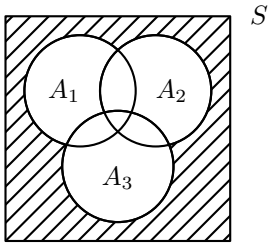
Mit dieser Abkürzung erhält man die Siebformel in kompakter Form:

$$|A_1 \cup \ldots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \ldots + (-1)^{n-1}\alpha_n.$$

In der Praxis benutzt man meistens die folgende direkte Folgerung aus der Siebformel. Es seien $A_1, \ldots, A_n$ Teilmengen einer gewissen Menge S mit $|S| = N$. Gefragt ist nach der Anzahl der Elemente von S, die in *keiner* der Mengen A_i enthalten sind. Für diese Anzahl gilt dann aufgrund der Siebformel

$$|S \setminus (A_1 \cup \ldots \cup A_n)| = N - \alpha_1 + \alpha_2 - \ldots + (-1)^n \alpha_n$$

Das folgende Venn-Diagramm und die anschließenden Beispiele illustrieren den Fall $n = 3$.



Beispiel 1: In einer Menge S von 95 Personen spielen 52 Fußball, 25 spielen Tennis und 20 spielen Golf. Sowohl Fußball als auch Tennis spielen 17 Personen, 12 spielen Fußball und Golf; Tennis und Golf werden von 7 Personen gespielt, und es gibt nur eine einzige Person, die allen drei Sportarten nachgeht. Wie viele Mitglieder von S betreiben keine der drei Sportarten?

Antwort: Nach der Siebformel sind dies genau 95 - (52 + 25 + 20) + (17 + 12 + 7) - 1 = 33 Personen.

Beispiel 2: Es sei $S = \{k \in \mathbb{N} : 1 \leq k \leq 1000\}$. Es soll die Anzahl derjenigen $k \in S$ bestimmt werden, die weder durch 2 noch durch 3 noch durch 5 teilbar sind.

Es sei $A_1 = \{k \in S : 2 \mid k\}, A_2 = \{k \in S : 3 \mid k\}, A_3 = \{k \in S : 5 \mid k\}$. Es folgt $N = |S| = 1000$ sowie $|A_1| = \frac{1000}{2} = 500, |A_2| = \left\lfloor \frac{1000}{3} \right\rfloor = 333, |A_3| = \frac{1000}{5} = 200$.

Ferner haben wir $A_1 \cap A_2 = \{k \in S : 6 \mid k\}, A_1 \cap A_3 = \{k \in S : 10 \mid k\}, A_2 \cap A_3 = \{k \in S : 15 \mid k\}$ und $A_1 \cap A_2 \cap A_3 = \{k \in S : 30 \mid k\}$. Also gilt $|A_1 \cap A_2| = \left\lfloor \frac{1000}{6} \right\rfloor = 166, |A_1 \cap A_3| = \frac{1000}{10} = 100, |A_2 \cap A_3| = \left\lfloor \frac{1000}{15} \right\rfloor = 66, |A_1 \cap A_2 \cap A_3| = \left\lfloor \frac{1000}{30} \right\rfloor = 33$.

Insgesamt erhält man $|S \setminus (A_1 \cup A_2 \cup A_3)| = 1000 - (500 + 333 + 200) + 166 + 100 + 66 - 33 = \underline{\underline{266}}$.

2.8 Abzählbarkeit von $\mathbb{Q}$ und Überabzählbarkeit von $\mathbb{R}$

Definition 1.
Man nennt zwei Mengen A und B *gleichmächtig*, wenn es eine bijektive Abbildung $f : A \to B$ gibt.

Wenn A und B endliche Mengen sind, so bedeutet die Feststellung „A und B sind gleichmächtig“ offenbar nichts anderes als „A und B besitzen die gleiche Anzahl von Elementen“. In diesem Abschnitt geht es uns allerdings nicht so sehr um endliche Mengen, sondern um unendliche Mengen wie beispielsweise $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$.

Definition 2.
Man nennt eine Menge M *abzählbar*, falls $|M|$ endlich ist oder falls es eine bijektive Abbildung $f : \mathbb{N} \to M$ gibt. Eine derartige bijektive Abbildung nennt man auch *Nummerierung*, *Durchnummerierung* oder *Abzählung* von M.

Beispiele abzählbarer Mengen:

1. Die Menge $M = \{2, 4, 6, \ldots\}$ der geraden natürlichen Zahlen ist abzählbar. Um dies nachzuweisen, müssen wir eine bijektive Abbildung $f : \mathbb{N} \to M$ angeben. Mit anderen Worten: Wir müssen die Elemente von $M = \{2, 4, 6, \ldots\}$ „durchnummerieren". Dies ist sehr einfach: Als erstes Element von M wählen wir 2, als zweites wählen wir 4, als drittes wählen wir 6, usw. Auf diese Art erhalten wir eine bijektive Abbildung $f : \mathbb{N} \to M$, die wir auch wie folgt darstellen können:

n	1	2	3	4	5	...
$f(n)$	2	4	6	8	10	...

bzw. $f(n) = 2n$.

2. Die Menge $\mathbb{Z}$ der ganzen Zahlen ist abzählbar.

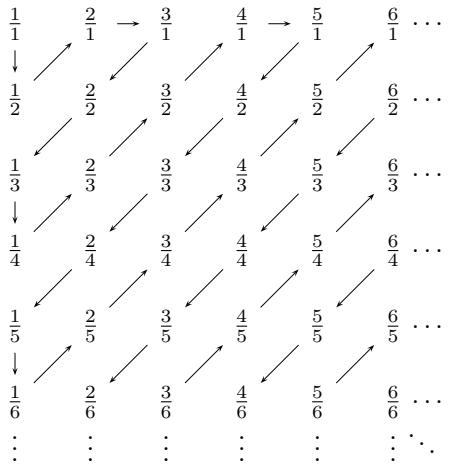
Man kann die ganzen Zahlen beispielsweise nach dem folgenden Schema durchnummerieren:

$$0,\ 1,\ -1,\ 2,\ -2,\ 3\ -3,\ 4,\ -4,\ 5,\ \ldots$$

3. Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar.

In diesem Fall ist das Schema, nach dem die Elemente von $\mathbb{Q}$ durchnummeriert werden, allerdings etwas komplizierter als beispielsweise im Fall von $\mathbb{Z}$.

Wir betrachten zunächst einmal die Menge $\mathbb{Q}^+$ der positiven rationalen Zahlen (d.h., $\mathbb{Q}^+ = \{q \in \mathbb{Q} : q > 0\}$) und zeigen, dass $\mathbb{Q}^+$ abzählbar ist. Wir machen dies mit dem sogenannten *ersten Cantorschen Diagonalverfahren*. Wir ordnen die Elemente von $\mathbb{Q}^+$ nach dem folgenden Schema an und folgen bei ihrer Nummerierung dem Verlauf der Pfeile. Alle Zahlen, die in der Nummerierung schon einmal (in anderer Darstellung) aufgetreten sind, werden einfach übersprungen.



Auf diese Art erhält man eine Nummerierung der Elemente von $\mathbb{Q}^+$, nämlich:

$$q_1 = 1, \quad q_2 = \frac{1}{2}, \quad q_3 = 2, \quad q_4 = 3, \quad q_5 = \frac{1}{3}, \quad q_6 = \frac{1}{4}, \quad \ldots$$

Hieraus kann man dann nach dem folgenden Schema eine Nummerierung sämtlicher Elemente von $\mathbb{Q}$ gewinnen:

$$0, \quad q_1, \quad -q_1, \quad q_2, \quad -q_2, \quad q_3, \quad -q_3, \quad \ldots$$

Wir haben also durch Angabe einer Nummerierung der Elemente von $\mathbb{Q}$ den folgenden Satz bewiesen.

Satz 1.
$\mathbb{Q}$ ist abzählbar.

Im Gegensatz hierzu gilt für die reellen Zahlen der folgende Satz.

Satz 2.
$\mathbb{R}$ ist nicht abzählbar.

Beweis. Es genügt nachzuweisen, dass die Menge $I = \{r \in \mathbb{R} : 0 \leq r < 1\}$ nicht abzählbar ist. Wegen $I \subseteq \mathbb{R}$ ist dann auch die Menge $\mathbb{R}$ nicht abzählbar. Wir führen einen Widerspruchsbeweis und nehmen daher an, dass diese Menge abzählbar sei: Es sei r_1, r_2, ... eine Nummerierung der Elemente von I. Wir stellen die Zahlen r_1, r_2, ... als unendliche Dezimalbrüche dar:

$$\begin{array}{rcll} r_1 & = & 0.s_{11}s_{12}s_{13}s_{14}s_{15} & \dots \\ r_2 & = & 0.s_{21}s_{22}s_{23}s_{24}s_{25} & \dots \\ r_3 & = & 0.s_{31}s_{32}s_{33}s_{34}s_{35} & \dots \\ r_4 & = & 0.s_{41}s_{42}s_{43}s_{44}s_{45} & \dots \\ & \vdots & & \\ r_i & = & 0.s_{i1}s_{i2}s_{i3}s_{i4}s_{i5} & \dots \\ & \vdots & & \end{array}$$

$s_{ij} \in \{0, 1, 2, \dots, 9\}$ bezeichnet also die j-te Stelle der Dezimalbruchdarstellung von r_i. Es sei vorausgesetzt, dass in diesen Dezimaldarstellungen nicht alle Ziffern von einer bestimmten Stelle an 9 sind, d.h. beispielsweise, dass wir anstelle von $0.19999\dots$ schreiben $0.2000\dots$. Dadurch haben wir sichergestellt, dass die Darstellung als Dezimalbruch eindeutig ist.

Es sei r die Zahl mit der Dezimaldarstellung $r = 0.s_1s_2s_3s_4s_5\dots$, wobei gelte:

$$s_i = \begin{cases} s_{ii} - 1 & \text{, falls } s_{ii} \geq 1 \\ 1 & \text{, falls } s_{ii} = 0 \end{cases}$$

Es gilt $r \in I$, aber r kommt unter den Zahlen r_1, r_2, ... nicht vor, da sich r und r_i an der i-ten Stelle unterscheiden ($i = 1, 2, \dots$). Dies ist ein Widerspruch und Satz 2 ist somit bewiesen. □

Bemerkung. Man nennt die Beweismethode von Satz 2 auch *zweites Cantorsches Diagonalverfahren.*

Eine Menge, die nicht abzählbar ist, nennt man auch *überabzählbar*. Zusammenfassend können wir also feststellen: *Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar, während die Menge $\mathbb{R}$ der reellen Zahlen überabzählbar ist.*

3 Relationen

3.1 Eigenschaften von Relationen

Im Abschnitt 1.2 haben wir die Menge $M^2 = M \times M = \big\{(a,b) : a,b \in M\big\}$ aller geordneten Paare von Elementen aus M kennengelernt. Allgemeiner definieren wir jetzt für Mengen A und B:

$$A \times B := \Big\{(a,b) : a \in A,\ b \in B\Big\}.$$

$A \times B$ ist also die Menge aller *geordneten Paare* $\big(a,b\big)$ mit $a \in A$ und $b \in B$. Man nennt $A \times B$ das *kartesische Produkt* von A und B.

Beispiel. $A = \big\{1,2,3\big\}$ und $B = \big\{0,1\big\}$.

Dann ist $A \times B = \Big\{(1,0),\ (1,1),\ (2,0),\ (2,1),\ (3,0),\ (3,1)\Big\}$.

Definition.
Unter einer *Relation von A nach B* versteht man eine Teilmenge R von $A \times B$.

Mit anderen Worten: Jede Teilmenge $R \subseteq A \times B$ wird eine Relation von A nach B genannt; genauer spricht man hier von einer binären Relation. Ist $A = B$, so spricht man von einer *Relation auf A*.

Beispiel. $A = \big\{1,2,3\big\}$ und $B = \big\{0,1\big\}$. Einige Relationen von A nach B sind beispielsweise:

1. $R_1 = \Big\{(1,0),\ (1,1),\ (2,1),\ (3,0)\Big\}$

2. $R_2 = \Big\{(1,1),\ (2,0),\ (3,1)\Big\}$

3. $R_3 = A \times B$

4. $R_4 = \emptyset$

Für endliche Mengen lassen sich Relationen auf zwei Arten veranschaulichen:

- als $0,1$ - *Matrix*;
- als *bipartiter gerichteter Graph*.

Wir demonstrieren dies für die obigen Relationen R_1 und R_2:

	0	1
1	1	1
2	0	1
3	1	0

R_1 als $0,1$ - Matrix

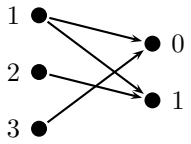
	0	1
1	0	1
2	1	0
3	0	1

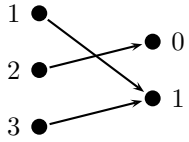
R_2 als $0,1$ - Matrix

Der Eintrag „1“ bedeutet: Das betreffende Paar ist in R.

Der Eintrag „0“ bedeutet: Das betreffende Paar ist nicht in R.

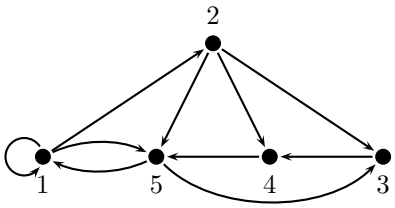
Darstellung von R_1 und R_2 als gerichteter bipartiter Graph: Jedem $(a,b) \in R$ entspricht hier ein Pfeil von a nach b.





Ist R eine Relation auf A (d.h., $R \subseteq A \times A$), so gibt es eine dritte Art der Darstellung von R, nämlich als *gerichteter Graph*. Wir führen dies für das folgende Beispiel vor:

$$\begin{aligned} A &= \Big\{1,2,3,4,5\Big\} \\ R &= \Big\{(1,1),\ (1,2),\ (1,5),\ (2,3),\ (2,4),\ (2,5),\ (3,4),\ (4,5),\ (5,1),\ (5,3)\Big\} \end{aligned}$$



Jedem Pfeil entspricht ein Paar $(a,b) \in R$. Statt „Pfeil“ sagt man auch *gerichtete Kante* oder einfach nur *Kante* des Graphen; eine Kante der Art $\circlearrowleft$ nennt man *Schlinge*.

Die Punkte 1, 2, 3, 4 und 5 nennt man *Knoten* des Graphen.

In den Abschnitten 3.1 und 3.3 sagen wir der Einfachheit halber statt „gerichteter Graph“ nur „Graph“. In späteren Abschnitten werden wir genauer sein und immer zwischen den Begriffen „Graph“ und „gerichteter Graph“ unterscheiden: „Graph“ wird dann immer „ungerichteter Graph“ bedeuten.

Definition.
R sei eine Relation auf A (d.h., $R \subseteq A \times A$). Man nennt R

(1) *reflexiv*, falls $(a,a) \in R$ für alle $a \in A$ gilt;

(2) *irreflexiv*, falls $(a,a) \notin R$ für alle $a \in A$ gilt;

(3) *symmetrisch*, falls aus $(a,b) \in R$ stets $(b,a) \in R$ folgt;

(4) *antisymmetrisch*, falls aus $(a,b) \in R$, $a \neq b$, stets $(b,a) \notin R$ folgt;

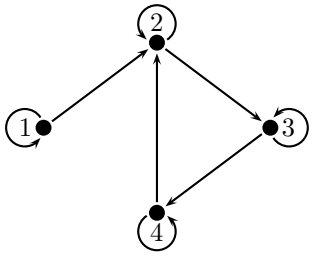
(5) *transitiv*, falls aus $(a,b) \in R$ und $(b,c) \in R$ stets $(a,c) \in R$ folgt.

Wir wollen uns diese Begriffe an der Darstellung von R als $0,1$ - Matrix und als Graph veranschaulichen, und zwar für $A = \big\{1,2,3,4\big\}$:

1. Reflexivität

R ist reflexiv bedeutet: In der Matrix stehen in der *Hauptdiagonalen*[1] lauter Einsen; im Graphen hat jeder Knoten eine Schlinge.

1	1	0	0
0	1	1	0
0	0	1	1
0	1	0	1

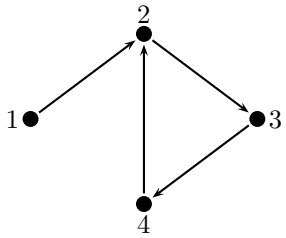


[1]So bezeichnet man die Diagonale einer quadratischen Matrix, die von links oben nach rechts unten verläuft.

2. Irreflexivität

R ist irreflexiv bedeutet: In der Hauptdiagonalen stehen lauter Nullen; der Graph ist schlingenlos.

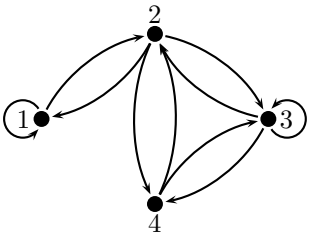
0	1	0	0
0	0	1	0
0	0	0	1
0	1	0	0



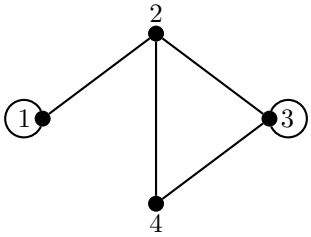
3. Symmetrie

R ist symmetrisch bedeutet: Steht in der Matrix an der Stelle (i, j) (d.h. am Schnittpunkt der i-ten Zeile und der j-ten Spalte) eine Eins, so steht auch an der Stelle (j, i) eine Eins. Mit anderen Worten: Die Matrix ist „spiegelsymmetrisch zur Hauptdiagonalen“. Für den Graphen bedeutet „symmetrisch“: Geht eine Kante von a nach b, so geht auch eine Kante von b nach a:

1	1	0	0
1	0	1	1
0	1	1	1
0	1	1	0



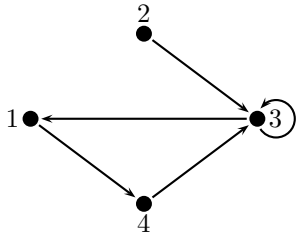
Symmetrische Graphen stellt man gewöhnlich durch „Kanten ohne Pfeile“ dar; man spricht hier von „ungerichteten Kanten“ oder auch einfach wieder nur von „Kanten“.



4. Antisymmetrie

R ist antisymmetrisch bedeutet: Steht in der Matrix an der Stelle (i, j) eine Eins und ist $i \neq j$, so steht an der Stelle (j, i) eine Null. Im Graphen: Führt eine Kante von i nach j und ist $i \neq j$, so führt keine Kante zurück von j nach i:

0	0	0	1
0	0	1	0
1	0	1	0
0	0	1	0



5. Transitivität

Dies wollen wir nur anhand des Graphen veranschaulichen; R ist transitiv bedeutet hier: Wenn eine Kante von a nach b und eine Kante von b nach c geht, dann geht immer auch eine Kante von a nach c. Dabei müssen a, b und c nicht notwendigerweise verschieden sein.

Veranschaulichung im Graphen:

Man beachte:

- „Nicht reflexiv“ ist nicht dasselbe wie irreflexiv; „nicht reflexiv“ bedeutet, dass „mindestens eine Schlinge fehlt“. Irreflexiv bedeutet, dass „sämtliche Schlingen fehlen“.

Aus ähnlichen Gründen gilt:

- „Nicht symmetrisch“ ist nicht dasselbe wie antisymmetrisch. (Wieso nämlich nicht?)

Noch eine Bemerkung zur Schreib- und Sprechweise, die wir an einem **Beispiel** erläutern: Es sei

$$A = \Big\{1, 2, 3, \ldots, 50\Big\}$$

und R sei die folgende Relation auf A:

$$R = \Big\{(a, b) : a \text{ und } b \text{ haben dieselbe Quersumme}\Big\} .$$

Beispielsweise gilt $(13, 31), (27, 9), (48, 39) \in R$. Zur Abkürzung wollen wir hierfür $13 \sim 31$, $27 \sim 9$ bzw. $48 \sim 39$ schreiben. Anstelle von $(a, b) \in R$ schreiben wir immer $a \sim b$. Es ist nun üblich, nicht mehr streng zwischen der Relation R und dem Zeichen $\sim$ zu unterscheiden und beispielsweise von der „der Relation $\sim$“ zu sprechen.

Ein **Beispiel** hierfür: Man spricht von der Relation $\leq$ auf $\mathbb{N}$, anstatt (was wesentlich umständlicher wäre) zunächst zu definieren $R = \big\{(n, m) : n, m \in \mathbb{N}, n \leq m\big\}$ und dann von der Relation R zu sprechen.

3.2 Partitionen und Äquivalenzrelationen

Definition.
Eine Relation R auf einer Menge M heißt *Äquivalenzrelation*, wenn R reflexiv, symmetrisch und transitiv ist.

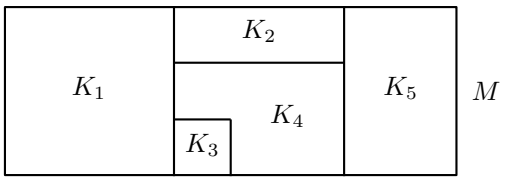
Beispiele für Äquivalenzrelationen erhält man, wenn man Partitionen (Klasseneinteilungen) einer Menge M betrachtet. Man definiert den Begriff der Partition wie folgt.

Definition.
M sei eine Menge, die Mengen K_i $(i \in I)$ seien nichtleere Teilmengen von M. Es gelte:

(a) $K_i \cap K_j = \emptyset$ für alle $i, j \in I$ mit $i \neq j$.

(b) $\bigcup\limits_{i \in I} K_i = M$.

Dann nennt man $P = \big\{K_i : i \in I\big\}$ eine *Partition* (oder *Klasseneinteilung*) von M. Die Mengen K_i heißen *Klassen* der *Partition* P.



Zu einer gegebenen Partition P von M lässt sich immer eine zugehörige Relation R auf M bilden, indem man definiert:

$$R := \Big\{(x,y) : \text{Es gibt ein } i \in I \text{ mit } x,y \in K_i\Big\}.$$

Mit anderen Worten:

- $(x,y) \in R$, falls x und y in derselben Klasse liegen;
- $(x,y) \notin R$, falls x und y in verschiedenen Klassen liegen.

Man überzeugt sich sofort, dass diese Relation R eine Äquivalenzrelation ist:

(1) R ist reflexiv.

(2) R ist symmetrisch.

(3) R ist transitiv.

Wir haben gesehen: Zu jeder Partition P von M gehört auf die beschriebene Weise eine Äquivalenzrelation R auf M; wir nennen diese Äquivalenzrelation R die *durch die Partition P erzeugte Äquivalenzrelation*.

Damit haben wir eine Vielzahl von Beispielen für Äquivalenzrelationen erhalten: Man braucht sich nur irgendeine Partition P einer Menge M herzunehmen, schon hat man „automatisch“ auch eine Äquivalenzrelation erhalten, nämlich die durch P erzeugte Äquivalenzrelation. Wir fragen uns nun: *Haben wir damit bereits alle Äquivalenzrelationen erfasst oder gibt es noch andere Äquivalenzrelationen, die nicht von einer Partition erzeugt werden?* Wir zeigen, dass letzteres nicht der Fall ist.

Satz.
Sei R eine Äquivalenzrelation auf einer nichtleeren Menge M. Dann gibt es immer eine Partition P von M, so dass R durch P erzeugt wird.

Beweis. Es sei R eine Äquivalenzrelation auf $M \neq \emptyset$. Anstelle von $(a,b) \in R$ wollen wir im Folgenden $a \sim b$ schreiben; die drei Bedingungen, die R laut Annahme erfüllt, schreiben sich dann so:

$$\begin{aligned} \text{Reflexivität}: &\quad a \sim a \text{ gilt für alle } a \in M. && (3.1)\\ \text{Symmetrie}: &\quad \text{Aus } a \sim b \text{ folgt immer } b \sim a. && (3.2)\\ \text{Transitivität}: &\quad \text{Aus } a \sim b \text{ und } b \sim c \text{ folgt immer } a \sim c. && (3.3) \end{aligned}$$

Zu finden ist eine Partition P von M, so dass gilt: R wird durch P erzeugt. Zu diesem Zweck definieren wir zu jedem $a \in M$ eine Teilmenge T_a von M durch

$$T_a := \Big\{x \in M : a \sim x\Big\}.$$

Aus (3.1) folgt dann zunächst einmal $a \in T_a$ für alle $a \in M$. Wir behaupten:

$$\text{Für je zwei Mengen } T_a \text{ und } T_b \text{ gilt entweder } T_a \cap T_b = \emptyset \text{ oder } T_a = T_b. \qquad (3.4)$$

Nachweis von (3.4): Es seien T_a und T_b gegeben. Falls $T_a \cap T_b = \emptyset$ gilt, so ist (3.4) für diese Mengen T_a und T_b erfüllt. Wir können also voraussetzen, dass $T_a \cap T_b \neq \emptyset$ gilt. Wir müssen zeigen, dass in diesem Fall $T_a = T_b$ gilt.

Wegen $T_a \cap T_b \neq \emptyset$ können wir ein $c \in T_a \cap T_b$ wählen. Es gilt also $a \sim c$ und $b \sim c$, woraus man mittels (3.2) und (3.3) $a \sim b$ und $b \sim a$ erhält.

Zum Nachweis von $T_a = T_b$ haben wir zwei Dinge zu zeigen:

1. $\underline{T_a \subseteq T_b}$
   Sei $x \in T_a$. Dann gilt $a \sim x$. Aus $b \sim a$ und $a \sim x$ folgt $b \sim x$ (vgl. (3.3)). Es folgt $x \in T_b$, womit $T_a \subseteq T_b$ gezeigt ist.
2. $\underline{T_b \subseteq T_a}$
   Dies funktioniert analog zu $T_a \subseteq T_b$. Es werden lediglich die Rollen von a und b vertauscht.

Damit ist $T_a = T_b$ gezeigt und folglich (3.4) bewiesen.

(3.4) besagt, dass die Mengen T_a paarweise disjunkt sind. Wegen $a \in T_a$ gilt außerdem, dass die Mengen T_a nichtleer sind und dass die Vereinigung aller Mengen T_a gleich M ist. Also gilt:

$$\text{Die verschiedenen unter den Mengen } T_a \text{ bilden eine Partition } P \text{ von } M. \tag{3.5}$$

Ferner gilt für alle $x, y \in M$:

$$x \text{ und } y \text{ liegen genau dann in einer gemeinsamen Menge } T_a, \text{ wenn } x \sim y \text{ gilt.} \tag{3.6}$$

Nachweis von (3.6):

(1) $\underline{x, y \in T_a \Rightarrow x \sim y}$

Es gelte $x, y \in T_a$. Dann folgt $a \sim x$ und $a \sim y$, woraus man mittels (3.2) und (3.3) $x \sim y$ erhält.

(2) $\underline{x, y \in T_a \Leftarrow x \sim y}$

Es gelte $x \sim y$. Dann folgt $y \in T_x$. Ferner gilt $x \in T_x$. Für $a = x$ gilt also $x, y \in T_a$.

Damit ist (3.6) gezeigt.

Da (3.6) bedeutet, dass R durch die Partition P erzeugt wird, ist der Satz bewiesen. □

Zusammenfassend ergibt sich die folgende Feststellung.

Feststellung.
Jede Partition erzeugt eine Äquivalenzrelation; umgekehrt wird jede Äquivalenzrelation durch eine Partition erzeugt.

Definition und Bezeichnung.
Es sei $\sim$ eine Äquivalenzrelation auf M und P sei die zugehörige Partition von M (d.h., P erzeugt $\sim$). Die Teilmengen K von M, für die $K \in P$ gilt, nennt man die *Äquivalenzklassen von* $\sim$. Für $x \in M$ bezeichnet man diejenige Äquivalenzklasse von $\sim$, die x enthält, meist mit $[x]$.

Beispiel. Es sei $M = \mathbb{Z}$. Auf $\mathbb{Z}$ betrachten wir die Relation der Kongruenz $\equiv$ modulo m. Diese lässt sich auch als die folgende Menge R schreiben:

$$R = \Big\{(a, b) : a, b \in \mathbb{Z},\ a \equiv b \pmod{m}\Big\}.$$

Dies ist eine Äquivalenzrelation (siehe dazu Regeln 1 - 3 für das Rechnen mit Kongruenzen, Seite 27). Die zugehörige Partition haben wir bereits in (2.10) bestimmt: Sie besteht aus den m Klassen $\mathcal{K}_0$, $\mathcal{K}_1$, …, $\mathcal{K}_{m-1}$, den sogenannten *Restklassen modulo* m. Es gilt:

$$\mathcal{K}_r = \Big\{a \in \mathbb{Z} : a = q \cdot m + r \text{ für ein } q \in \mathbb{Z}\Big\} \qquad (0 \le r \le m-1).$$

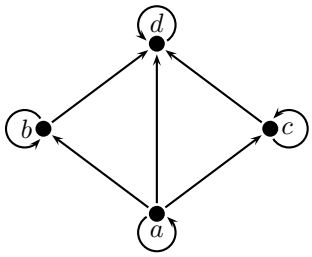
3.3 Ordnungsrelationen

Definition.
Eine Relation R auf einer Menge A heißt *Ordnungsrelation*, falls R reflexiv, antisymmetrisch und transitiv ist.

Beispiele:

1. Es seien $A = \Big\{a, b, c, d\Big\}$ und $R = \Big\{(a, b),\ (a, c),\ (a, d),\ (b, d),\ (c, d),\ (a, a),\ (b, b),\ (c, c),\ (d, d)\Big\}$.

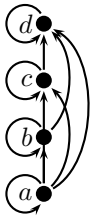
Der Graph dieser Relation:



An diesem Graph erkennt man, dass es sich um eine Ordnungsrelation handelt, da die Bedingungen „reflexiv“, „antisymmetrisch“ und „transitiv“ erfüllt sind. (Man mache sich dies anhand dessen klar, was in Abschnitt 3.1 über die anschauliche Bedeutung von „reflexiv“, „antisymmetrisch“ und „transitiv“ gesagt wurde.)

2. Es seien $A = \Big\{a, b, c, d\Big\}$ und $R = \Big\{(a,b),\ (a,c),\ (a,d),\ (b,c),\ (b,d),\ (c,d),\ (a,a),\ (b,b),\ (c,c),\ (d,d)\Big\}$.

Der Graph dieser Relation:



Ebenso wie für Beispiel 1 prüft man leicht nach, dass es sich auch hier um eine Ordnungsrelation handelt.

Ist R eine Ordnungsrelation, so schreibt man anstelle von $(a,b) \in R$ meistens $a \leq b$.

Achtung: Hierbei handelt es sich im Allgemeinen nicht um die bekannte „Kleiner-Gleich-Relation“ für Zahlen; es wird lediglich dasselbe Symbol $\leq$ benutzt.

Im ersten Beispiel kann man die Ordnungsrelation R also auch wie folgt beschreiben:

$$a \leq b, \quad a \leq c, \quad a \leq d, \quad b \leq d, \quad c \leq d, \quad a \leq a, \quad b \leq b, \quad c \leq c \quad \text{und} \quad d \leq d.$$

Die drei Bedingungen „reflexiv“, „antisymmetrisch“ und „transitiv“ lassen sich mit dem Zeichen $\leq$ dann so schreiben:

Reflexivität :	$a \leq a$ gilt für alle $a \in M$.	(3.7)
Antisymmetrie :	Gilt $a \leq b$ für verschiedene a und b, so gilt nicht $b \leq a$.	(3.8)
Transitivität :	Aus $a \leq b$ und $b \leq c$ folgt immer $a \leq c$.	(3.9)

Definition.

Eine Ordnungsrelation $\leq$ auf A heißt *totale Ordnung* von A, falls neben (3.7), (3.8) und (3.9) die folgende Bedingung (3.10) erfüllt ist:

Vollständigkeit :	Für alle Elemente $a, b \in A$ mit $a \neq b$ gilt stets $a \leq b$ oder $b \leq a$.	(3.10)

Beim zweiten obigen Beispiel handelt es sich um eine totale Ordnung, beim ersten nicht.

Bemerkungen zur Terminologie:

- Statt „Ordnungsrelation“ sagt man auch *partielle Ordnung* und spricht von einer *partiell geordneten Menge* A; eine andere Bezeichnung für „Ordnungsrelation“ bzw. „partielle Ordnung“, die man gelegentlich antrifft, ist *Halbordnung*.
- Anstelle von „totale Ordnung“ sagt man auch *vollständige Ordnung*, *Kette* oder *lineare Ordnung*.

Weitere Beispiele:

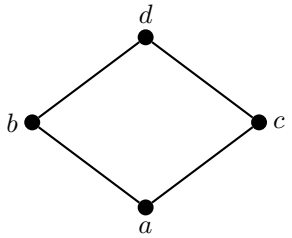
3. Es sei M eine Menge und $A = \mathcal{P}(M)$ sei die Potenzmenge dieser Menge M. Die Relation $\subseteq$ ist eine Ordnungsrelation auf A.

4. Die Teilbarkeitsrelation | ist eine Ordnungsrelation auf $\mathbb{N}$. (Zur Erinnerung: Für $a, b \in \mathbb{N}$ gilt $a \mid b$, falls es ein $c \in \mathbb{N}$ mit $b = a \cdot c$ gibt.)

5. Die gewöhnliche $\leq$ - Relation auf $\mathbb{N}$ ist eine Ordnungsrelation. (Sie ist sogar eine totale Ordnung.) Entsprechendes gilt für $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$.

Zur Übung überlege man sich, warum es sich bei den Beispielen 3 und 4 tatsächlich um Ordnungsrelationen handelt und begründe, dass dies im Allgemeinen keine totalen Ordnungen sind. Ist die Teilbarkeitsrelation auch eine Ordnungsrelation auf $\mathbb{Z}$?

Abschließend kommen wir noch einmal auf die Beispiele 1 und 2 zurück. Um diese Ordnungsrelationen graphisch darzustellen, hätte es genügt, die folgenden Diagramme zu zeichnen:



Wenn man weiß, dass es sich bei den betrachteten Relationen um Ordnungsrelationen handelt, kann man „ohne Informationsverlust“ zu diesen einfacheren Diagrammen übergehen. Die neuen einfacheren Diagramme sind aus den ursprünglichen dadurch entstanden, dass

- die Schlingen weggelassen wurden;
- alle Kanten weggelassen wurden, die sich „automatisch“ aufgrund der Transitivität ergeben (wie beispielsweise die Kante von a nach d im ersten Beispiel bzw. die Kanten von a nach c, von a nach d sowie von b nach d im zweiten Beispiel);
- die Richtungspfeile durch die Konvention ersetzt wurden, dass Kanten immer von unten nach oben gerichtet sind.

Auf diese Art entstandene Diagramme von Ordnungsrelationen werden in der Literatur auch als *Hasse-Diagramme* bezeichnet.

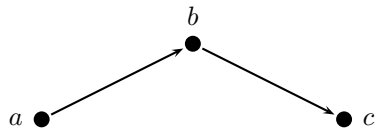
3.4 Hüllenbildungen

Es sei R eine Relation auf einer Menge A, d.h. $R \subseteq A \times A$. Ist R nicht bereits reflexiv, so kann man aus R eine reflexive Relation R' gewinnen, indem man alle nicht in R vorkommenden Paare (a, a) zu R hinzunimmt (für $a \in A$); man definiert dementsprechend

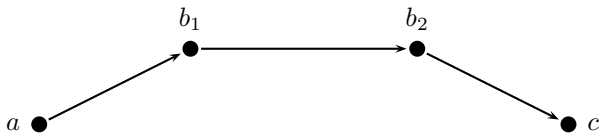
$$R' := R \cup \Big\{ (a, a) : a \in A \Big\}$$

und nennt R' die *reflexive Hülle* von R. (Falls R bereits reflexiv ist, gilt also $R' = R$.) Man beachte: Die Definition ist so abgefasst, dass R' die kleinste reflexive Relation ist, die R umfasst.

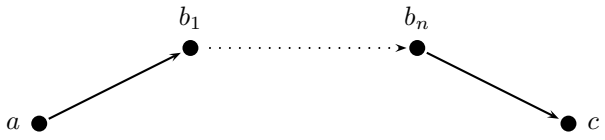
Entsprechend geht man bei der Definition der *transitiven Hülle* von R vor: Falls R nicht bereits transitiv ist, nimmt man zu R Paare $(a, c) \in A \times A$ derart hinzu, dass eine transitive Relation entsteht. Dabei beschränkt man sich allerdings (wie im Fall der reflexiven Hülle) auf diejenigen Paare, deren Hinzunahme unbedingt nötig ist: Gilt beispielsweise $(a, c) \notin R$ und gibt es ein $b \in A$ mit $(a, b), (b, c) \in R$, so ist die Hinzunahme von (a, c) zu R unbedingt nötig.



Ähnlich: Gilt $(a, c) \notin R$ und gibt es $b_1, b_2 \in A$ mit $(a, b_1), (b_1, b_2), (b_2, c) \in R$, so ist die Hinzunahme von (a, c) zu R ebenfalls unbedingt nötig.



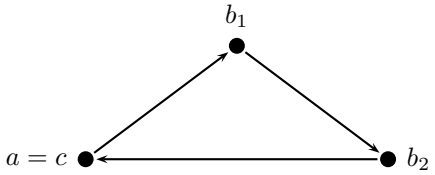
Allgemein: Es gelte $(a, c) \notin R$ und es gebe für ein $n \in \mathbb{N}$ Elemente $b_1, \ldots, b_n \in A$ mit $(a, b_1), (b_n, c) \in R$ sowie $(b_i, b_{i+1}) \in R$ $(i = 1, \ldots, n-1)$. Dann ist die Hinzunahme von (a, c) zu R unbedingt nötig, um eine transitive Relation entstehen zu lassen.



Man definiert die *transitive Hülle* R^+ einer Relation R auf A durch:

$R^+ := R \cup \{(a, c)$: Es gibt ein $n \in \mathbb{N}$ sowie $b_1, \ldots, b_n \in A$ mit $(a, b_1), (b_n, c) \in R$ und $(b_i, b_{i+1}) \in R$ $(i = 1, \ldots, n-1)\}$.

Die so definierte Relation R^+ ist dann tatsächlich transitiv (, wie man sich unschwer überlegen kann). Man beachte ferner, dass obige Definition als *Sonderfall*, den Fall umfasst, dass $a = c$ gilt: Gilt also beispielsweise $(a, b_1), (b_1, b_2), (b_2, a) \in R$, so folgt $(a, a) \in R^+$ (und im übrigen auch $(b_1, b_1), (b_2, b_2) \in R^+$).



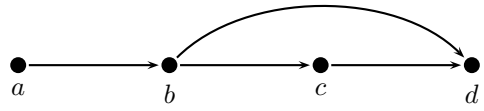
Die *reflexive, transitive Hülle* R^* von R wird definiert durch $R^* := R^+ \cup \{(a, a) : a \in A\}$.

Anstelle von „transitive Hülle“ sagt man auch *transitiver Abschluss*. (Entsprechend benutzt man auch die Begriffe *reflexiver Abschluss* bzw. *reflexiver, transitiver Abschluss*).

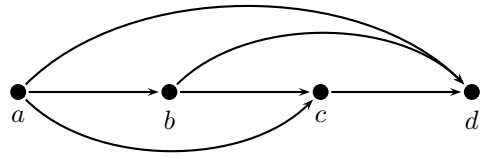
Beispiele:

1. Es seien $A = \{a, b, c, d\}$ und $R = \{(a, b), (b, c), (c, d), (b, d)\}$. Es folgt $R^+ = R \cup \{(a, c), (a, d)\}$ und $R^* = R^+ \cup \{(a, a), (b, b), (c, c), (d, d)\}$.

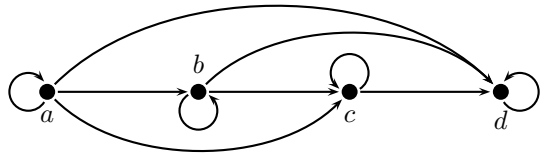
R :



R^+ :



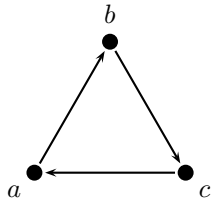
R^* :



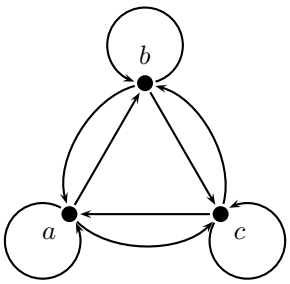
2. Es seien $A = \{a, b, c\}$ und $R = \{(a, b), (b, c), (c, a)\}$. Es folgt $(a, c) \in R^+$, da $(a, b), (b, c) \in R$. Analog findet man $(c, b) \in R^+$ und $(b, a) \in R^+$. Ferner gilt $(a, a) \in R^+$, da $(a, b), (b, c), (c, a) \in R^+$. Entsprechend findet man $(b, b) \in R^+$ und $(c, c) \in R^+$. Also gilt

$$R^+ = A \times A \qquad \text{sowie} \qquad R^* = A \times A.$$

R :



$R^+ = R^* = A \times A$:

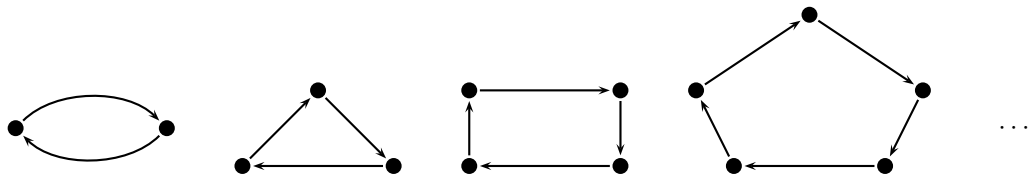


Die reflexive, transitive Hülle R^* einer Relation $R \subseteq A \times A$ ist eine reflexive, transitive Relation auf A. Da Relationen mit diesen beiden Eigenschaften recht häufig auftreten, hat man ihnen einen eigenen Namen gegeben: Man nennt eine Relation eine *Quasiordnung*, wenn sie reflexiv und transitiv ist.

Die reflexive, transitive Hülle R^* einer Relation $R \subseteq A \times A$ *braucht aber nicht antisymmetrisch zu sein*, selbst dann nicht, wenn R antisymmetrisch ist (wie das obige Beispiel 2 zeigt). Mit anderen Worten:

Die reflexive, transitive Hülle R^* einer beliebigen Relation R ist immer eine Quasiordnung, aber nicht notwendigerweise eine partielle Ordnung.

Unter bestimmten Umständen kann man sich allerdings sicher sein, dass R^* doch eine partielle Ordnung und nicht nur eine Quasiordnung ist: Es liege der Fall vor, dass R keine „zyklischen Strukturen“ der folgenden Art enthält:



Dann lässt sich unschwer einsehen (Übungsaufgabe!), dass R^* antisymmetrisch (und somit eine partielle Ordnung) ist.

In der Graphentheorie nennt man zyklische Strukturen der obigen Art „gerichtete Kreise der Länge ≥ 2“. Wir können unser Ergebnis also auch so aussprechen:

Enthält der zu R gehörige gerichtete Graph keine gerichteten Kreise der Länge ≥ 2, so ist der reflexive, transitive Abschluss R^* von R eine partielle Ordnung.

3.5 Grundlegendes über Abbildungen (Fortsetzung)

Einiges Grundlegendes über Funktionen haben wir bereits im Abschnitt 1.2 behandelt. Dies soll nun um einige neue Inhalte ergänzt werden.

Im Folgenden sei $f : A \to B$ eine Funktion, A', A_1 und A_2 seien Teilmengen von A und B', B_1 und B_2 seien Teilmengen von B.

Definition.
Unter dem *Bild von* A' unter f versteht man die folgende Menge:

$$f\big(A'\big) := \Big\{b \in B : \text{ Es gibt ein } a \in A' \text{ mit } f(a) = b\Big\}.$$

Definition.
Unter dem *Urbild von* B' bezüglich f versteht man die folgende Menge:

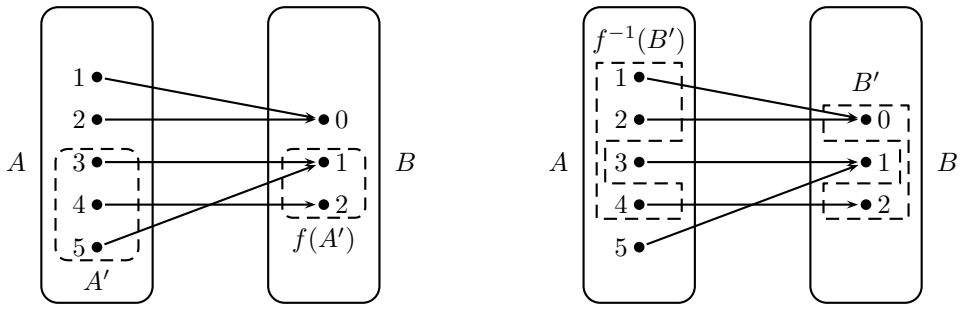
$$f^{-1}\big(B'\big) := \Big\{a \in A : \text{ Es gibt ein } b \in B' \text{ mit } f(a) = b\Big\}.$$

Beispiel. Es sei $A = \big\{1, 2, 3, 4, 5\big\}$ und $B = \big\{0, 1, 2\big\}$; f sei wie folgt definiert:

n	1	2	3	4	5
$f(n)$	0	0	1	2	1

Es sei $A' = \big\{3, 4, 5\big\}$ und $B' = \big\{0, 2\big\}$. Dann gilt:

$$\begin{aligned} f(A') &= \Big\{1, 2\Big\} \\ f^{-1}(B') &= \Big\{1, 2, 4\Big\} \end{aligned}$$



Für beliebige Mengen A und B sei $f : A \to B$ eine Funktion. Für alle Teilmengen $A', A_1, A_2 \subseteq A$ und $B', B_1, B_2 \subseteq B$ gelten die folgenden Beziehungen:

(1) $f\big(A_1 \cap A_2\big) \subseteq f\big(A_1\big) \cap f\big(A_2\big)$

(2) $f\big(A_1 \cup A_2\big) = f\big(A_1\big) \cup f\big(A_2\big)$

(3) $f^{-1}\big(B_1 \cap B_2\big) = f^{-1}\big(B_1\big) \cap f^{-1}\big(B_2\big)$

(4) $f^{-1}\big(B_1 \cup B_2\big) = f^{-1}\big(B_1\big) \cup f^{-1}\big(B_2\big)$

(5) $f^{-1}\big(f(A')\big) \supseteq A'$

(6) $f\big(f^{-1}(B')\big) \subseteq B'$

Exemplarisch führen wir den Beweis von (1) vor; die Beweise der übrigen Beziehungen gehen ähnlich und werden zum Teil in der Vorlesung bzw. in den Übungen behandelt.

Nachweis von (1). Es ist zu zeigen, dass für jedes $b \in f(A_1 \cap A_2)$ Folgendes gilt:

$$b \in f(A_1) \cap f(A_2).$$

Dies folgt so: Es sei $b \in f(A_1 \cap A_2)$. Dann gibt es ein $a \in A_1 \cap A_2$ mit $f(a) = b$. Da insbesondere $a \in A_1$ gilt, folgt $b \in f(A_1)$; da auch $a \in A_2$ gilt, folgt $b \in f(A_2)$. Also gilt $b \in f(A_1) \cap f(A_2)$. □

Definition.
Sind $f : A \to B$ und $g : B \to C$ Funktionen, so versteht man unter der *Komposition* von f und g die Funktion $k : A \to C$, die wie folgt definiert ist:

$$k(a) = g\big(f(a)\big).$$

Statt „Komposition von f und g“ sagt man auch „*Hintereinanderausführung von f und g*“. Man bezeichnet die Komposition von f und g meistens mit $g \circ f$ (sprich: *g nach f*). Also:

$$\big(g \circ f\big)\big(a\big) = g\big(f(a)\big).$$

Beispiel. Es seien $A = \big\{1, 2, 3\big\}$, $B = \big\{2, 3, 4, 5\big\}$ und $C = \big\{0, 1\big\}$. Die Funktionen f und g seien durch die folgenden Tabellen definiert:

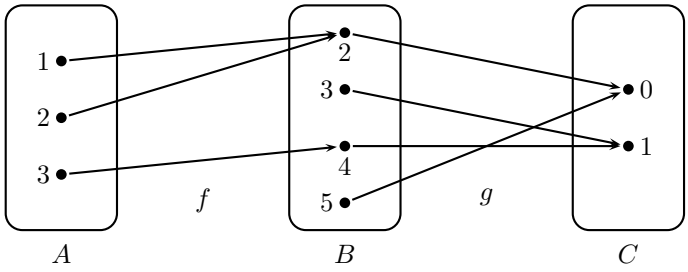
a	1	2	3
$f(a)$	2	2	4

b	2	3	4	5
$g(b)$	0	1	1	0

Dann ist die Funktion $g \circ f : A \to C$ durch die folgende Tabelle gegeben:

a	1	2	3
$(g \circ f)(a)$	0	0	1

Besonders anschaulich wird der Begriff der Komposition durch die Betrachtung der bipartiten gerichteten Graphen:



Um anhand der Zeichnung festzustellen, worauf ein bestimmtes Element $a \in A$ durch $g \circ f$ abgebildet wird, braucht man nur den Pfeilen zu folgen: zunächst dem Pfeil, der von a ausgeht und anschließend dem Pfeil, der von $f(a)$ ausgeht.

Für die Hintereinanderausführung von Funktionen gilt das *Assoziativgesetz*[2]: Es seien $f : A \to B$, $g : B \to C$ und $h : C \to D$ Funktionen. Dann gilt:

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Aus diesem Grund kann man hier die Klammern weglassen und einfach $h \circ g \circ f$ schreiben.

Zwei weitere wichtige Begriffe im Zusammenhang mit Funktionen sind der Begriff der *Restriktion* und der Begriff der *Umkehrfunktion*.

Definition.

Ist $f : A \to B$ eine Funktion und gilt $A' \subseteq A$, so versteht man unter der *Restriktion* (oder *Einschränkung*) von f auf A' die Funktion $r : A' \to B$, die durch $r(a) = f(a)$ (für $a \in A'$) definiert wird. Statt r schreibt man meistens $f\,|_{A'}$.

Für alle $a \in A'$ gilt:

$$\big(f\,|_{A'}\big)(a) = f(a)\ .$$

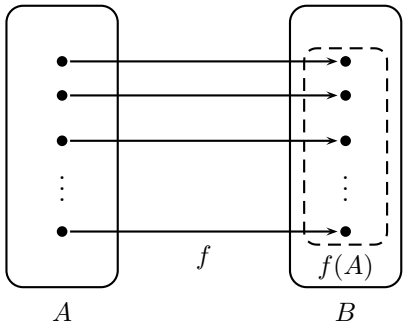
Definition.

Ist $f : A \to B$ eine *injektive* Funktion, so lässt sich zu f eine Funktion $u : f(A) \to A$ dadurch definieren, dass man festlegt: Für $b \in f(A)$ gelte $u(b) = a$ genau dann, wenn $f(a) = b$ gilt. Man nennt u die *Umkehrfunktion* von f. Statt u schreibt man f^{-1} für die Umkehrfunktion von f.

Für alle $b \in f(A)$ gilt:

$$f^{-1}(b) = a \quad \Leftrightarrow \quad f(a) = b.$$

Veranschaulichung der Umkehrfunktion:



Man erhält die Umkehrfunktion f^{-1}, indem man die Richtung der Pfeile umkehrt.

[2]Man mache sich dies mit Hilfe von bipartiten gerichteten Graphen klar.

4 Graphen

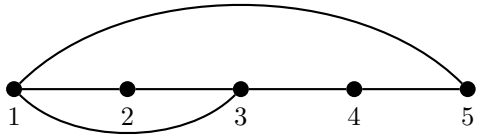
In vielen Bereichen der Informatik treten Strukturen auf, die mit Hilfe von Graphen dargestellt werden. In diesem Abschnitt sollen die wichtigsten Grundbegriffe der Graphentheorie vorgestellt werden.

4.1 Grundlegende Definitionen

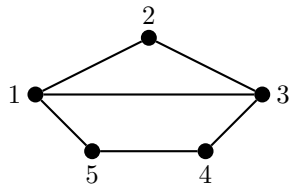
Ein *ungerichteter Graph* G ist ein Paar (V, E), wobei V eine beliebige endliche Menge ist; E ist eine Menge von zweielementigen Teilmengen von V. Die Elemente von V nennt man die *Knoten* von G, die Elemente von E nennt man die *Kanten* von G.

Graphen lassen sich durch Punkte und Linien veranschaulichen: Man zeichnet die Knoten als Punkte in die Ebene und stellt die Kanten als Verbindungslinien dar.

Beispiel 1. $G = (V, E)$ mit $V = \Big\{1, 2, 3, 4, 5\Big\}$ und $E = \Big\{\big\{1, 2\big\},\ \big\{1, 3\big\},\ \big\{1, 5\big\},\ \big\{2, 3\big\},\ \big\{3, 4\big\},\ \big\{4, 5\big\}\Big\}$.



Eine solche Darstellung ist natürlich keineswegs eindeutig. Eine andere Darstellung desselben Graphen ist beispielsweise die folgende:



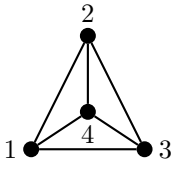
Bemerkungen zur Terminologie

(1) Anstelle von Knoten sagt man auch *Ecke* eines Graphen.

(2) Der Buchstabe V steht für das englische „vertex“ (Ecke); der Buchstabe E steht für das englische „edge“ (Kante).

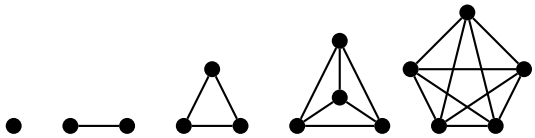
(3) Anstelle von „ungerichteter Graph“ wollen wir auch einfach nur *Graph* sagen.

Beispiel 2. $G = (V, E)$ mit $V = \Big\{1, 2, 3, 4\Big\}$ und $E = \Big\{\big\{1, 2\big\},\ \big\{1, 3\big\},\ \big\{1, 4\big\},\ \big\{2, 3\big\},\ \big\{2, 4\big\},\ \big\{3, 4\big\}\Big\}$.

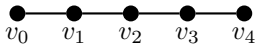


In diesem Beispiel besteht E aus allen zweielementigen Teilmengen von V, d.h., jeder Knoten ist mit jedem anderen Knoten verbunden. Graphen mit dieser Eigenschaft nennt man *vollständige Graphen*.

Vollständige Graphen mit $n = 1, \ldots, 5$ Knoten:



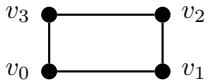
Beispiel 3. $G = (V, E)$ mit $V = \Big\{v_0, v_1, v_2, v_3, v_4\Big\}$ und $E = \Big\{\big\{v_0, v_1\big\},\ \big\{v_1, v_2\big\},\ \big\{v_2, v_3\big\},\ \big\{v_3, v_4\big\}\Big\}$.



Den Graphen aus Beispiel 3 nennt man einen Weg der Länge 4. Allgemein versteht man unter einem *Weg der Länge* n einen Graphen $G = (V, E)$ mit einer Knotenmenge $V = \Big\{v_0, \ldots, v_n\Big\}$ von genau $n + 1$ verschiedenen Knoten und der Kantenmenge $E = \Big\{\big\{v_i, v_{i+1}\big\} : i = 0, \ldots, n - 1\Big\}$ $(n \in \mathbb{N} \cup \{0\})$.

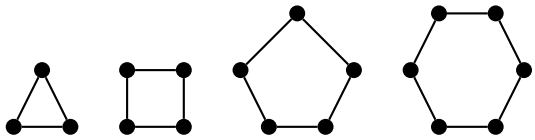
Wege der Länge n für $n = 0, \ldots, 4$:

Beispiel 4. $G = (V, E)$ mit $V = \Big\{v_0, v_1, v_2, v_3\Big\}$ und $E = \Big\{\big\{v_0, v_1\big\},\ \big\{v_1, v_2\big\},\ \big\{v_2, v_3\big\},\ \big\{v_3, v_0\big\}\Big\}$.



Den Graphen aus Beispiel 4 nennt man einen Kreis der Länge 4. Allgemein versteht man unter einem *Kreis der Länge* n $(n \geq 3)$ einen Graphen $G = (V, E)$ mit einer Knotenmenge $V = \Big\{v_0, \ldots, v_{n-1}\Big\}$ von genau n verschiedenen Knoten und der Kantenmenge $E = \Big\{\big\{v_i, v_{i+1}\big\} : i = 0, \ldots, n-2\Big\} \cup \Big\{\big\{v_0, v_{n-1}\big\}\Big\}$.

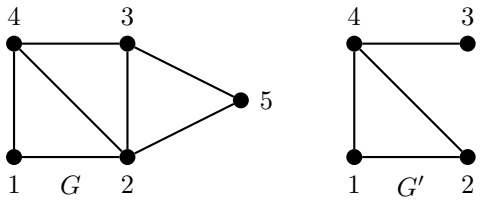
Kreise der Länge n für $n = 3, 4, 5, 6$:



Für einen Graphen $G = (V, E)$ bezeichnet man die Knotenmenge V auch mit $V(G)$ und die Kantenmenge E bezeichnet man mit $E(G)$.

Definition.
Ein Graph $G' = (V', E')$ heißt ein *Teilgraph* von $G = (V, E)$, falls $V' \subseteq V$ und $E' \subseteq E$ gilt. $G' \subseteq G$ bedeutet, dass G' ein Teilgraph von G ist.

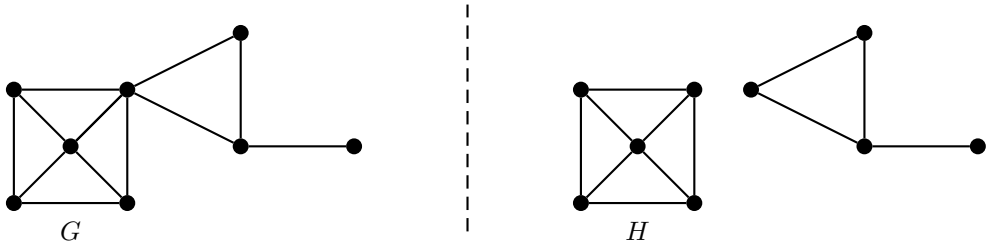
Beispiel.



Definition.

Ein Graph G heißt *zusammenhängend*, falls es in G zu je zwei Knoten v und w einen Weg gibt, der v und w verbindet.

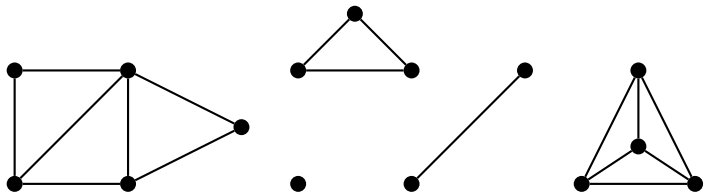
Beispiel. Ein zusammenhängender Graph G und ein nicht zusammenhängender Graph H:



Definition.

Ein Teilgraph G' von G wird *Zusammenhangskomponente* von G genannt, wenn G' zusammenhängend ist und wenn es keinen zusammenhängenden Teilgraphen H von G gibt, für den $G' \subseteq H$ und $H \neq G'$ gilt.

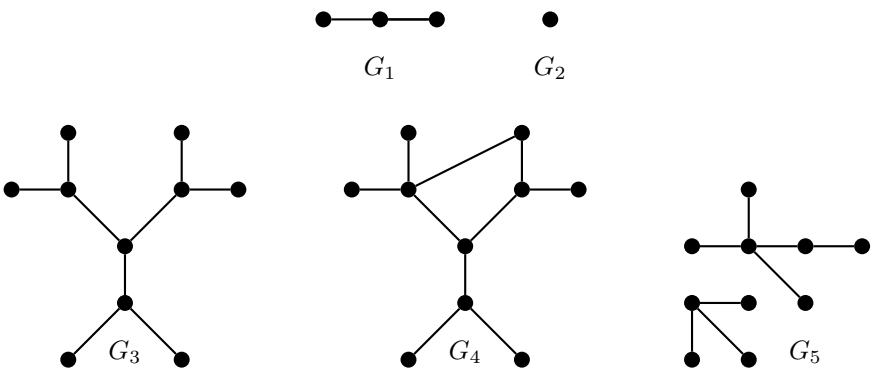
Beispiel. Ein Graph mit fünf Zusammenhangskomponenten:



Definition.

Ein Graph heißt ein *Baum*, falls er zusammenhängend ist und keinen Kreis enthält.

Beispiel. Die folgenden Graphen G_1, G_2 und G_3 sind Bäume; die Graphen G_4 und G_5 sind keine Bäume.



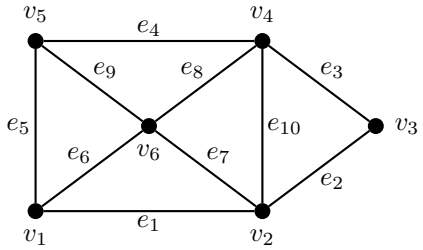
In der Informatik betrachtet man meistens Bäume mit einer *Wurzel*, d.h., für einem bestimmten Knoten ist festgelegt, dass er die Wurzel des Baumes sein soll.

Definition.

Ist G ein Graph und v ein Knoten von G, so versteht man unter dem Grad von v in G die Anzahl der Kanten von G, die an v anstoßen[1]. Den Grad von v wollen wir mit $d(v)$ bezeichnen.

[1] **Sprechweisen**: Ist $e = \{v_1, v_2\}$ eine Kante von G, so nennt man v_1 und v_2 *benachbart* oder *adjazent*. Man sagt ferner: e *stößt an* v_1 (bzw. v_2) oder e ist *inzident* mit v_1 (bzw. v_2).

Beispiel. G sei der folgende Graph mit Knotenmenge $V(G) = \{v_1, v_2, v_3, v_4, v_5, v_6\}$ und der Kantenmenge $E(G) = \{e_1, e_2, \ldots, e_{10}\}$.



In diesem Beispiel ist $d(v_1) = 3$, $d(v_2) = 4$, $d(v_3) = 2$, $d(v_4) = 4$, $d(v_5) = 3$ sowie $d(v_6) = 4$. Für die Anzahl der Kanten von $E(G)$ gilt $|E(G)| = 10$. Bilden wir die Summe

$$\sum_{i=1}^{6} d(v_i) = 3 + 4 + 2 + 4 + 3 + 4 = 20,$$

so ergibt sich genau die doppelte Kantenzahl. Das kommt daher, dass jede Kante an genau zwei Knoten stößt und daher in der Summe $\sum_{i=1}^{6} d(v_i)$ genau zweimal gezählt wird.

Der allgemeine Fall wird im folgenden Satz festgehalten.

Satz 1.
Ist G ein Graph mit der Knotenmenge $V(G) = \{v_1, \ldots, v_n\}$ und der Kantenmenge $E(G)$, so gilt

$$\sum_{i=1}^{n} d(v_i) = 2|E(G)| \tag{4.1}$$

In Worten besagt Satz 1, dass in jedem Graphen[2] die Summe der Knotengrade gleich der doppelten Kantenzahl ist.

Beweis von Satz 1. Ist e eine Kante von G, so stößt e an genau zwei Knoten, etwa an v_j und v_k ($j \neq k$). Dies bedeutet, dass e genau zweimal einen Beitrag zur Summe $\sum_{i=1}^{n} d(v_i)$ leistet, nämlich sowohl im Summanden $d(v_j)$ als auch im Summanden $d(v_k)$. Mit anderen Worten: e wird in der Summe $\sum_{i=1}^{n} d(v_i)$ genau zweimal gezählt. Also gilt (4.1). □

Als Folgerung aus Satz 1 erhält man den folgenden Satz.

Satz 2.
In einem Graphen ist die Anzahl der Knoten ungeraden Grades immer eine gerade Zahl.

Bevor wir Satz 2 beweisen, wollen wir die Richtigkeit der Aussage am letzten Beispiel überprüfen: Dort sind v_2, v_3, v_4 und v_6 die Knoten geraden Grades; v_1 und v_5 sind die Knoten ungeraden Grades. Es gibt hier also genau zwei Knoten ungeraden Grades.

Beweis von Satz 2. $G = (V, E)$ sei ein beliebiger Graph. Die Knoten von G seien mit v_1, …, v_n bezeichnet und die Bezeichnungen seien so gewählt, dass $\{v_i : 1 \leq i \leq k\}$ die Menge der Knoten ungeraden Grades und $\{v_i : k+1 \leq i \leq n\}$ die Menge der Knoten geraden Grades ist ($k \in \{0, \ldots, n\}$).

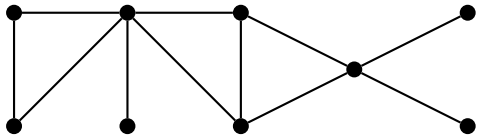
Aus Satz 1 folgt

$$\sum_{i=1}^{k} d(v_i) = 2|E| - \sum_{i=k+1}^{n} d(v_i). \tag{4.2}$$

[2] Es sei nochmals darauf hingewiesen, dass der Begriff „Graph“ hier immer in der Bedeutung von „ungerichteter Graph“ benutzt wird.

Da $2|E|$ eine gerade Zahl ist und da $d(v_i)$ für alle $i = k+1, \ldots, n$ eine gerade Zahl ist, ist wegen (4.2) die Summe $\sum_{i=1}^{k} d(v_i)$ eine gerade Zahl. Da $d(v_i)$ für alle $i = 1, \ldots, k$ eine ungerade Zahl ist, muss also die Anzahl k der Summanden gerade sein. □

Einen Knoten vom Grad 1 nennt man *Endknoten* eines Graphen. Ein Graph mit drei Endknoten:



Für Bäume gilt folgende einfache Feststellung:

Ist B ein Baum mit mindestens zwei Knoten, so hat B auch mindestens zwei Endknoten. (4.3)

Beweis. Unter allen Wegen in B betrachte man einen Weg W mit möglichst großer Länge. Der erste und der letzte Knoten von W sind dann zwei verschiedene Endknoten von B. □

Satz 3.
Es sei $B = (V, E)$ ein Baum mit genau n Knoten. Dann gilt $|E| = n - 1$.

Beweis von Satz 3 (vollständige Induktion).

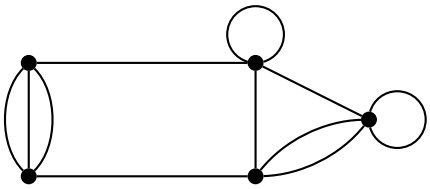
(I) *Induktionsanfang*

Es sei $n = 1$. Dann besteht B aus einem einzigen Knoten und besitzt keine Kanten. Also gilt die Behauptung für $n = 1$.

(II) *Induktionsschritt*

Wir setzen jetzt voraus, dass die Behauptung für ein festes n richtig sei. B' sei ein Baum mit $n+1$ Knoten. Nach (4.3) gibt es in B' einen Endknoten v. Lässt man v und die an v anstoßende Kante aus B' weg, so entsteht ein Baum B mit genau n Knoten. Nach Induktionsannahme hat B genau $n-1$ Kanten. Da B' eine Kante mehr als B hat, folgt: B' hat genau n Kanten. Also gilt die Behauptung auch für $n+1$. □

Oftmals betrachtet man auch Graphen der folgenden Art, d.h. Graphen, bei denen *Schlingen* oder *Mehrfachkanten* vorkommen:



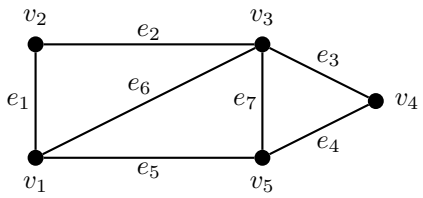
Sind Schlingen und Mehrfachkanten zugelassen, so wollen wir zur besseren Unterscheidung nicht von einem Graphen, sondern von einem *Multigraphen* sprechen. Ein Multigraph kann also (muss aber nicht!) Schlingen bzw. Mehrfachkanten enthalten. („Multigraph“ ist also der allgemeinere Begriff: Jeder Graph ist ein spezieller Multigraph, nämlich ein Multigraph ohne Schlingen und Mehrfachkanten.)

Formal kann man den Begriff des Multigraphen wie folgt definieren.

Definition.
Ein *Multigraph* G ist ein Tripel $G = (V, E, f)$, wobei V und E disjunkte Mengen sind („Knoten- und Kantenmenge“) und f eine Abbildung ist, die jedem Element aus E entweder eine zweielementige oder eine einelementige Teilmenge von V zuordnet.

Die Elemente von E, denen eine einelementige Teilmenge von V zugeordnet wird, heißen *Schlingen*; wird zwei verschiedenen Elementen von E dieselbe zweielementige Teilmenge $\{v_1, v_2\}$ von V zugeordnet, so spricht man von *Mehrfachkanten* zwischen v_1 und v_2.

Wir haben bereits zuvor den Begriff des *Weges* eingeführt. Hiervon zu unterscheiden sind die Begriffe der *Kantenfolge* und des *Kantenzugs*. Wir erläutern dies zunächst an einem Beispiel. G sei der folgende Graph:



Um in G vom Knoten v_1 zum Knoten v_4 zu gelangen, kann man beispielsweise über e_1 von v_1 nach v_2 gehen, dann über e_2 von v_2 nach v_3, dann über e_7 von v_3 nach v_5 und schließlich über e_4 von v_5 nach v_4. Dabei wurde keine Kante mehrfach durchlaufen und kein Knoten wurde mehrfach besucht. Man könnte auch (ausgehend von v_1) Kanten wie folgt durchlaufen: e_1, e_2, e_7, e_5, e_6, e_3. Dann hat man zwar lauter verschiedene Kanten benutzt, aber man hat die Knoten v_1 und v_3 mehrfach durchlaufen. Eine dritte Möglichkeit, um von v_1 nach v_4 zu gelangen: e_1, e_2, e_7, e_5, e_6, e_7, e_4. Diesmal wurde eine Kante (nämlich e_7) doppelt durchlaufen.

Diese Beispiele führen zur folgenden Definition.

Definition.

Gegeben seien ein Multigraph G mit Knotenmenge V und Kantenmenge E sowie eine Folge

$$v_0,\ e_1,\ v_1,\ e_2,\ v_2,\ \ldots,\ v_{\ell-1},\ e_\ell,\ v_\ell \quad \big(\ell \in \mathbb{N} \cup \{0\}\big) \tag{4.4}$$

mit $v_i \in V$ $(i = 0, \ldots, \ell)$ und $e_i \in E$ $(i = 1, \ldots, \ell)$.

(1) Diese Folge heißt *Kantenfolge* von v_0 nach v_ℓ, falls e_i die Knoten v_{i-1} und v_i verbindet (für $i = 1, \ldots, \ell$).

(2) Sind in dieser Kantenfolge alle Kanten e_i verschieden, so spricht man von einem *Kantenzug* von v_0 nach v_ℓ.

(3) Sind außerdem alle Knoten v_i verschieden, so spricht man von einem *Weg* von v_0 nach v_ℓ.

(4) Man nennt ℓ die *Länge* der Kantenfolge (4.4).

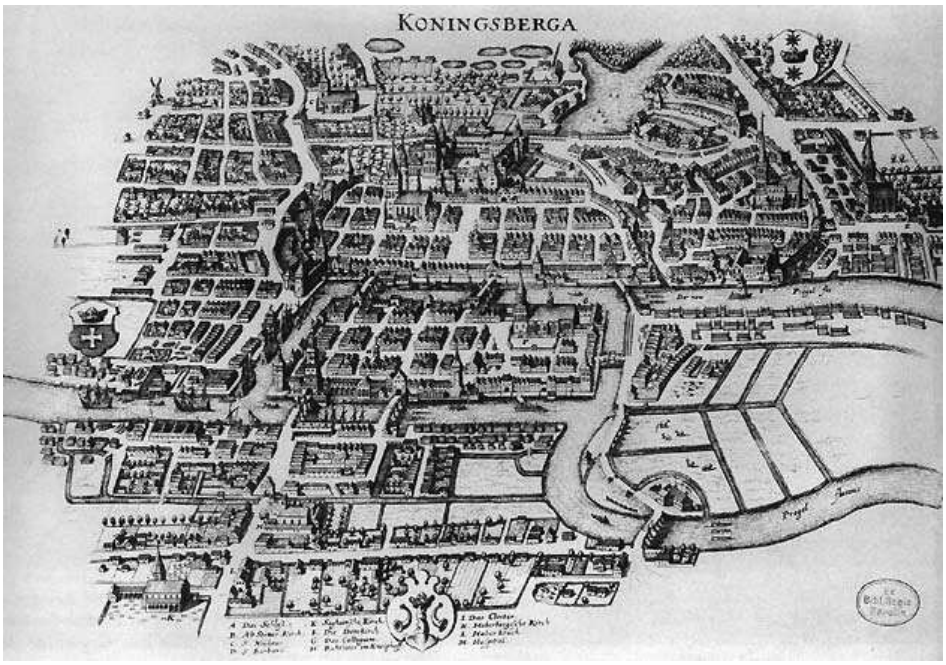
(5) Eine Kantenfolge heißt *geschlossen*, falls $v_0 = v_\ell$ gilt.

Hinweis. Die Terminologie, die in der Literatur benutzt wird, ist nicht einheitlich. Beispielsweise findet man oft die Bezeichnungen *Pfad* für Kantenfolge, *einfacher Pfad* für Kantenzug sowie *elementarer Pfad* für Weg.

In (4.4) ist auch der Fall eingeschlossen, dass $\ell = 0$ gilt. In diesem Fall besteht (4.4) nur aus dem Knoten v_0; man nennt (4.4) dann eine *triviale Kantenfolge*. Ein geschlossener, nichttrivialer Kantenzug wird auch *Zyklus* genannt.

4.2 Eulersche Linien und Hamiltonsche Kreise

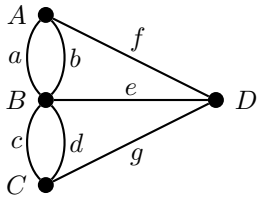
Wir beginnen mit dem sogenannten *Königsberger Brückenproblem*. Die folgende Abbildung zeigt die Stadt Königsberg im 18. Jahrhundert mit einem Fluss (der *Pregel*), vier Landstücken sowie sieben Brücken.



Eine Frage aus der damaligen Zeit: *Ist es möglich, einen Spaziergang zu machen, bei dem man jede Brücke genau einmal überquert und am Schluss wieder am Ausgangspunkt ankommt?*

Königsberger Bürger stellten diese Frage dem Mathematiker LEONHARD EULER (1707 - 1783), der sie nach kurzem Überlegen beantwortete.

In graphentheoretische Terminologie umformuliert lautet die Frage: Besitzt der folgende Multigraph einen geschlossenen Kantenzug, der alle Kanten durchläuft?



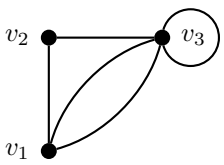
A, B, C und D seien dabei die vier Landstücke, während a, ..., g die sieben Brücken repräsentieren.

Definition.

G sei ein zusammenhängender Multigraph. Einen Kantenzug in G nennt man eine *Eulersche Linie*, falls er geschlossen ist und sämtliche Kanten von G durchläuft.

Den *Grad* $d(v)$ eines Knoten v in einem Multigraphen definiert man (wie für Graphen) als Zahl der anstoßenden Kanten, wobei Schlingen doppelt gezählt werden.

Beispiel:



In diesem Multigraphen gilt $d(v_1) = 3$, $d(v_2) = 2$ und $d(v_3) = 5$.

G sei ein zusammenhängender Multigraph. Hat G eine Eulersche Linie L, so gibt es beim Durchlaufen von L zu jeder Kante, auf der man zu einem Knoten v hingeht, eine andere Kante in L, auf der man von v wieder weggeht. Sucht man beim Durchlaufen von L den Knoten v genau m mal auf, so gilt $d(v) = 2m$. Also:

Hat G eine Eulersche Linie, so muss der Grad jedes Knotens gerade sein. (4.5)

Da beim Königsberger Brückenproblem der Knoten A (ebenso wie alle anderen Knoten) einen ungeraden Grad hat, lautet die Antwort auf die Frage des Brückenproblems also: „Nein“.

In (4.5) haben wir eine Bedingung angegeben, die immer gelten muss, wenn G eine Eulersche Linie hat. Oder anders ausgedrückt: Schreiben wir (A) für die Aussage „G hat eine Eulersche Linie“ und (B) für die Aussage „In G ist der Grad jedes Knotens gerade“, so gilt immer

$$(A) \Rightarrow (B). \tag{4.6}$$

Definition.
Gilt für zwei Aussagen (A) und (B) die Beziehung (4.6), so nennt man (B) eine *notwendige Bedingung* für (A).

In unserem Beispiel: Die Bedingung, dass jeder Knoten von G einen geraden Grad hat, ist eine notwendige Bedingung für die Existenz einer Eulerschen Linie in G.

Wir werden unten sehen, dass auch die Umkehrung von (4.5) richtig ist: Wenn in G der Grad jedes Knotens gerade ist, so hat G immer eine Eulersche Linie (vgl. Satz 4). Mit unseren obigen Bezeichnungen gilt also auch:

$$(A) \Leftarrow (B)\ . \tag{4.7}$$

Definition.
Gilt für zwei Aussagen (A) und (B) die Beziehung (4.7), so nennt man (B) eine *hinreichende Bedingung* für (A).

Satz 4.
Für jeden zusammenhängenden Multigraphen G gilt: G hat genau dann eine Eulersche Linie, wenn der Grad jedes Knotens gerade ist.

Beweis von Satz 4. G sei ein zusammenhängender Multigraph. Dass der Grad jedes Knotens gerade sein muss, wenn G eine Eulersche Linie hat, wurde bereits in (4.5) festgestellt. Umgekehrt zeigen wir nun:

Hat jeder Knoten in G einen geraden Grad, so hat G eine Eulersche Linie. (4.8)

Wir setzen $m = |E(G)|$. Der Beweis von (4.8) erfolgt mit Induktion nach m.

(I) *Induktionsanfang*

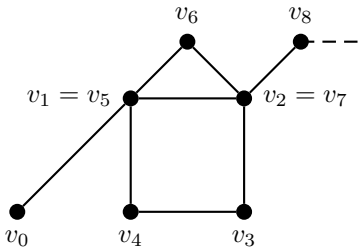
Ist $m = 0$ (d.h., G hat keine Kanten), so gilt $|V(G)| = 1$ (wegen des Zusammenhangs von G); G besteht also nur aus einem einzigen Knoten v_0. Dann hat G selbstverständlich eine Eulersche Linie, nämlich die triviale Eulersche Linie, die nur aus v_0 besteht.

(II) *Induktionsschritt*

Es sei nun $m \geq 1$. Wir nehmen an (Induktionsannahme), dass die Behauptung (4.8) für alle G mit weniger als m Kanten richtig ist. Wir haben zu zeigen, dass (4.8) dann auch für alle G mit m Kanten richtig ist.

Sei G also ein zusammenhängender Multigraph mit $|E(G)| = m$, in dem jeder Knoten einen geraden Grad hat. Man konstruiert nun ausgehend von einem beliebigen Knoten v_0 einen Kantenzug Z, indem man nach der folgenden Regel vorgeht:

> Steht man auf einem Knoten v_i und gibt es eine Kante e, die an v_i stößt und die man noch nicht durchlaufen hat, so wählt man eine solche Kante e beliebig und läuft über e zum nächsten Knoten. Diesen Knoten nennt man v_{i+1}. (⋆)



Kann der Kantenzug Z nicht fortgesetzt werden, so steht man auf dem Anfangsknoten v_0, denn: Steht man auf einem Knoten $v_i \neq v_0$, so hat man bisher eine ungerade Zahl von Kanten, die an v_i stoßen, durchlaufen. Da aber $d(v_i)$ eine gerade Zahl ist, hat man noch mindestens eine Kante zur Verfügung, auf der man v_i wieder verlassen kann.

Der konstruierte Kantenzug Z ist also ein geschlossener Kantenzug. Enthält Z alle Kanten von G, so ist Z eine Eulersche Linie und man ist fertig. Andernfalls bildet man den Multigraphen G', der aus G dadurch entsteht, dass man alle Kanten von Z aus G weglässt.

In G' hat jede Ecke einen geraden Grad. (Warum? Man gebe eine Begründung!)

G' muss nicht zusammenhängend sein; es seien etwa $G'_1, \ldots, G'_r$ die Zusammenhangskomponenten von G'. Es gilt

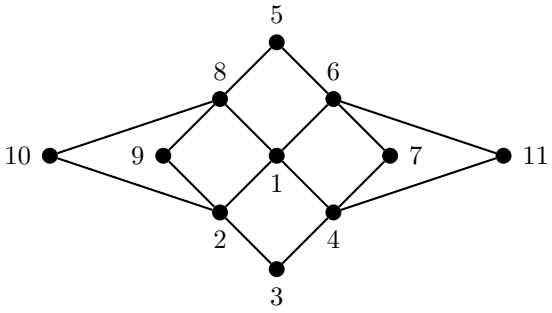
$$|E(G')| < |E(G)| = m.$$

Folglich gilt also auch für jedes G'_i:

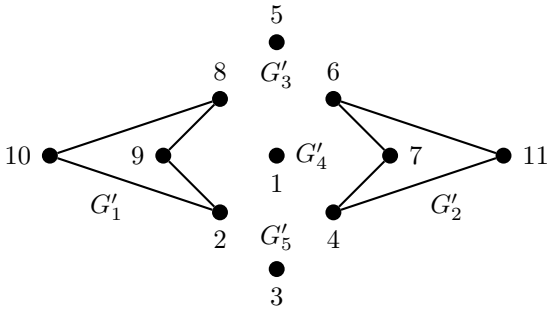
$$|E(G'_i)| < m.$$

Wir können also die Induktionsannahme auf jedes G'_i anwenden und erhalten, dass jedes G'_i eine Eulersche Linie L_i besitzt ($i = 1, \ldots, r$). Da G zusammenhängend ist, hat jede dieser Eulerschen Linien L_i mindestens einen Knoten mit Z gemeinsam. Man kann daher die Eulerschen Linien L_1, …, L_r mit Z zu einer Eulerschen Linie L von G zusammenfügen. □

Beispiel zum Beweis von Satz 4.



In diesem Graphen G hat jede Ecke geraden Grad. Man starte in dem Knoten 1 und konstruiert den Kantenzug Z nach der Regel (⋆), d.h., man läuft immer (falls möglich) auf einer beliebigen, noch nicht benutzten Kante zum nächsten Knoten. Die Reihenfolge, in der Z die Knoten besucht, ist also beispielsweise 1, 2, 3, 4, 1, 6, 5, 8, 1. Nimmt man die durchlaufenen Kanten aus G heraus, so entsteht folgender Graph G':



G' besteht aus fünf Komponenten $G'_1, \ldots, G'_5$. In G'_1 gibt es die Eulersche Linie L_1: 2, 9, 8, 10, 2 und in G'_2 gibt es die Eulersche Linie L_2: 4, 7, 6, 11, 4.

Setzt man Z, L_1 und L_2 zusammen[3], so erhält man in G die Eulersche Linie L:

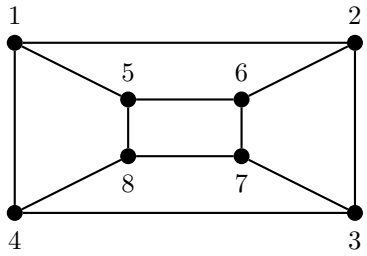
$$1,\ 2,\ 9,\ 8,\ 10,\ 2,\ 3,\ 4,\ 7,\ 6,\ 11,\ 4,\ 1,\ 6,\ 5,\ 8,\ 1.$$

Der obige Beweis von Satz 4 enthält ein Verfahren, wie man in einem Multigraphen, in dem jeder Knoten einen geraden Grad hat, eine Eulersche Linie auch tatsächlich finden kann.

Definition.

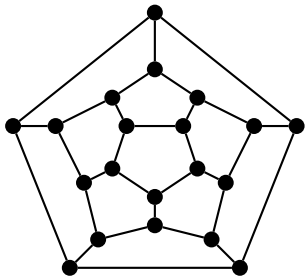
G sei ein Graph und C sei ein Kreis in G. Man nennt C einen *Hamiltonschen Kreis*, wenn C sämtliche Knoten von G enthält.

Beispiel 1. Gegeben sei der folgende Graph G:



Durch 1, 5, 6, 2, 3, 7, 8, 4, 1 wird ein Hamiltonscher Kreis von G beschrieben.

Zur Übung: Hat der folgende Graph einen Hamiltonschen Kreis?



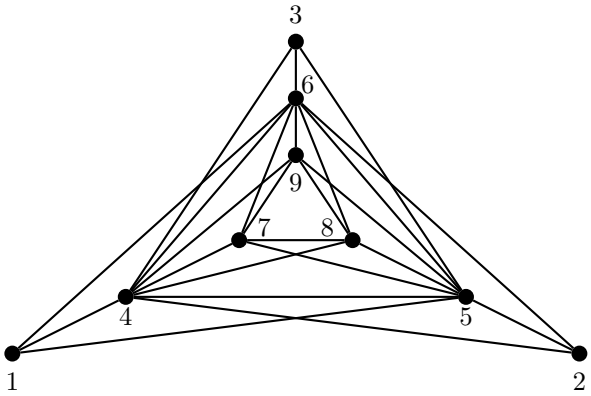
Ist $G = (V, E)$ ein Graph und $A \subseteq V$ eine Teilmenge der Knotenmenge, so bezeichnet man mit $G - A$ den Graphen, der entsteht, wenn man alle Knoten $v \in A$ und alle mit diesen Knoten inzidenten Kanten entfernt.

Die Anzahl der Komponenten[4] eines Graphen G sei mit $c(G)$ bezeichnet.

Beispiel 2. Gegeben sei der folgender Graph G mit 9 Knoten:

[3] Die Komponenten G_i $(i = 3, 4, 5)$ haben triviale Eulersche Linien L_i $(i = 3, 4, 5)$. Diese braucht man beim Zusammensetzen natürlich nicht zu berücksichtigen.

[4] Statt *Zusammenhangskomponente* sagt man auch einfach *Komponente*.



Es sei $A = \{4, 5, 6\}$. Dann gilt $c(G - A) = 4$; der Graph $G - A$ besteht nämlich aus dem Dreieck, das durch 7, 8 und 9 gebildet wird sowie aus den 3 isolierten Knoten 1, 2 und 3.

Eine notwendige Bedingung für die Existenz eines Hamiltonschen Kreises liefert der folgende Satz.

Satz 5.

Hat ein Graph G einen Hamiltonschen Kreis, so gilt für jede nicht leere Teilmenge A der Knotenmenge von G:

$$c(G - A) \leq |A|.$$

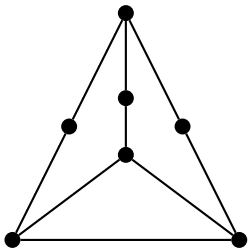
Beweis von Satz 5. Für jeden Kreis C gilt offenbar: Entfernt man aus C genau k Knoten für $k \geq 1$ sowie die mit diesen Knoten inzidenten Kanten, so zerfällt C in höchstens k Komponenten. Hat ein Graph G einen Hamiltonschen Kreis H, so gilt demnach für jedes nichtleere $A \subseteq V(G)$:

$$c(H - A) \leq |A|.$$

Da H ein Teilgraph von G ist, der alle Knoten von G enthält, gilt $c(G - A) \leq c(H - A)$ und somit auch $c(G - A) \leq |A|$. □

Aus Satz 5 folgt, dass der Graph aus Beispiel 2 keinen Hamiltonschen Kreis haben kann, da (wie oben bereits festgestellt) für $A = \{4, 5, 6\}$ gilt: $c(G - A) = 4$.

Ist die Bedingung aus Satz 5 auch hinreichend für die Existenz eines Hamiltonschen Kreises? Die Antwort ist nein. Dies kann man beispielsweise durch die Betrachtung des folgenden Graphen erkennen:



Dieser Graph G erfüllt die Bedingung, dass $c(G - A) \leq |A|$ für alle $A \subseteq V(G)$ gilt; trotzdem hat G keinen Hamiltonschen Kreis. (Übungsaufgabe: Man mache sich klar, dass dies tatsächlich so ist!)

Wir betrachten die folgende Bedingung:

$$c(G - A) \leq |A| \text{ für alle nichtleeren } A \subseteq V(G) \qquad (\star)$$

Wir können feststellen: Die Bedingung ($\star$) ist zwar notwendig, aber nicht hinreichend für die Existenz eines Hamiltonschen Kreises. Man kennt andere Bedingungen, die ebenfalls notwendig für die Existenz eines Hamiltonschen Kreises sind, hinreichend ist allerdings keine dieser Bedingungen. Umgekehrt kennt man auch hinreichende Bedingungen, die allerdings nicht notwendig sind.

Hier liegt ein entscheidender Unterschied zwischen dem Problem der Eulerschen Linie und dem Problem des Hamiltonschen Kreises: *Während geklärt ist, welche Graphen eine Eulersche Linie haben und welche nicht (vgl. Satz 4), ist die entsprechende Frage für Hamiltonsche Kreise ein ungelöstes Problem.*

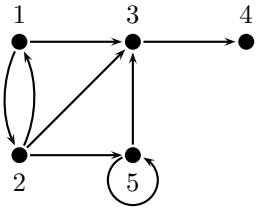
Ein weiterer Unterschied: Es gibt effiziente Algorithmen, mit denen man für jeden beliebigen Graphen G entscheiden kann, ob G eine Eulersche Linie besitzt und die, falls vorhanden, eine Eulersche Linie von G liefern[5]. Entsprechendes kennt man für Hamiltonsche Kreise nicht[6].

4.3 Gerichtete Graphen

Ein *gerichteter Graph* (oder *Digraph*) G ist ein Paar (V, E), wobei V eine beliebige endliche Menge ist; E ist eine Relation auf V, d.h., $E \subseteq V \times V$. Die Elemente von V nennt man die *Knoten* von G, die Elemente von E heißen *Kanten* von G. Eine Kante der Form (v, v) nennt man *Schlinge*.

Wie schon in Abschnitt 3.1 dargelegt, kann man jeden gerichteten Graphen G durch eine Matrix darstellen. Diese Matrix heißt *Adjazenzmatrix* von G. Die Adjazenzmatrix von G ist nur bis auf die Reihenfolge ihrer Zeilen und Spalten eindeutig bestimmt. Daneben spielt die Darstellung eines gerichteten Graphen durch *Nachbarschaftslisten* eine große Rolle.

Beispiel. $G = (V, E)$ sei der folgende gerichtete Graph:



Darstellung von G durch eine Adjazenzmatrix und durch Nachbarschaftslisten:

	1	2	3	4	5
1	0	1	1	0	0
2	1	0	1	0	1
3	0	0	0	1	0
4	0	0	0	0	0
5	0	0	1	0	1

$1: \quad 2, 3$
$2: \quad 1, 3, 5$
$3: \quad 4$
$4:$
$5: \quad 3, 5$

Im Übrigen sind diese Darstellungsformen auch für ungerichtete Graphen möglich, da sich jeder ungerichtete Graph als ein gerichteter Graph auffassen lässt, bei dem zu jeder Kante (x, y) auch die Kante (y, x) vorhanden ist.

Beispiel. Ein ungerichteter Graph G und der zu G gehörende gerichtete Graph:

[5] Siehe Beweis von Satz 4 und die an diesen Beweis anschließende Bemerkung.

[6] Wir erwähnen, ohne dies näher zu erläutern, dass es sich bei dem Entscheidungsproblem HAMILTONSCHER KREIS (Eingabe: Ein Graph G; Frage: Hat G einen Hamiltonschen Kreis?) um ein sogenanntes NP-vollständiges Problem handelt.

Darstellung von G durch eine Adjazenzmatrix und durch Nachbarschaftslisten:

	1	2	3	4
1	0	1	1	1
2	1	0	1	0
3	1	1	0	1
4	1	0	1	0

$1: \quad 2, 3, 4$
$2: \quad 1, 3$
$3: \quad 1, 2, 4$
$4: \quad 1, 3$

Viele Begriffe, die wir zuvor für ungerichtete Graphen kennengelernt haben, lassen sich ganz ähnlich auch für gerichtete Graphen definieren. Dies gilt beispielsweise für Begriffe wie „Kantenfolge“, „Kantenzug“, „Weg“ oder „geschlossene Kantenfolge“.

Definition.
Gegeben sei ein gerichteter Graph $G = (V, E)$ sowie eine Folge

$$v_0,\ e_1,\ v_1,\ e_2,\ v_2,\ \ldots,\ v_{\ell-1},\ e_\ell,\ v_\ell \quad \big(\ell \in \mathbb{N} \cup \{0\}\big) \tag{4.9}$$

mit $v_i \in V$ $(i = 0, \ldots, \ell)$ und $e_i \in E$ $(i = 1, \ldots, \ell)$.

(1) Diese Folge heißt *gerichtete Kantenfolge* von v_0 nach v_ℓ, falls (für $i = 1, \ldots, \ell$) $e_i = \big(v_{i-1}, v_i\big)$ gilt, d.h., e_i ist eine gerichtete Kante von v_{i-1} nach v_i.

(2) Sind in dieser Kantenfolge alle Kanten verschieden, so spricht man von einem *gerichteten Kantenzug*.

(3) Sind außerdem alle Knoten verschieden, so spricht man von einem *gerichteten Weg*.

(4) Eine gerichtete Kantenfolge heißt *geschlossen*, falls $v_0 = v_\ell$ gilt.

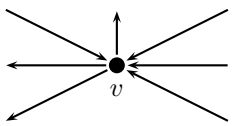
Alternative Terminologie: Pfad, einfacher Pfad, elementarer Pfad bzw. Zyklus[7].

Viele Begriffe für ungerichtete Graphen, wie z.B. „Länge eines Pfades“, lassen sich unmittelbar auf gerichtete Graphen übertragen; in solchen Fällen wollen wir die Übertragung nicht explizit aufführen. Neue Aspekte ergeben sich allerdings bei der Übertragung der Begriffe „Grad eines Knotens“ und „Zusammenhangskomponente“.

Im Gegensatz zu ungerichteten Graphen unterscheidet man bei gerichteten Graphen zwischen dem Innen- und dem Außengrad:

- Der *Innengrad* $d^-(v)$ eines Knotens v ist die Anzahl der Kanten, die zu v hinführen.
- Der *Außengrad* $d^+(v)$ eines Knotens v ist die Anzahl der Kanten, die von v wegführen.

Beispiel:



Hier gilt $d^-(v) = 4$ und $d^+(v) = 3$.

Nun zur Übertragung des Begriffs der Zusammenhangskomponente. Bei gerichteten Graphen unterscheidet man zwischen „schwach zusammenhängend“ und „stark zusammenhängend“ bzw. zwischen „schwachen Komponenten“ und „starken Komponenten“.

In den folgenden Definitionen sei G stets ein gerichteter Graph.

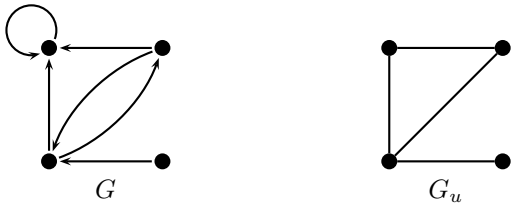
[7] Man lässt hier das Adjektiv „gerichtet“ weg. Da für gerichtete Graphen diese Terminologie weniger umständlich ist, werden wir sie ab jetzt benutzen. Ein Zyklus ist ein geschlossener, gerichteter Kantenzug mit mindestens zwei Kanten.

Definition.

Unter dem G *zugrunde liegenden ungerichteten Graphen* G_u versteht man den Graphen mit derselben Knotenmenge wie G und der Kantenmenge

$$E(G_u) = \Big\{\{x, y\} : (x, y) \in E(G) \text{ oder } (y, x) \in E(G),\ x \neq y\Big\}.$$

Beispiel:



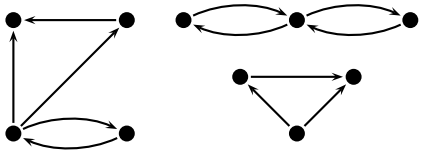
Definition.

G heißt *schwach zusammenhängend*, falls G_u zusammenhängend ist.

Definition.

Ein schwach zusammenhängender gerichteter Graph $G' \subseteq G$ wird *schwache Komponente* von G genannt, falls es außer G' selber keinen schwach zusammenhängenden Teilgraphen von G gibt, der G' enthält.

Beispiel für einen gerichteten Graphen G mit drei schwachen Komponenten (Man begründe, dass dies tatsächlich so ist!):



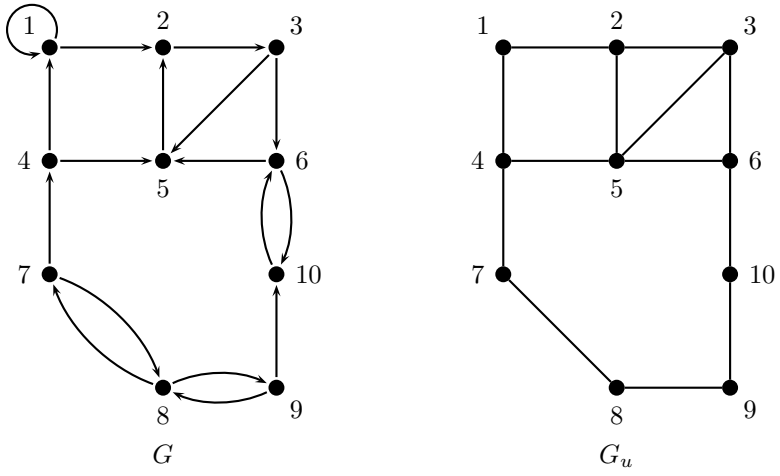
Definition.

G heißt *stark zusammenhängend*, falls es für je zwei Knoten v und w einen Pfad P_1 von v nach w und einen Pfad P_2 von w nach v gibt.

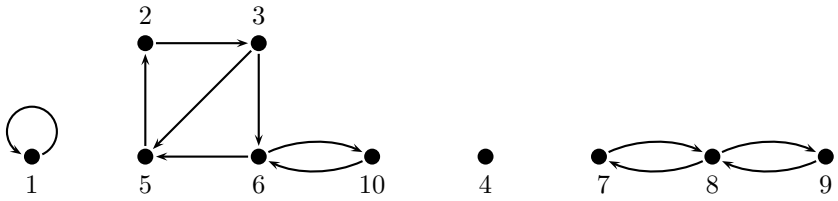
Definition.

Ein stark zusammenhängender gerichteter Graph $G' \subseteq G$ wird *starke Komponente* von G genannt, falls es außer G' selber keinen stark zusammenhängenden Teilgraphen von G gibt, der G' enthält.

Beispiel. Ein gerichteter Graph G und der zugrunde liegende ungerichtete Graph G_u:



G ist schwach zusammenhängend, da G_u zusammenhängend ist. G ist nicht stark zusammenhängend, da es beispielsweise keinen Pfad von 3 nach 1 gibt. G hat vier starke Komponenten; diese werden von den Knotenmengen $\{1\}$, $\{2,3,5,6,10\}$, $\{4\}$ und $\{7,8,9\}$ gebildet:



4.4 Bäume

Da in Büchern über Algorithmen und Datenstrukturen Bäume meist sehr ausführlich behandelt werden, wollen wir uns hier auf weniges beschränken.

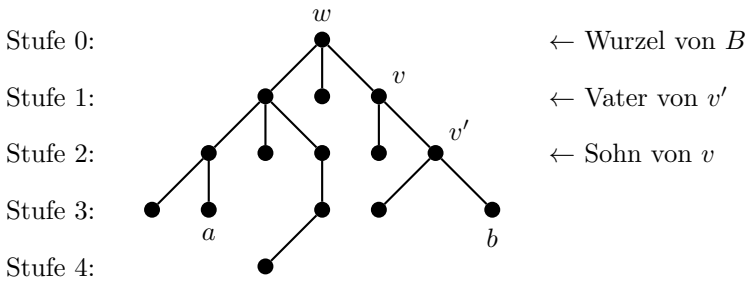
Zur Erinnerung: Ein Baum ist ein kreisloser, zusammenhängender Graph. In Satz 3 und in (4.3) haben wir schon erste Resultate für Bäume festgehalten. Darüber hinaus gilt:

In einem Baum sind je zwei Knoten durch genau einen Weg verbunden. (4.10)

Der Beweis von (4.10) sei als Übungsaufgabe empfohlen.

Im Folgenden sei $B = (V, E)$ immer ein Baum, bei dem ein fester Knoten w als *Wurzel* ausgezeichnet ist. Wir wollen jetzt B als einen gerichteten Graphen auffassen, bei dem alle Kanten von der Wurzel weg gerichtet sind. Ist (bei dieser Orientierung der Kanten von B) eine Kante von v nach v' gerichtet, so nennt man v den *Vater* von v'; v' heißt der *Sohn* von v. Ein Knoten, der keine Söhne hat, heißt ein *Blatt*.

Beispiel



Insgesamt gibt es in diesem Beispiel acht Blätter (z.B. a und b). Ein Knoten, der kein Blatt ist, heißt *innerer Knoten*. Unter dem *Grad von* B versteht man die größte Zahl s, für die es in B einen Knoten v mit s Söhnen gibt[8]. Ein Baum vom Grad 2 bzw. 3 heißt *binärer* bzw. *ternärer Baum*. Hat jeder innere Knoten dieselbe Zahl s von Söhnen, so heißt B *regulär*. Hat der (nach (4.10) eindeutig bestimmte) Weg von der Wurzel w zum Knoten v die Länge ℓ, so sagt man, dass v auf *Stufe* ℓ liegt. Die größte Stufe eines Knotens von B heißt die *Höhe* von B. Der Baum aus obigem Beispiel hat also die Höhe 4.

Wir wollen uns jetzt binäre reguläre Bäume noch etwas genauer ansehen. In einem regulären binären Baum hat jeder innere Knoten genau zwei Söhne; bezeichnen wir mit $d(v)$ den Grad des Knoten v, so gilt $d(w) = 2$ für die Wurzel w, $d(v) = 3$ für alle inneren Knoten $v \neq w$ und $d(v) = 1$ für alle Blätter. Es

[8] Mit anderen Worten: Orientiert man (wie angenommen) alle Kanten von der Wurzel weg, so ist s der Außengrad von v.

folgt:

$$\begin{gathered}\text{Ist } B \text{ ein regulärer, binärer Baum mit genau } n \text{ Knoten,} \\ \text{so hat } B \text{ genau } \frac{n+1}{2} \text{ Blätter und genau } \frac{n-1}{2} \text{ innere Knoten.}\end{gathered} \tag{4.11}$$

Beweis. Ist p die Zahl der Blätter, so folgt nach den Sätzen 1 und 3, dass

$$2 + (n - 1 - p) \cdot 3 + p = 2(n - 1)$$

gilt. Hieraus folgt $p = \frac{n+1}{2}$. Die Zahl der inneren Knoten ist dann $n - p = \frac{n-1}{2}$. □
Abschließend wollen wir noch Folgendes festhalten:

$$B \text{ sei ein Baum vom Grad } s \geq 2 \text{ mit Höhe } h. \text{ Dann hat } B \text{ höchstens } \frac{s^{h+1} - 1}{s - 1} \text{ Knoten.} \tag{4.12}$$

Beweis. In Stufe 0 hat B genau $s^0 = 1$ Knoten (nämlich die Wurzel), in Stufe 1 hat B höchstens s Knoten, in Stufe 2 hat B höchstens s^2 Knoten, ... und in Stufe h hat B höchstens s^h Knoten. Also hat B insgesamt höchstens $\sum_{i=0}^{h} s^i$ Knoten. Nach der geometrischen Summenformel gilt:

$$\sum_{i=0}^{h} s^i = \frac{s^{h+1} - 1}{s - 1} \quad \square$$

5 Elementare Zahlentheorie und Kombinatorik (Fortsetzung)

5.1 Modulare Arithmetik

Es sei $\sim$ eine Äquivalenzrelation auf einer Menge M und x sei ein Element von M. Mit $[x]$ bezeichnen wir diejenige Äquivalenzklasse, die x enthält. Es ist in diesem Zusammenhang zu beachten, dass $[x] = [x']$ gelten kann, obwohl x und x' verschieden sind: Dies ist genau dann der Fall, wenn x und x' derselben Äquivalenzklasse angehören.

Ist beispielsweise $M = \{a, b, c, d, e, f, g, h\}$ und sind $K_1 = \{a, b, c\}$, $K_2 = \{d\}$ und $K_3 = \{e, f, g, h\}$ die Äquivalenzklassen von M, so gilt:

$$\begin{aligned} K_1 &= [a] = [b] = [c] \\ K_2 &= [d] \\ K_3 &= [e] = [f] = [g] = [h] \end{aligned}$$

D.h., *für ein und dieselbe Äquivalenzklasse kann es eine ganze Reihe von verschiedenen Bezeichnungen geben*, je nachdem, welches Element man zur Darstellung benutzt.

Jedes Element einer Äquivalenzklasse nennt man einen *Vertreter* (oder *Repräsentanten*) dieser Äquivalenzklasse. Nehmen wir aus jeder Äquivalenzklasse genau einen Vertreter, so sprechen wir von einem (vollständigen) *Vertretersystem* (oder *Repräsentantensystem*).

Wir betrachten in diesem Abschnitt eine besonders wichtige Äquivalenzrelation auf der Menge $\mathbb{Z}$ der ganzen Zahlen, nämlich die *Kongruenzrelation* modulo m, die wir bereits in Abschnitt 2.4 kennengelernt haben. Wir wiederholen die Definition und stellen nochmal die wichtigsten Eigenschaften zusammen.

Definition.
Es sei $m \in \mathbb{N}$. Für $a, b \in \mathbb{Z}$ gilt $a \equiv b \pmod{m}$, falls m ein Teiler von $a - b$ ist.

Regeln für das Rechnen mit Kongruenzen.

(1) $a \equiv a \pmod{m}$ für alle $a \in \mathbb{Z}$

(2) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

(3) $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

(4) $a_1 \equiv b_1 \pmod{m} \wedge a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$

$a_1 \equiv b_1 \pmod{m} \wedge a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$

(5) $a_1 \equiv b_1 \pmod{m} \wedge a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$

(6) Gilt $\mathrm{ggT}(k, m) = 1$, dann folgt aus $k \cdot a \equiv k \cdot b \pmod{m}$, dass $a \equiv b \pmod{m}$ ist.

Beweis.

(1) Dies gilt wegen $m \mid (a - a)$.

(2) Dies gilt, da aus $m \mid (a - b)$ selbstverständlich $m \mid (b - a)$ folgt.

(3) Es gelte $m \mid (a-b)$ und $m \mid (b-c)$. Dann gibt es $x_1, x_2 \in \mathbb{Z}$ mit $m \cdot x_1 = a - b$ und $m \cdot x_2 = b - c$. Addition der beiden Gleichungen ergibt:

$$m \cdot (x_1 + x_2) = a - c.$$

Also gilt $m \mid (a-c)$, womit (3) gezeigt ist.

(4) Es gelte $m \mid (a_1 - b_1)$ und $m \mid (a_2 - b_2)$. Dann gibt es $x_1, x_2 \in \mathbb{Z}$ mit $m \cdot x_1 = a_1 - b_1$ und $m \cdot x_2 = a_2 - b_2$. Durch Addition bzw. Subtraktion der beiden Gleichungen erhält man:

$$\begin{aligned} m \cdot (x_1 + x_2) &= (a_1 + a_2) - (b_1 + b_2) \\ m \cdot (x_1 - x_2) &= (a_1 - a_2) - (b_1 - b_2). \end{aligned}$$

Es folgt $m \mid (a_1 + a_2) - (b_1 + b_2)$ und $m \mid (a_1 - a_2) - (b_1 - b_2)$. Also gilt (4).

(5) Es gelte $m \mid (a_1 - b_1)$ und $m \mid (a_2 - b_2)$. Dann gibt es $x_1, x_2 \in \mathbb{Z}$ mit $m \cdot x_1 = a_1 - b_1$ und $m \cdot x_2 = a_2 - b_2$. Aus $m \cdot x_1 = a_1 - b_1$ und $m \cdot x_2 = a_2 - b_2$ erhält man durch Multiplikation mit a_2 bzw. b_1:

$$\begin{aligned} m \cdot x_1 a_2 &= a_1 a_2 - b_1 a_2 \\ m \cdot x_2 b_1 &= a_2 b_1 - b_2 b_1. \end{aligned}$$

Durch Addition dieser beiden Gleichungen erhält man

$$m \cdot \big(x_1 a_2 + x_2 b_1\big) = a_1 a_2 - b_1 b_2.$$

Also gilt $m \mid (a_1 a_2 - b_1 b_2)$, womit (5) gezeigt ist.

(6) Es gelte $\mathrm{ggT}\,(k, m) = 1$ und $m \mid (ka - kb) = k(a-b)$. Zu zeigen ist $m \mid (a-b)$.

Für $m = 1$ ist dies klar, also können wir $m \geq 2$ annehmen. Es sei

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$$

die Primfaktorzerlegung von m, wobei die p_i verschiedene Primzahlen sind. Wegen $\mathrm{ggT}\,(k, m) = 1$ ist p_i kein Teiler von k $(i = 1, \ldots, s)$. Wegen $m \mid k(a-b)$ ist andererseits $p_i^{\alpha_i}$ ein Teiler von $k(a-b)$. Nach ($\star\star$) in Abschnitt 2.4 muss $p_i^{\alpha_i}$ also ein Teiler von $a - b$ sein. Da dies für alle $i \in \{1, \ldots, s\}$ gilt, folgt $m \mid (a-b)$. □

Gilt $\mathrm{ggT}\,(a, b) = 1$ für $a, b \in \mathbb{Z}$, so nennt man a und b *teilerfremd* oder *relativ prim*.

Die Regeln (1), (2) und (3) besagen, dass es sich bei der Kongruenzrelation modulo m um eine Äquivalenzrelation auf $\mathbb{Z}$ handelt. Die zugehörigen Äquivalenzklassen, die man auch *Kongruenz-* oder *Restklassen* nennt, wollen wir mit

$$[x]_m$$

bezeichnen. Die Äquivalenzklasse $[x]_m$ besteht also aus allen Zahlen $y \in \mathbb{Z}$, für die $m \mid (x - y)$ gilt.

Beispielsweise gilt (vgl. auch (2.10) in Abschnitt 2.4):

$$\begin{aligned} [7]_3 &= \big\{\ldots,\ -5,\ -2,\ 1,\ 4,\ 7,\ 10,\ \ldots\big\} \\ [5]_7 &= \big\{\ldots,\ -9,\ -2,\ 5,\ 12,\ 19,\ \ldots\big\} \end{aligned}$$

Für jede Äquivalenzklasse gibt es unendlich viele verschiedene Bezeichnungen:

$$\begin{aligned} \ldots &= [-5]_3 = [-2]_3 = [1]_3 = [4]_3 = [7]_3 = \ldots \\ \ldots &= [-9]_7 = [-2]_7 = [5]_7 = [12]_7 = [19]_7 = \ldots \end{aligned}$$

Wir definieren

$$\mathbb{Z}_m := \Big\{ [x]_m : x \in \mathbb{Z} \Big\}.$$

$\mathbb{Z}_m$ ist also die Menge der zur Äquivalenzrelation $\equiv \pmod m$ gehörigen Äquivalenzklassen. Wie viele Elemente enthält $\mathbb{Z}_m$? Die Antwort erhält man unmittelbar aus der Feststellung (2.10) in Abschnitt 2.4: Es gibt genau m Äquivalenzklassen bzgl. der Relation $\equiv \pmod m$, nämlich $[0]_m$, $[1]_m$, ..., $[m-1]_m$. Es gilt also:

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

Beispiel. Für $m = 3$ gilt:

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

Man nennt $\mathbb{Z}_m$ die *Menge der ganzen Zahlen modulo m*. Wir definieren zwei Operationen auf $\mathbb{Z}_m$, die wir *Addition* und *Multiplikation modulo m* nennen und für die wir die Zeichen $\oplus$ und $\odot$ verwenden.

Definition.
Für alle $x, y \in \mathbb{Z}$ seien die Operationen $\oplus$ und $\odot$ wie folgt definiert:

$$\begin{aligned}
[x]_m \oplus [y]_m &= [x+y]_m \\
[x]_m \odot [y]_m &= [x \cdot y]_m
\end{aligned}$$

Bevor wir diese Definition als vernünftig akzeptieren, müssen wir uns allerdings mit einer Schwierigkeit auseinandersetzen, die daher rührt, dass es für dieselbe Äquivalenzklasse verschiedene Bezeichnungen gibt: Nehmen wir an, dass $[x]_m = [x']_m$ und $[y]_m = [y']_m$ gilt. Damit die Definition von $\oplus$ als vernünftig angesehen werden kann, muss sichergestellt sein, dass auch durch $[x+y]_m$ und $[x'+y']_m$ dieselbe Äquivalenzklasse bezeichnet wird.

Aus unseren Annahmen $[x]_m = [x']_m$ und $[y]_m = [y']_m$ folgt:

$$\begin{aligned}
x &\equiv x' \pmod m \\
y &\equiv y' \pmod m
\end{aligned}$$

Mit (4) folgt hieraus:

$$x + y \equiv x' + y' \pmod m.$$

Es gilt also $[x+y]_m = [x'+y']_m$, d.h., die Definition von $\oplus$ ist in Ordnung. Mit Hilfe von Regel (5) zeigt man das Entsprechende für $\odot$.

Wir setzen ab jetzt immer $m \geq 2$ voraus. In der folgenden Feststellung 1 sind die wichtigsten Rechenregeln für $\mathbb{Z}_m$ zusammengestellt.

Feststellung 1.
Für beliebige $[a]_m, [b]_m, [c]_m \in \mathbb{Z}_m$ gilt:

(M1) $[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$

$[a]_m \odot [b]_m = [b]_m \odot [a]_m$

(M2) $\big([a]_m \oplus [b]_m\big) \oplus [c]_m = [a]_m \oplus \big([b]_m \oplus [c]_m\big)$

$\big([a]_m \odot [b]_m\big) \odot [c]_m = [a]_m \odot \big([b]_m \odot [c]_m\big)$

(M3) $[a]_m \oplus [0]_m = [a]_m$

$[a]_m \odot [1]_m = [a]_m$

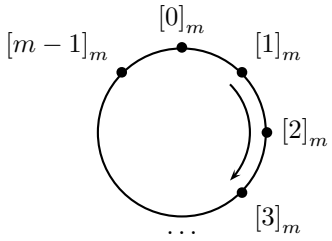
(M4) $[a]_m \odot \big([b]_m \oplus [c]_m\big) = \big([a]_m \odot [b]_m\big) \oplus \big([a]_m \odot [c]_m\big)$

(M5) $[a]_m \oplus [-a]_m = [0]_m$

Beweis. Wir führen nur den Beweis von (M4) vor; die Beweise der übrigen Eigenschaften gehen ähnlich.

$$\begin{aligned}
[a]_m \odot \big([b]_m \oplus [c]_m\big) &= [a]_m \odot [b+c]_m \\
&= [a\big(b+c\big)]_m \\
&= [ab+ac]_m \\
&= [ab]_m \oplus [ac]_m \\
&= \big([a]_m \odot [b]_m\big) \oplus \big([a]_m \odot [c]_m\big) \quad \square
\end{aligned}$$

Die folgende *Veranschaulichung von* $\mathbb{Z}_m$ ist nützlich. Man stellt sich die Elemente von $\mathbb{Z}_m$ als Punkte auf einem Kreis vor:



Es sei $x \in \mathbb{N}$. Wir starten bei $[0]_m$ und bewegen uns im Uhrzeigersinn in Einer-Schritten um den Kreis. Nach jeweils m Schritten sind wir dann wieder bei $[0]_m$ und nach x Schritten sind wir bei demjenigen $[r]_m \in \mathbb{Z}_m$, für das gilt $x = q \cdot m + r$, $0 \leq r \leq m-1$. Oder anders ausgedrückt: Nach x Schritten sind wir bei derjenigen Äquivalenzklasse $[r]_m \in \mathbb{Z}_m$, der x angehört. (Für $x \in \mathbb{Z}$, $x < 0$, verfährt man entsprechend, nur dass man sich entgegen dem Uhrzeigersinn um den Kreis bewegt.)

Wir geben für $m = 2, 3, 4, 5$ die Additions- und Multiplikationstabellen an, wobei wir anstelle von $[r]_m$ der Einfachheit halber r schreiben:

$m = 2$:

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

$\odot$	0	1
0	0	0
1	0	1

$m = 3$:

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

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$m = 4$:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$m = 5$:

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

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Wir nennen das Vertretersystem $0, 1, \ldots, m-1$ das *Standardvertretersystem* von $\mathbb{Z}_m$.

Wir haben in Feststellung 1 gesehen, dass sich eine Reihe von Eigenschaften von $\mathbb{Z}$ auf $\mathbb{Z}_m$ übertragen. Wir erwähnen eine Eigenschaft von $\mathbb{Z}$, die sich nicht auf $\mathbb{Z}_m$ überträgt: In $\mathbb{Z}$ gilt die *Kürzregel*, d.h., für alle $a, b, c \in \mathbb{Z}$ gilt

$$ab = ac \wedge a \neq 0 \Rightarrow b = c.$$

Eine entsprechende Regel gilt nicht in $\mathbb{Z}_m$, jedenfalls nicht für jedes m. Beispielsweise gilt in $\mathbb{Z}_4$:

$$[2]_4 \odot [1]_4 = [2]_4 \odot [3]_4 \quad \text{und} \quad [2]_4 \neq [0]_4, \quad \text{aber} \quad [1]_4 \neq [3]_4.$$

Definition.
Es sei $[a]_m \in \mathbb{Z}_m$. Ein Element $[x]_m \in \mathbb{Z}_m$ heißt *multiplikatives Inverses* von $[a]_m$, falls gilt:

$$[a]_m \odot [x]_m = [1]_m.$$

Besitzt $[a]_m$ ein multiplikatives Inverses, so nennt man $[a]_m$ *invertierbar*.

Beispiele:

1. $[2]_5$ ist invertierbar, da $[2]_5 \odot [3]_5 = [1]_5$ gilt.

2. $[4]_5$ ist invertierbar, da $[4]_5 \odot [4]_5 = [1]_5$ gilt.

3. $[2]_4$ ist nicht invertierbar, da in $\mathbb{Z}_4$ kein Element existiert, das mit $[2]_4$ multipliziert $[1]_4$ ergibt.

Falls keine Missverständnisse möglich sind, schreiben wir ab jetzt immer $+$ und $\cdot$ statt $\oplus$ und $\odot$ oder lassen das Multiplikationszeichen $\cdot$ ganz weg.

Feststellung 2.
Jedes Element aus $\mathbb{Z}_m$ besitzt höchstens ein multiplikatives Inverses.

Beweis. Sind $[x]_m$ und $[y]_m$ multiplikative Inverse von $[a]_m$, so gilt

$$\begin{aligned} [a]_m \cdot [x]_m &= [1]_m \\ [a]_m \cdot [y]_m &= [1]_m \end{aligned}$$

Es folgt

$$\begin{aligned}
[y]_m &= [y]_m \cdot [1]_m \\
&= [y]_m \cdot \big([a]_m \cdot [x]_m\big) \\
&= \big([y]_m \cdot [a]_m\big) \cdot [x]_m \\
&= \big([a]_m \cdot [y]_m\big) \cdot [x]_m \\
&= [1]_m \cdot [x]_m \\
&= [x]_m \quad \square
\end{aligned}$$

Feststellung 3.

Ein Element $[a]_m \in \mathbb{Z}_m$ ist genau dann invertierbar, wenn a und m teilerfremd sind. Insbesondere gilt also: Ist p eine Primzahl, so ist jedes Element aus $\mathbb{Z}_p \setminus \big\{[0]_p\big\}$ invertierbar.

Beweis. Sei $[a]_m$ invertierbar. Dann existiert ein $[x]_m \in \mathbb{Z}_m$, so dass $[a]_m \cdot [x]_m = [1]_m$ gilt. Es folgt $ax \equiv 1 \pmod{m}$. Es gibt also ein $k \in \mathbb{Z}$, so dass $ax - 1 = km$ gilt, woraus $ax - km = 1$ folgt. Es sei $g = \mathrm{ggT}\,(a, m)$. Da g sowohl a als auch m teilt, teilt g auch $ax - km$, d.h., g teilt 1. Also gilt $g = 1$, d.h., a und m sind teilerfremd.

Es sei nun umgekehrt $\mathrm{ggT}\,(a, m) = 1$. Wir betrachten die Äquivalenzklassen $[0a]_m$, $[1a]_m$, …, $[(m-1)a]_m$ und behaupten, dass sie alle verschieden sind.

In der Tat: Aus $[ra]_m = [sa]_m$ folgt $ra \equiv sa \pmod{m}$, woraus wegen der Voraussetzung $\mathrm{ggT}\,(a, m) = 1$ und wegen (6) $r \equiv s \pmod{m}$ folgt.

Damit ist gezeigt, dass $[0a]_m$, $[1a]_m$, …, $[(m-1)a]_m$ verschiedene Elemente von $\mathbb{Z}_m$ sind. Da $\mathbb{Z}_m$ genau m Elemente enthält, muss es also ein $r \in \big\{0, 1, \ldots, m-1\big\}$ geben, für das $[ra]_m = [1]_m$ gilt. Wegen $[ra]_m = [r]_m \cdot [a]_m$ folgt, dass $[a]_m$ invertierbar ist. $\square$

Wir illustrieren den zweiten Teil des obigen Beweises noch durch ein Beispiel: Es sei $m = 9$ und $a = 4$. Es gilt $\mathrm{ggT}\,(a, m) = 1$ und wir haben die folgenden Kongruenzklassen:

$$\begin{array}{lll}
[0 \cdot 4]_9 = [0]_9 & [3 \cdot 4]_9 = [3]_9 & [6 \cdot 4]_9 = [6]_9 \\
[1 \cdot 4]_9 = [4]_9 & [4 \cdot 4]_9 = [7]_9 & [7 \cdot 4]_9 = [1]_9 \\
[2 \cdot 4]_9 = [8]_9 & [5 \cdot 4]_9 = [2]_9 & [8 \cdot 4]_9 = [5]_9
\end{array}$$

Die Kongruenzklassen $[0 \cdot 4]_9$, …, $[8 \cdot 4]_9$ sind also tatsächlich alle verschieden und wegen $[7 \cdot 4]_9 = [1]_9$ ist $[7]_9$ das multiplikative Inverse von $[4]_9$.

Die nächste Feststellung folgt unmittelbar aus den Feststellungen 1 und 3.

Feststellung 4.

Ist p eine Primzahl, so ist $\mathbb{Z}_p$ ein Körper.

Insbesondere ist also $\mathbb{Z}_2$ ein Körper. Anders ausgedrückt bedeutet dies: Die Menge $B = \big\{0, 1\big\}$ versehen mit den Operationen $\oplus$ („Exklusiv-Oder“) und $\wedge$ („Konjunktion“) bildet einen Körper.

Ein klassischer Satz, der beispielsweise in der Kryptographie Anwendung findet, ist der folgende.

Satz von Fermat.

Es sei p eine Primzahl und n sei eine natürliche Zahl, für die $p \nmid n$ gilt. Dann folgt:

$$n^{p-1} \equiv 1 \pmod{p}.$$

Beweis. Da $p \nmid n$ gilt und da p eine Primzahl ist, gilt $\mathrm{ggT}\,(n, p) = 1$. Ähnlich zum zweiten Teil des Beweises von Feststellung 3 sowie dem darauf folgenden Beispiel sind $[1n]_p$, …, $[(p-1)n]_p$ genau die Äquivalenzklassen $[1]_p$, …, $[p-1]_p$ (möglicherweise in anderer Reihenfolge).

Für das Produkt $v = 1 \cdot 2 \cdot \ldots \cdot (p-1)$ folgt daher

$$v \equiv \big(1 \cdot n\big) \cdot \big(2 \cdot n\big) \cdot \ldots \cdot \big(p-1\big) \cdot n \equiv v \cdot n^{p-1} \pmod{p}$$

Aufgrund der Definition von v und der Tatsache, dass p eine Primzahl ist, gilt $\mathrm{ggT}\,(v,p) = 1$. Deshalb können wir (6) anwenden, um aus $v \equiv v \cdot n^{p-1} \pmod{p}$ die Behauptung $1 \equiv n^{p-1} \pmod{p}$ zu erhalten. □

Bemerkung zur Schreibweise. In der Praxis ist es üblich, vereinfachte Schreibweisen zu verwenden. Ähnlich wie wir unsere ursprüngliche Schreibweise $\oplus$ und $\odot$ durch $+$ und $\cdot$ ersetzt haben, schreibt man für die Elemente von $\mathbb{Z}_m$ einfach $0, 1, \ldots, m-1$ anstelle von $[0]_m, [1]_m, \ldots, [m-1]_m$. Um Missverständnisse auszuschließen muss man dann allerdings immer deutlich machen, ob man mit $0, 1, \ldots, m-1$ die Elemente aus $\mathbb{Z}_m$ oder aus $\mathbb{Z}$ meint. Das kann man durch erläuternde Zusätze wie „in $\mathbb{Z}_m$“ bzw. „in $\mathbb{Z}$“ machen. Außerdem verwendet man in $\mathbb{Z}_m$ die übliche Klammersparregel „Punktrechnung vor Strichrechnung“. Anstelle von

$$\big([7]_9 \cdot [2]_9\big) + [3]_9 = [8]_9$$

kann man also auch

$$7 \cdot 2 + 3 = 8 \quad (\text{in } \mathbb{Z}_9)$$

schreiben, was im Übrigen genau dieselbe Bedeutung hat wie

$$7 \cdot 2 + 3 \equiv 8 \pmod{9}.$$

Feststellung 5.
Es gelte $a, b \in \mathbb{N}$ und $d = \mathrm{ggT}\,(a,b)$. Dann gibt es $\lambda, \mu \in \mathbb{Z}$, so dass gilt:

$$d = \lambda a + \mu b. \tag{5.1}$$

Man beweist dies mit Hilfe des Euklidischen Algorithmus „durch Rückwärtseinsetzen“ (siehe etwa N. L. Biggs, Discrete Mathematics). Wir erläutern Feststellung 5 und ihren Beweis an einem Beispiel.

Beispiel. Es seien $a = 816$ und $b = 294$ gegeben.

Euklidischer Algorithmus:

$$\begin{aligned} 816 &= 2 \cdot 294 + 228 \\ 294 &= 1 \cdot 228 + 66 \\ 228 &= 3 \cdot 66 + 30 \\ 66 &= 2 \cdot 30 + 6 \\ 30 &= 5 \cdot 6 + 0 \end{aligned}$$

Es gilt also $d = \mathrm{ggT}\,(a,b) = 6$.

Ausgehend von der *vorletzten Gleichung* erhält man durch *Rückwärtseinsetzen*:

$$\begin{aligned} d = 6 &= 66 - 2 \cdot 30 \\ &= 66 - 2 \cdot \big(228 - 3 \cdot 66\big) \\ &= \big(-2\big) \cdot 228 + 7 \cdot 66 \\ &= \big(-2\big) \cdot 228 + 7 \cdot \big(294 - 1 \cdot 228\big) \\ &= 7 \cdot 294 + \big(-9\big) \cdot 228 \\ &= 7 \cdot 294 + \big(-9\big) \cdot \big(816 - 2 \cdot 294\big) \\ &= \big(-9\big) \cdot 816 + 25 \cdot 294 \\ &= \lambda \cdot 816 + \mu \cdot 294 \quad \text{für } \lambda = -9 \text{ und } \mu = 25 \end{aligned}$$

Für den Spezialfall, dass a und b *teilerfremd* sind, besagt Feststellung 5: Es gibt $\lambda, \mu \in \mathbb{Z}$, so dass gilt:

$$1 = \lambda a + \mu b \tag{5.2}$$

Anwendung

Gegeben seien $a, m \in \mathbb{N}$ mit $m \geq 2$.

Aufgabe. Es soll, falls vorhanden, das multiplikative Inverse von $a \in \mathbb{Z}_m$ bestimmt werden.

Lösung. Man bestimme mit dem Euklidischen Algorithmus $d = \mathrm{ggT}\,(a, m)$. Gilt $d \neq 1$, so ist a nicht invertierbar. Gilt hingegen $d = 1$, so bestimme man (wie oben erläutert) $\lambda, \mu \in \mathbb{Z}$, so dass gilt:

$$1 = \lambda a + \mu m.$$

Es folgt

$$1 \equiv \lambda a + \mu m \equiv \lambda a \pmod{m}.$$

Also: *λ ist das Inverse von a in $\mathbb{Z}_m$.*

Abschließend sollte man das Inverse von a in $\mathbb{Z}_m$ noch durch ein Element aus $\{1, \ldots, m-1\}$ ausdrücken. Wir erläutern dies durch **Beispiele**:

Es gelte $m = 13$.

1. Hat man z.B. $\lambda = 85$ erhalten, so teilt man 85 durch 13 und erhält

$$85 = 6 \cdot 13 + 7.$$

Es gilt also:

$$\lambda = 85 \equiv 7 \pmod{13}.$$

Das Ergebnis in seiner endgültigen Form lautet also 7.

2. Gilt $\lambda < 0$, so verfährt man ähnlich: Hat man z.B. $\lambda = -3229$ erhalten, so teilt man 3229 durch 13 und erhält

$$3229 = 248 \cdot 13 + 5.$$

Es folgt

$$3229 \equiv 5 \pmod{13},$$

woraus sich

$$\lambda = -3229 \equiv -5 \equiv 13 - 5 \equiv 8 \pmod{13}$$

ergibt. Das Ergebnis lautet also 8.

5.2 Gerade und ungerade Permutationen

Wir wiederholen zunächst einige Tatsachen über Permutationen (siehe auch Abschnitt 2.6). Man definiert eine Permutation einer nichtleeren Menge M als eine Bijektion $M \to M$. In diesem Abschnitt wird meistens $M = \{1, \ldots, n\}$ gelten (für ein $n \in \mathbb{N}$). Die Menge aller Permutationen von $\{1, 2, \ldots, n\}$ bezeichnen wir mit S_n. Es gilt $|S_n| = n!$.

Beispiel. $\pi \in S_7$ sei gegeben durch

$$\pi(1) = 3,\ \pi(2) = 7,\ \pi(3) = 5,\ \pi(4) = 4,\ \pi(5) = 6,\ \pi(6) = 1 \text{ und } \pi(7) = 2.$$

Zwei andere Möglichkeiten, π zu beschreiben:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{pmatrix}$$

oder (ähnlich, aber vielleicht etwas intuitiver)

$$\begin{array}{cccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \pi & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{array}$$

Eine Permutation $\pi \in S_n$ bewirkt eine Änderung der Reihenfolge der Zahlen 1, 2, ..., n und es kann nützlich sein, sich eine Permutation als eine solche Änderung der Reihenfolge vorzustellen. Man sollte aber nicht vergessen, *dass eine Permutation laut Definition eine bestimmte Art von Abbildung ist* (nämlich eine bijektive Abbildung einer Menge auf sich selbst).

Nacheinanderausführung (Komposition) von Permutationen

Sind π_1 und π_2 Permutationen derselben Menge M, so lassen sich π_1 und π_2 natürlich auch hintereinander ausführen, d.h., man kann $\pi_2 \circ \pi_1$ bilden. Die Abbildung $\pi_2 \circ \pi_1$ ist dann ebenfalls eine Permutation der Menge M.

Beispiel. Es seien

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{pmatrix} \quad \text{und} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

Dann ist

$$\pi_2 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 4 & 2 & 7 & 6 \end{pmatrix}.$$

Anstelle von $\pi_2 \circ \pi_1$ schreibt man auch einfach $\pi_2\pi_1$. Mit π^k wird die k-fache Nacheinanderausführung von π bezeichnet.

Die Nacheinanderausführung von Permutationen kann man sich auch folgendermaßen veranschaulichen:

$$\begin{array}{cccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \pi_1 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 7 & 5 & 4 & 6 & 1 & 2 \\ \pi_2 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 5 & 1 & 3 & 4 & 2 & 7 & 6 \end{array}$$

Die Komposition von Permutationen ist *nicht kommutativ*.

Beispiel. Es seien π_1 und π_2 wie oben, dann gilt (nachprüfen!):

$$\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 6 & 4 & 5 & 7 & 3 \end{pmatrix} \neq \pi_2 \circ \pi_1.$$

Gilt $\pi(i) = i$, so nennt man i einen *Fixpunkt* von π.

Feststellung 1.

(1) Für alle $\pi, \sigma, \tau \in S_n$ gilt:

$$\pi \circ \big(\sigma \circ \tau\big) = \big(\pi \circ \sigma\big) \circ \tau$$

(2) Für die Permutation $id \in S_n$, die durch $id(k) = k$ für alle $k \in \{1, \ldots, n\}$ definiert wird und die man *Identität* nennt, gilt für alle $\sigma \in S_n$:

$$id \circ \sigma = \sigma \circ id = \sigma.$$

(3) Für jede Permutation $\pi \in S_n$ gibt es eine inverse Permutation $\pi^{-1} \in S_n$, für die gilt:

$$\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = id.$$

Beweis.

(1) Für die Nacheinanderausführung von Abbildungen gilt das Assoziativgesetz (vgl. Abschnitt 3.3);

(2) Dies gilt klarerweise.

(3) Diese Aussage gilt, da die Umkehrfunktion einer bijektiven Abbildung ebenfalls bijektiv ist. □

Wir führen nun eine kompakte Art ein, Permutationen zu beschreiben: die *Zyklenschreibweise*.

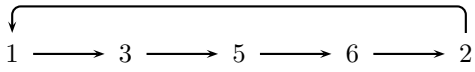
Definition.
Eine Permutation π von $\{1,\dots,n\}$ *heißt Zyklus der Länge* k (für $k \geq 2$), falls es k verschiedene Elemente a_1, …, a_k gibt, für die

$$\pi(a_i) = a_{i+1} \ (i = 1,\dots,k-1) \text{ und } \pi(a_k) = a_1$$

gilt und falls alle anderen Elemente von π festgelassen werden („π vertauscht k Elemente im Kreis und lässt die übrigen fest“).
Einen Zyklus der Länge 2 nennt man eine *Transposition*.
Ergänzend definieren wir noch, was ein *Zyklus der Länge* 1 sein soll: darunter sei die Identität verstanden.

Beispiele:

1. Es sei $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 4 & 6 & 2 & 7 \end{pmatrix}$; dann ist π_1 ein Zyklus der Länge 5, da π_1 die 4 und die 7 festlässt und die übrigen Zahlen nach dem folgenden Schema im Kreis vertauscht:



Als eine bequeme Art, einen solchen Zyklus zu beschreiben, verwendet man die *Zyklenschreibweise*; das bedeutet, dass man $\pi_1 = (1,3,5,6,2)$ schreibt.

2. Es sei $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 6 & 4 & 5 & 3 & 7 \end{pmatrix}$ bzw. in Zyklenschreibweise $\pi_2 = (3,6)$.

Man kann jede Permutation π als Nacheinanderausführung von Zyklen darstellen; wir erläutern dies anhand des Beispiels:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{pmatrix} \tag{5.3}$$

Die Permutation π bildet 1 auf 3, 3 auf 5, 5 auf 6 und 6 wieder auf 1 ab. Ein Zyklus von π lautet demnach $(1,3,5,6)$. Ferner wird 2 auf 7 und 7 auf 2 abgebildet. Ein weiterer Zyklus von π lautet also $(2,7)$. Übrig bleibt nur der Fixpunkt 4. Wir können π also als Nacheinanderausführung zweier Zyklen aufschreiben:

$$\pi = (2,7) \circ (1,3,5,6) \tag{5.4}$$

Die Gleichung (5.4) besagt also: Man erhält π, wenn man erst 1, 3, 5 und 6 im Kreis vertauscht und anschließend 2 und 7 vertauscht. Ebenso gut hätten wir π natürlich auch wie folgt schreiben können:

$$\pi = (1,3,5,6) \circ (2,7) \quad \text{oder} \quad \pi = (1,3,5,6)(2,7)$$

Für unsere Zwecke ist es nützlich, auch die Fixpunkte in die Darstellung von π einzubeziehen. Daher schreiben wir:

$$\pi = (1,3,5,6) \circ (2,7) \circ (4) \tag{5.5}$$

Dabei stellt (4) einen Zyklus der Länge 1 dar. Nach der Definition eines Zyklus der Länge 1 ist (4) nichts anderes als die Identität. Man sagt zu (5.5), dass π *in Zyklenschreibweise* dargestellt ist.

Für jede Permutation $\pi \in S_n$ kann eine Darstellung in Zyklenschreibweise wie folgt gewonnen werden: Man beginnt mit irgendeinem Element aus $M = \{1,\dots,n\}$, sagen wir mit 1, und bildet nacheinander

$$\pi(1),\ \pi(\pi(1)),\ \pi(\pi(\pi(1))),\ \dots$$

solange, bis die 1 wieder erreicht ist; dadurch erhält man den ersten Zyklus. Man wiederholt dies mit einem Element von M, das „noch nicht verwendet wurde“, und fährt mit dieser Prozedur fort, bis jedes Element von M in einem Zyklus vorkommt.

Beispiele:

1. Es sei $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 11 & 8 & 10 & 3 & 4 & 9 & 1 & 7 & 6 & 2 \end{pmatrix}$.

Darstellung von π in Zyklenschreibweise: $\pi = (1,5,3,8)(2,11)(4,10,6)(7,9)$.

2. Es sei $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 7 & 5 & 1 & 3 & 4 \end{pmatrix}$.

Darstellung von π in Zyklenschreibweise: $\pi = (1,2,6,3,7,4,5)$.

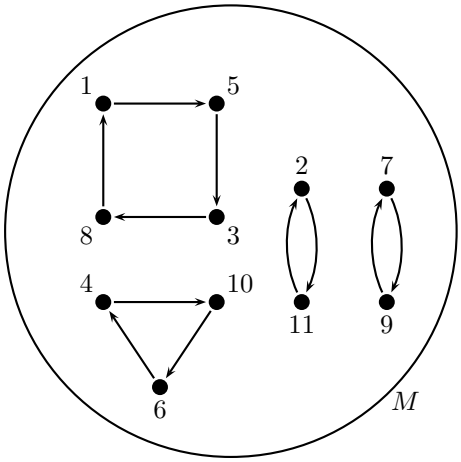
3. Es sei $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 1 & 5 & 3 & 7 & 6 \end{pmatrix}$.

Darstellung von π in Zyklenschreibweise: $\pi = (1,4,5,3)(2)(6,7)$.

Die Zyklenschreibweise ist nicht ganz eindeutig: Man hat die Möglichkeit, die Symbole innerhalb eines Zyklus „im Kreis zu vertauschen“; ferner spielt die Reihenfolge, in der die Zyklen aufgeschrieben werden, keine Rolle. Für die Permutation π aus Beispiel 1 gilt beispielsweise auch:

$$\pi = (2,11)(10,6,4)(8,1,5,3)(9,7).$$

Man kann sich die Zyklen von π auch so vorstellen:



Man sieht, dass zu jeder Permutation π von M eine Partition von M gehört, deren Klassen den Zyklen entsprechen. In unserem Beispiel gibt es zwei Zyklen der Länge 2 und jeweils einen Zyklus der Länge 3 und 4.

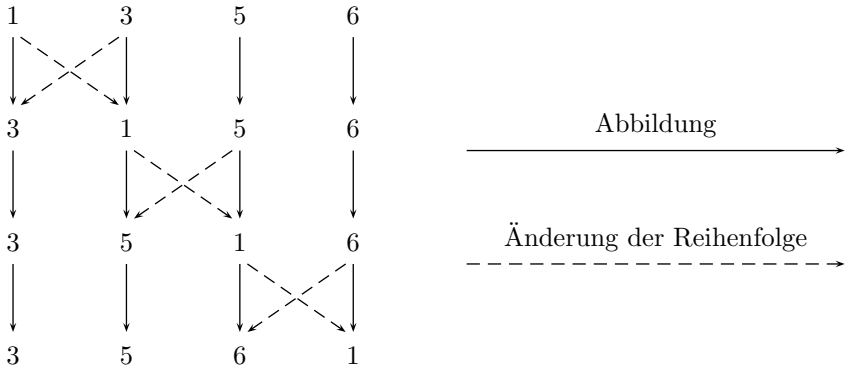
Man kann jede Permutation nicht nur als Nacheinanderausführung von Zyklen, sondern sogar als Nacheinanderausführung von Transpositionen aufschreiben. Wir erläutern dies am obigen Beispiel (5.3): Zunächst stellt man π wie in (5.4) als Nacheinanderausführung von Zyklen dar, danach stellt man die Zyklen, die eine Länge ≥ 3 haben, als Nacheinanderausführung von Transpositionen dar; in unserem Beispiel:

$$(1,3,5,6) = (1,6) \circ (1,5) \circ (1,3) \tag{5.6}$$

Also insgesamt:

$$\pi = (2,7) \circ (1,6) \circ (1,5) \circ (1,3).$$

Dass die in (5.6) behauptete Gleichheit tatsächlich gilt, kann man direkt „durch Nachrechnen“ überprüfen oder sich an folgender Darstellung klarmachen:



Auf dieselbe Art und Weise erkennt man, dass allgemein für einen beliebigen Zyklus $(a_1, a_2, \ldots, a_k)$ der Länge $k \geq 3$ gilt:

$$\big(a_1, a_2, \ldots, a_k\big) = \big(a_1, a_k\big) \circ \big(a_1, a_{k-1}\big) \circ \ldots \circ \big(a_1, a_3\big) \circ \big(a_1, a_2\big) \tag{5.7}$$

Insgesamt haben wir erhalten:

Feststellung 2.
Es sei $n \geq 2$. Dann lässt sich jede Permutation π von $\big\{1, \ldots, n\big\}$ als Nacheinanderausführung von Transpositionen darstellen und man kann eine solche Darstellung gewinnen, indem man π zunächst als Nacheinanderausführung von Zyklen der Länge ≥ 2 darstellt und danach (5.7) auf die Zyklen der Länge ≥ 3 anwendet.

Es sei darauf hingewiesen, dass die Darstellung einer Permutation als Nacheinanderausführung von Transpositionen keineswegs eindeutig ist. Wir haben die Permutation π aus (5.3) dargestellt als

$$\pi = \big(2, 7\big) \circ \big(1, 6\big) \circ \big(1, 5\big) \circ \big(1, 3\big).$$

Eine andere Darstellung derselben Permutation:

$$\begin{aligned} \pi \quad = \quad & \big(2, 3\big) \circ \big(1, 2\big) \circ \big(3, 4\big) \circ \big(2, 3\big) \circ \big(4, 5\big) \circ \big(3, 4\big) \circ \big(2, 3\big) \circ \\ & \big(5, 6\big) \circ \big(4, 5\big) \circ \big(6, 7\big) \circ \big(5, 6\big) \circ \big(4, 5\big) \circ \big(3, 4\big) \circ \big(2, 3\big) \end{aligned}$$

In der ersten Darstellung haben wir π also durch 4, in der zweiten Darstellung durch 14 Transpositionen dargestellt. Wir können andere Darstellungen, etwa durch 6, 8, 10 oder 12 Transpositionen finden; wir können π jedoch nicht als Nacheinanderausführung einer ungeraden Zahl von Transpositionen darstellen. Das besagt der folgende Satz.

Satz 1.
Nehmen wir an, dass die Permutation $\pi \in S_n$ sowohl als Nacheinanderausführung von r als auch als Nacheinanderausführung von r' Transpositionen dargestellt werden kann. Dann gilt: Entweder sind r und r' beide gerade oder sie sind beide ungerade.

Einen Beweis dieses Satzes findet man beispielsweise im Lehrbuch von N. L. Biggs, Discrete Mathematics, Oxford University Press, 2001.

Definition.
Es sei $n \geq 2$. Eine Permutation $\pi \in S_n$ heißt *gerade*, wenn für jede Darstellung von π als Nacheinanderausführung von Transpositionen gilt: Die Anzahl von Transpositionen in einer solchen Darstellung ist gerade. Analog wird definiert, wann eine Permutation *ungerade* heißt.
Man definiert das *Vorzeichen von* π (Bezeichnung: $\operatorname{sign} \pi$) folgendermaßen:

$$\operatorname{sign} \pi := \begin{cases} 1 & \text{, falls } \pi \text{ eine gerade Permutation ist} \\ -1 & \text{, falls } \pi \text{ eine ungerade Permutation ist} \end{cases}$$

Wir schließen mit folgendem Satz, dessen Beweis man ebenfalls im Buch von N. L. Biggs, Discrete Mathematics findet.

Satz 2.

Für jedes $n \geq 2$ gilt: Genau die Hälfte aller Permutationen aus S_n ist gerade. Die andere Hälfte ist ungerade.

5.3 Matrizen

Definition.

Es seien $I = \{1, 2, \ldots, m\}$, $J = \{1, 2, \ldots, n\}$ und $I \times J$ sei das kartesische Produkt von I und J, d.h. die Menge der Zahlenpaare (i, j) mit $i \in I$ und $j \in J$. M sei eine beliebige Menge. Eine $m \times n$ - Matrix A über M ist eine Abbildung

$$A : I \times J \to M$$

Man stellt eine $m \times n$ - Matrix A als ein rechteckiges Schema mit m *Zeilen*, n *Spalten* und $m \cdot n$ *Einträgen* $a_{ij} \in M$ $(i = 1, \ldots, m$ sowie $j = 1, \ldots, n)$ dar:

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn}. \end{pmatrix}$$

i heißt *Zeilenindex*, j heißt *Spaltenindex* von A.

Man schreibt auch

$$A = \big(a_{ij}\big)_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} \quad \text{oder} \quad A = (a_{ij}).$$

Ist die Anzahl m der Zeilen gleich der Anzahl n der Spalten, so spricht man von einer *quadratischen Matrix*.

Ist $a_{ij} \in \mathbb{R}$ für alle i und j, so spricht man von einer *reellen Matrix*. Ab jetzt seien alle betrachteten Matrizen reell, sofern nicht ausdrücklich etwas anderes gesagt wird.

Beispiele:

$$\begin{pmatrix} 2 & 4 \\ 5 & 6 \\ 7 & 7 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \qquad \begin{pmatrix} 5 & 5 & 5 \\ 6 & 6 & 6 \\ 7 & 7 & 0 \end{pmatrix} \qquad \begin{pmatrix} 4 & -1 & -2 \end{pmatrix} \qquad \begin{pmatrix} 4 \\ 3 \\ 3 \end{pmatrix}$$

$3 \times 2 -$ Matrix $\quad 2 \times 3 -$ Matrix $\quad 3 \times 3 -$ Matrix $\quad 1 \times 3 -$ Matrix $\quad 3 \times 1 -$ Matrix

5.3.1 Operationen mit Matrizen

Addition zweier $\mathbf{m \times n}$ - Matrizen

Definition.

Es seien $A = \big(a_{ij}\big)$ und $B = \big(b_{ij}\big)$ zwei $m \times n$ - Matrizen; dann versteht man unter der Summe $A + B$ die $m \times n$ - Matrix, die wie folgt definiert ist:

$$A + B = \big(a_{ij} + b_{ij}\big)$$

Beispiel. Gegeben seien $A = \begin{pmatrix} 1 & 2 \\ -2 & 3 \end{pmatrix}$ und $B = \begin{pmatrix} -2 & 5 \\ 1 & 0 \end{pmatrix}$. Es folgt:

$$A + B = \begin{pmatrix} -1 & 7 \\ -1 & 3 \end{pmatrix}.$$

Multiplikation einer Matrix mit $\alpha \in \mathbb{R}$ („Skalare Multiplikation“)

Definition.
Es sei $A = (a_{ij})$ und $\alpha \in \mathbb{R}$. Dann versteht man unter αA die Matrix, die wie folgt definiert ist:

$$\alpha A = (\alpha \cdot a_{ij})$$

Beispiel. Gegeben seien $A = \begin{pmatrix} 1 & 2 \\ -2 & 3 \end{pmatrix}$ und $\alpha = -4$. Es folgt:

$$\alpha A = \begin{pmatrix} -4 & -8 \\ 8 & -12 \end{pmatrix}.$$

Multiplikation einer $\mathbf{m \times n}$ - Matrix mit einer $\mathbf{n \times p}$ - Matrix („Matrizenmultiplikation“)

Definition.
Es sei $A = (a_{ik})$ eine $m \times n$ - Matrix und $B = (b_{kj})$ sei eine $n \times p$ - Matrix. Dann versteht man unter dem Produkt AB die folgende $m \times p$ - Matrix $C = (c_{ij})$:

$$AB = C = (c_{ij}) \quad \text{mit} \quad c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$$

Beispiele:

1. Gegeben seien die Matrizen $A = \begin{pmatrix} 4 & 2 & 3 & 1 \\ 2 & 5 & -2 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 3 & 3 \\ 1 & -1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$.

   Dann folgt:

$$\begin{aligned} AB &= \begin{pmatrix} 4 & 2 & 3 & 1 \\ 2 & 5 & -2 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 3 \\ 1 & -1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 12+2+3+0 & 12-2+0+1 \\ 6+5-2+0 & 6-5+0+0 \\ 3+0+1+0 & 3+0+0+0 \end{pmatrix} \\ &= \begin{pmatrix} 17 & 11 \\ 9 & 1 \\ 4 & 3 \end{pmatrix} \end{aligned}$$

   Das Produkt BA ist nicht definiert, da die Zahl der Spalten von B verschieden von der Zahl der Zeilen von A ist.

2. Gegeben seien die Matrizen $A = \begin{pmatrix} 1 & 3 \\ -2 & 5 \end{pmatrix}$ und $B = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$.

   Dann folgt:

$$\begin{aligned} AB &= \begin{pmatrix} 1 & 3 \\ -2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1+0 & 2+9 \\ -2+0 & -4+15 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 11 \\ -2 & 11 \end{pmatrix} \\ BA &= \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 \\ -2 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1-4 & 3+10 \\ 0-6 & 0+15 \end{pmatrix} \\ &= \begin{pmatrix} -3 & 13 \\ -6 & 15 \end{pmatrix} \end{aligned}$$

   An $AB \neq BA$ erkennt man, dass die Matrizenmultiplikation nicht kommutativ ist.

3. Gegeben seien die Matrizen $A = \begin{pmatrix} 4 & 2 & 3 & 1 \\ 2 & 5 & -2 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 2 \\ 0 \\ 1 \\ 1 \end{pmatrix}$.

   Dann folgt:

$$\begin{aligned} AB &= \begin{pmatrix} 4 & 2 & 3 & 1 \\ 2 & 5 & -2 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 0 \\ 1 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 12 \\ 2 \\ 3 \end{pmatrix} \end{aligned}$$

4. Gegeben seien die Matrizen $A = \begin{pmatrix} 2 & 3 & -1 & 9 \end{pmatrix}$ und $B = \begin{pmatrix} 1 \\ 2 \\ 3 \\ -1 \end{pmatrix}$.

   Dann folgt:

$$\begin{aligned} AB &= \begin{pmatrix} 2 & 3 & -1 & 9 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \\ -1 \end{pmatrix} \\ &= \begin{pmatrix} 2+6-3-9 \end{pmatrix} \\ &= \begin{pmatrix} -4 \end{pmatrix} \end{aligned}$$

5. Gegeben seien die Matrizen $A = \begin{pmatrix} 1 & 3 & 7 \\ 4 & 5 & 6 \\ 1 & 1 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Dann folgt:

$$\begin{aligned} AB &= \begin{pmatrix} 1 & 3 & 7 \\ 4 & 5 & 6 \\ 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3 & 7 \\ 4 & 5 & 6 \\ 1 & 1 & 0 \end{pmatrix} \\ &= A \end{aligned}$$

Ebenso gilt $BA = B$.

Definition.
Die $n \times n$ - Matrix $E_n = (\delta_{ij})$ sei definiert durch

$$\delta_{ij} = \begin{cases} 1 & \text{, falls } i = j \\ 0 & \text{, falls } i \neq j \end{cases}$$

Die Matrix E_n hat also in der Hauptdiagonalen lauter Einsen und sonst lauter Nullen als Einträge.
Beispiel:

$$E_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Man nennt E_n die (n-reihige) *Einheitsmatrix*. Eine Matrix mit lauter Nullen nennen wir *Nullmatrix*. Eine Nullmatrix werden wir meistens mit 0 bezeichnen.

Transponieren einer Matrix

Definition.
Ist $A = (a_{ij})$ eine $m \times n$ - Matrix, so versteht man unter der *transponierten Matrix* A^T die $n \times m$ - Matrix, die gegeben ist durch

$$A^T = (b_{ij}) \quad \text{mit} \quad b_{ij} = a_{ji}.$$

Beispiele:

A	A^T
$\begin{pmatrix} 2 & 3 & 4 \\ 1 & 6 & 7 \\ 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 & 1 & 4 \\ 3 & 6 & 2 & 5 \\ 4 & 7 & 3 & 6 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 & 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 2 \\ 0 \\ -1 \end{pmatrix}$
$\begin{pmatrix} 1 \\ 5 \\ 2 \\ 6 \end{pmatrix}$	$\begin{pmatrix} 1 & 5 & 2 & 6 \end{pmatrix}$

5.3.2 Regeln für das Rechnen mit Matrizen

Für das Rechnen mit Matrizen gelten die folgenden Regeln:

Regeln für die Addition von Matrizen

Es seien A, B und C $m \times n$ - Matrizen; mit 0 sei die $m \times n$ - Matrix mit lauter Nullen bezeichnet („Nullmatrix“); für $A = \big(a_{ij}\big)$ sei mit $-A$ die Matrix $\big(-a_{ij}\big)$ bezeichnet.

Dann gelten die folgenden Regeln:

(I.1) $A + \big(B + C\big) = \big(A + B\big) + C$

(I.2) $A + 0 = A$

(I.3) $A + \big(-A\big) = 0$

(I.4) $A + B = B + A$

Regeln für die skalare Multiplikation

Es seien A und B $m \times n$ - Matrizen und $\alpha, \beta \in \mathbb{R}$.

Dann gelten die folgenden Regeln:

(II.1) $\alpha\big(A + B\big) = \alpha A + \alpha B$

(II.2) $\big(\alpha + \beta\big)A = \alpha A + \beta A$

(II.3) $\big(\alpha\beta\big)A = \alpha\big(\beta A\big)$

(II.4) $1A = A$

Regeln für die Matrizenmultiplikation

Es seien A, A_1 und A_2 $m \times n$ - Matrizen, B, B_1 und B_2 seien $n \times p$ - Matrizen, C sei eine $p \times q$ - Matrix und α sei eine reelle Zahl.

Dann gelten die folgende Regeln:

(III.1) $A\big(B_1 + B_2\big) = AB_1 + AB_2$

(III.2) $\big(A_1 + A_2\big)B = A_1B + A_2B$

(III.3) $A\big(BC\big) = \big(AB\big)C$

(III.4) $A\big(\alpha B\big) = \big(\alpha A\big)B = \alpha\big(AB\big)$

Ist A eine $n \times n$ - Matrix und E_n die n-reihige Einheitsmatrix, so gilt:

(III.5) $AE_n = E_nA = A$

Regeln für die Transposition

Es sei A eine $m \times n$ - Matrix und $\alpha \in \mathbb{R}$.

Dann gelten die folgenden Regeln:

(IV.1) $\big(A^T\big)^T = A$

(IV.2) $\big(\alpha A\big)^T = \alpha A^T$

(IV.3) $\big(A + B\big)^T = A^T + B^T$ für eine $m \times n$ - Matrix B

(IV.4) $\big(A \cdot B\big)^T = B^T \cdot A^T$ für eine $n \times p$ - Matrix B

Alle diese Regeln folgen mehr oder weniger direkt aus den Definitionen. Wir führen dies exemplarisch für Regel (III.2) durch.

Beweis von Regel (III.2)

Es sei

$$A_1 = (a_{ij})_{\substack{i=1,\dots,m\\ j=1,\dots,n}},\ A_2 = (a'_{ij})_{\substack{i=1,\dots,m\\ j=1,\dots,n}},\ B = (b_{jk})_{\substack{j=1,\dots,n\\ k=1,\dots,p}}.$$

Dann gilt

$$A_1 + A_2 = (a_{ij} + a'_{ij})_{\substack{i=1,\dots,m\\ j=1,\dots,n}}.$$

Es folgt:

$$\begin{aligned}
(A_1 + A_2)B &= \left(\sum_{j=1}^{n}(a_{ij} + a'_{ij})b_{jk}\right)_{\substack{i=1,\dots,m\\ k=1,\dots,p}} \\
&= \left(\sum_{j=1}^{n}(a_{ij}b_{jk} + a'_{ij}b_{jk})\right)_{\substack{i=1,\dots,m\\ k=1,\dots,p}} \\
&= \left(\sum_{j=1}^{n}(a_{ij}b_{jk}) + \sum_{j=1}^{n}(a'_{ij}b_{jk})\right)_{\substack{i=1,\dots,m\\ k=1,\dots,p}} \\
&= \left(\sum_{j=1}^{n}a_{ij}b_{jk}\right)_{\substack{i=1,\dots,m\\ k=1,\dots,p}} + \left(\sum_{j=1}^{n}a'_{ij}b_{jk}\right)_{\substack{i=1,\dots,m\\ k=1,\dots,p}} \\
&= A_1B + A_2B. \ \square
\end{aligned}$$

Wir weisen abschließend auf eine Verallgemeinerung hin: Alle Aussagen dieses Abschnitts bleiben gültig, wenn man anstelle von $\mathbb{R}$ einen beliebigen Körper K (beispielsweise $\mathbb{Q}$ oder $\mathbb{Z}_2$) zugrunde legt; die Aussagen bleiben sogar für einen beliebigen Ring R (wie beispielsweise $\mathbb{Z}$ oder $\mathbb{Z}_m$) gültig.

Das bedeutet: Man betrachtet Matrizen $A = (a_{ij})$ mit Einträgen a_{ij} aus K (bzw. R) und man definiert die skalare Multiplikation aA für Elemente $a \in K$ (bzw. $a \in R$), etc.

Bei einem Ring handelt es sich um eine algebraische Struktur, die etwas schwächer als die algebraische Struktur eines Körpers ist, welche bereits in Abschnitt 2.2 behandelt wurde. Die genaue Definition eines Rings wird später in Abschnitt 7.1 gegeben.

6 Gruppen

Wir folgen in diesem Abschnitt teilweise dem Lehrbuch

Norman L. Biggs, *Discrete Mathematics*, Oxford University Press.

Als begleitende und ergänzende Literatur sei ferner empfohlen:

Angelika Steger, *Diskrete Strukturen*, Band 1 (Kombinatorik-Graphentheorie-Algebra), Springer-Verlag.

6.1 Der Begriff der algebraischen Struktur, Halbgruppen und Monoide

Zur Erinnerung: Unter einer *n-stelligen Verknüpfung* auf einer Menge M versteht man eine Abbildung $f : M^n \to M$ (für $n \in \mathbb{N}$) und statt „n-stellige Verknüpfung“ sagt man auch „n-stellige Operation“.

Es ist außerdem auch üblich, eine Abbildung $f : M^n \to M$ einen *n-stelligen Operator* auf M zu nennen; n heißt dann die *Stelligkeit* des Operators f.

Unter einer *algebraischen Struktur* versteht man eine (endliche oder unendliche) Menge $M \neq \varnothing$ zusammen mit einer endlichen Anzahl von Operatoren $f_1, \ldots, f_t$ auf M. Häufig wird eine algebraische Struktur auch in der Form eines $(t+1)$-Tupels aufgeschrieben:

$$\big(M, f_1, \ldots, f_t\big).$$

Man nennt M die *Grundmenge* der algebraischen Struktur.

Die Operatoren $f_1, \ldots, f_t$ können dabei durchaus auch unterschiedliche Stelligkeit haben. Beispielsweise könnte es sein, dass

- f_1 ein 3-stelliger Operator ist (d.h. $f_1 : M^3 \to M$),
- f_2 ein 1-stelliger Operator ist (d.h. $f_2 : M \to M$),
- alle weiteren Operatoren $f_3, \ldots, f_t$ binär sind (d.h. $f_i : M^2 \to M$ für $i = 3, \ldots, t$).

Statt „algebraische Struktur“ sagt man häufig auch *universelle Algebra* oder einfach nur *Algebra*. Wenn Sie also irgendwann einmal (beispielsweise in einem Informatiklehrbuch) lesen, „es sei $(M, f_1, \ldots, f_t)$ eine Algebra“, dann wissen Sie, was das bedeutet.

Wir werden hier den Ausdruck „algebraische Struktur“ bevorzugen, werden aber hin und wieder auch einfach „Algebra“ sagen.

Beispiele:

1. Es seien $+$ und $\cdot$ die üblichen arithmetischen Operationen auf $\mathbb{Z}$; wir definieren Operatoren f_1 und f_2 auf $\mathbb{Z}$ durch

$$\begin{aligned} f_1 \quad : \quad & \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ & (x, y) \mapsto x + y \end{aligned}$$

und

$$\begin{aligned} f_2 \quad : \quad & \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ & (x, y) \mapsto x \cdot y. \end{aligned}$$

Dann ist $(\mathbb{Z}, f_1, f_2)$ eine algebraische Struktur. In der Regel schreibt man anstelle von f_1 und f_2 hier einfach $+$ und $\cdot$, spricht also von der algebraischen Struktur $(\mathbb{Z}, +, \cdot)$.

2. Für $+$ und $\cdot$ wie in 1. kann man weitere algebraische Strukturen bilden; beispielsweise sind $(\mathbb{N}, +, \cdot)$, $(\mathbb{N}, +)$ und $(\mathbb{N}, \cdot)$ algebraische Strukturen. Sind $(M, +, \cdot)$, $(M, +)$ und $(M, \cdot)$ *für alle* Teilmengen $M \subseteq \mathbb{Z}$ algebraische Strukturen?

Die Antwort ist nein, da die Menge M ja *nicht immer abgeschlossen* bezüglich $+$ und $\cdot$ sein muss. Ist beispielsweise $M := \{x \in \mathbb{N} : x \text{ ist Quadratzahl}\}$, so ist $(M, +)$ keine algebraische Struktur, da es Elemente aus M gibt, deren Summe nicht in M liegt. (Beispielsweise gilt $1 \in M$, $4 \in M$ aber $1 + 4 = 5 \notin M$.)

3. Ist $M = \mathcal{P}(S)$ die Potenzmenge einer Menge S, so ist $(M, \cap, \cup, ^-)$ eine algebraische Struktur. Der dritte Operator ist dabei ein 1-stelliger Operator, nämlich die Komplementbildung. („Jedem $A \in \mathcal{P}(S)$ wird sein Komplement $\bar{A} = S \setminus A$ zugeordnet.“)

4. Jede Boolesche Algebra B (vgl. Seite 10) ist eine algebraische Struktur $(B, \sqcap, \sqcup, ^-)$; jeder Ring R (vgl. Seite 120) und damit auch jeder Körper stellt eine algebraische Struktur $(R, +, \cdot)$ dar.

5. Ist A eine beliebige Menge, so wollen wir mit $F(A)$ die Menge aller Abbildungen $f : A \to A$ bezeichnen; dann ist $(F(A), \circ)$ eine algebraische Struktur.

6. Ist $S(A) \subseteq F(A)$ die Menge aller bijektiven Abbildungen aus $F(A)$, so ist $(S(A), \circ)$ eine algebraische Struktur. (Wieso nämlich?)

Definition.
Es sei $(M, *)$ eine algebraische Struktur mit einem 2-stelligen Operator $*$. Ein Element $e \in M$ wird *neutrales Element* für den Operator $*$ genannt, falls

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

Zur Übung:

a) Man prüfe für die in den obigen Beispielen vorkommenden binären Operatoren, ob neutrale Elemente vorhanden sind.

b) Es sei $M = \{a, b, c\}$. Wir betrachten die Algebra $(M, *)$, wobei $*$ durch die folgende Tabelle definiert sei:

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

Es gilt hier also beispielsweise $a * c = b$.

Frage: Gibt es ein neutrales Element für $*$? Dieselbe Frage für folgende Tabelle:

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

Eine algebraische Struktur $(M, *)$ mit einem binären Operator $*$ kann ein neutrales Element enthalten oder auch nicht. Sicher ist nur: $(M, *)$ kann nie mehr als ein neutrales Element enthalten. Dies ist Gegenstand der folgenden Feststellung.

Feststellung 1.
Jede algebraische Struktur $(M, *)$ mit 2-stelliger Verknüpfung $*$ enthält höchstens ein neutrales Element.

Beweis. Es seien c und d neutrale Elemente. Der Beweis unserer Feststellung ist erbracht, wenn wir

$c = d$ zeigen. Da c ein neutrales Element ist, gilt $c * a = a$ *für alle* $a \in M$; also gilt insbesondere

$$c * d = d.$$

Da d ein neutrales Element ist, gilt $a * d = a$ für alle $a \in M$, also insbesondere auch

$$c * d = c.$$

Insgesamt haben wir $c = c * d = d$. □

Definition.
Sei $(M, *)$ eine algebraische Struktur mit 2-stelligem Operator $*$ und neutralem Element e. Ein Element $x \in M$ heißt *inverses Element* von $a \in M$, falls

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

Nicht jedes Element muss ein inverses Element besitzen. Man betrachte beispielsweise die Algebra $(\mathbb{Z}, \cdot)$; in dieser Algebra besitzt kein Element außer 1 und -1 ein inverses Element. (Wieso nämlich?)

Definition.

a) Es sei $(M, *)$ eine algebraische Struktur mit 2-stelligem Operator $*$. Gilt das *Assoziativgesetz*

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

so spricht man von einer *assoziativen Verknüpfung* $*$ und nennt $(M, *)$ eine *Halbgruppe*.

b) Eine Halbgruppe $(M, *)$ mit neutralem Element nennt man ein *Monoid*.

Liegt eine algebraische Struktur $(M, *)$ mit einem 2-stelligen Operator vor, so nennt man diese also genau dann ein *Monoid*, falls die folgenden Bedingungen gelten:

(M1) (*Assoziativität*): Für alle $a, b, c \in M$ gilt $a * (b * c) = (a * b) * c$.

(M2) (*Existenz eines neutralen Elements*): Es gibt ein Element $e \in M$, für das $e * a = a * e = a$ für alle $a \in M$ gilt.

Feststellung 2.
Ist $(M, *)$ ein Monoid, so besitzt jedes $a \in M$ höchstens ein inverses Element.

Beweis. Für ein $a \in M$ seien x und y inverse Elemente von a. Mit e sei das neutrale Element von $(M, *)$ bezeichnet. Da x und y inverse Elemente von a sind, gilt $x * a = e$ und $a * y = e$; da e neutrales Element ist, gilt $e * y = y$ und $x * e = x$. Es folgt

$$y = e * y = (x * a) * y \overset{(M1)}{=} x * (a * y) = x * e = x. \square$$

Ist ein Monoid $(M, *)$ gegeben und gehört a zu den Elementen von M, die bzgl. $*$ ein inverses Element besitzen, so können wir aufgrund von Feststellung 2 von *dem Inversen* von a sprechen.

Elemente, die in Bezug auf einen Operator $*$ ein inverses Element besitzen, nennt man auch *invertierbar* (bzgl. $*$).

Beispiele für Monoide:

1. $(\mathbb{Z}, \cdot)$ ist ein Monoid, da das Assoziativgesetz $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ gilt und da bzgl. $\cdot$ ein neutrales Element vorhanden ist, nämlich die 1. Welches sind in diesem Monoid die invertierbaren Elemente?
2. Wir betrachten $\mathbb{Z}_m$ für $m \geq 2$; mit $\cdot$ sei die Multiplikation modulo m bezeichnet. Dann ist $(\mathbb{Z}_m, \cdot)$ ebenfalls ein Monoid (vgl. Seite 82). Welche Elemente von $\mathbb{Z}_4$ sind invertierbar im Monoid $(\mathbb{Z}_4, \cdot)$? Zur Beantwortung dieser Frage kann man sich beispielsweise die Multiplikationstabelle für $\mathbb{Z}_4$ auf Seite 83 anschauen.

Allgemein: Welches sind die Elemente aus $\mathbb{Z}_m$, die bzgl. $\cdot$ ein Inverses besitzen und wie kann man, falls vorhanden, das Inverse finden? (Falls Sie es nicht mehr wissen: Schauen Sie in Abschnitt 5.1 nach!)

3. $(\mathbb{Z}, +)$ und $(\mathbb{Z}_m, +)$ sind ebenfalls Monoide. Was ist in diesen Monoiden das neutrale Element? Und welche Elemente sind invertierbar?

4. Für eine beliebige Menge A sei $F(A)$ die Menge aller Abbildungen $f : A \to A$. Dann ist $\big(F(A), \circ\big)$ ein Monoid, da die Hintereinanderausführung $\circ$ von Abbildungen assoziativ ist (es gilt immer $f \circ (g \circ h) = (f \circ g) \circ h$, vgl. Seite 61f) und da ein neutrales Element vorhanden ist. Welches Element ist dies und welche Elemente sind invertierbar?

5. Es sei $\Sigma = \big\{u, v, w\big\}$. Wir nennen Σ ein *Alphabet mit drei Elementen* und betrachten Zeichenfolgen, die man mit Hilfe von Σ bilden kann: $vwwuvv$ ist beispielsweise eine Zeichenfolge der Länge 6; uu, uv, uw, vu, vv, vw, wu, wv und ww sind die möglichen Zeichenfolgen der Länge 2.

Auch Zeichenfolgen der Länge 1 werden betrachtet: Dies sind die 3 Zeichenfolgen u, v und w. Darüber hinaus soll es auch noch eine Zeichenfolge der Länge 0 geben, die wir die leere Zeichenfolge nennen und mit ε bezeichnen wollen.

Statt „Zeichenfolge“ wollen wir im Folgenden *Wort* (der Länge n für $n \in \mathbb{N} \cup \big\{0\big\}$) sagen; ε heiße *leeres Wort*. Mit Σ^* sei die Menge aller Wörter (beliebiger Länge n für $n \in \mathbb{N} \cup \big\{0\big\}$) bezeichnet und $\circ$ bezeichne den Operator der *Konkatenation*, der aus zwei Wörtern x und y ein neues Wort $x \circ y$ erzeugt, indem y rechts an x angehängt wird; für das leere Wort ε gelte dabei $x \circ \varepsilon = \varepsilon \circ x = x$ für alle $x \in \Sigma^*$.

Beispiel: $x = vwu,\ y = www \Longrightarrow x \circ y = vwuwww,\ \varepsilon \circ x = x \circ \varepsilon = x = vwu.$

Dann ist $(\Sigma^*, \circ)$ ein Monoid, da offenbar das Assoziativgesetz $x \circ (y \circ z) = (x \circ y) \circ z$ gilt und da ε neutrales Element bzgl. $\circ$ ist.

Welche Elemente sind in diesem Beispiel invertierbar?

Das vorausgegangene Beispiel lässt sich ohne weiteres auf Fälle übertragen, in denen das zugrunde liegende Alphabet Σ eine andere Menge als $\big\{u, v, w\big\}$ ist. Dabei können auch unendliche Mengen Σ zugelassen werden, wobei die Wörter selbstverständlich nach wie vor endliche Länge haben sollen.

6. Es sei K ein Körper (also z.B. $\mathbb{R}$, $\mathbb{Q}$ oder $\mathbb{Z}_2$) und $M(n \times n, K)$ bezeichne die Menge aller $n \times n$ -Matrizen A über K. Mit $\cdot$ sei die übliche Matrizenmultiplikation bezeichnet. Dann ist $\big(M(n \times n, K), \cdot\big)$ ein Monoid, da die Matrizenmultiplikation assoziativ ist und da die Einheitsmatrix E_n ein neutrales Element bzgl. $\cdot$ ist.

Welche Elemente in diesem letzten Beispiel invertierbar sind und welche nicht, ist eine wichtige Frage, die später behandelt werden wird, wenn wir uns mit Vektor- und Matrizenrechnung befassen.

6.2 Die Gruppenaxiome und einführende Beispiele

In einem Monoid $(M, *)$ ist das neutrale Element e immer invertierbar. (Wieso eigentlich?) In Bezug auf die übrigen Elemente von M ist jedoch keine allgemeine Aussage möglich: Wie wir gesehen haben, kann es vorkommen, dass außer e keine weiteren Elemente invertierbar sind; es kann ebenfalls vorkommen, dass gewisse Elemente $\neq e$ invertierbar sind, andere aber nicht. Liegt dagegen der Fall vor, dass sämtliche Elemente von M invertierbar sind, so benutzt man wegen der besonderen Wichtigkeit dieses Falles einen eigenen Namen: Man spricht von einer *Gruppe*.

Was eine Gruppe ist, kann man dementsprechend auf zwei Arten sagen; entweder kurz und knapp: *Eine Gruppe ist ein Monoid, in dem jedes Element invertierbar ist.* Oder aber man führt wie im Folgenden alle Eigenschaften noch einmal explizit auf.

Definition.
Eine algebraische Struktur $(G, *)$ mit 2-stelligem Operator $*$ heißt eine *Gruppe*, falls Folgendes gilt:

(G1) (*Assoziativität*): Für alle $a, b, c \in G$ gilt $a * (b * c) = (a * b) * c$.

(G2) (*Existenz eines neutralen Elements*): Es gibt ein Element $e \in G$, für das $e * a = a * e = a$ für alle $a \in G$ gilt.

(G3) (*Existenz von inversen Elementen*): Zu jedem $a \in G$ gibt es ein $a' \in G$, für das $a * a' = a' * a = e$ gilt.

Wie wir bereits im vorhergehenden Abschnitt erkannt haben (Feststellungen 1 und 2), kann es außer e kein weiteres neutrales Element in G geben, und für jedes a ist a' das jeweils einzige Inverse.

Ist G eine Gruppe und ist $|G|$ endlich, so nennt man $|G|$ die *Ordnung* von G; eine Gruppe mit unendlich vielen Elementen wird eine Gruppe *von unendlicher Ordnung* genannt.

Man nennt (G1), (G2) und (G3) die *Gruppenaxiome*. Hin und wieder findet man als Gruppenaxiom zusätzlich aufgeführt, dass G *abgeschlossen* ist, dass also $a * b \in G$ für alle $a, b \in G$ gilt. Wir brauchen die Abgeschlossenheit hier nicht gesondert aufzuführen, da sie bereits in der Forderung, dass $(G, *)$ eine algebraische Struktur sein soll, enthalten ist.

Beispiele:

1. Für die übliche Addition ist $(\mathbb{Z}, +)$ eine Gruppe.

Begründung: (G1) gilt, da die übliche Addition assoziativ ist; (G2) gilt, da 0 neutrales Element bzgl. $+$ ist; (G3) ist ebenfalls erfüllt, da für das Negative $-a$ von a gilt: $a + (-a) = (-a) + a = 0$.

2. Mit $+$ und $\cdot$ seien die übliche Addition und Multiplikation bezeichnet. Wir fragen uns, ob $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ Gruppen sind.

Antwort: $(\mathbb{R}, +)$ ist aus ähnlichen Gründen wie $(\mathbb{Z}, +)$ eine Gruppe.
$(\mathbb{R}, \cdot)$ ist *keine* Gruppe, da 0 kein Inverses bzgl. $\cdot$ besitzt
$(\mathbb{R} \setminus \{0\}, \cdot)$ ist eine Gruppe. *Begründung*: (G1) gilt, da die übliche Multiplikation assoziativ ist; (G2) gilt, da 1 neutrales Element bzgl. $\cdot$ ist; (G3) gilt auch, da für $\frac{1}{a}$ gilt: $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$.

Analog erkennt man: $(\mathbb{Q}, +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot)$ sind Gruppen; $(\mathbb{Q}, \cdot)$ ist keine Gruppe.

3. Wie früher schon bezeichnen wir mit S_n die Menge aller Permutationen von $\{1, 2, \ldots, n\}$ und $\circ$ bezeichne die Nacheinanderausführung von Abbildungen. Dann ist

$$(S_n, \circ)$$

eine Gruppe; dies ist gerade der Inhalt von Feststellung 1, Seite 87. Man nennt $(S_n, \circ)$ die *symmetrische Gruppe*. Welche Ordnung hat diese Gruppe?

4. Für welche Werte von $m \geq 2$ handelt es sich um eine Gruppe? (Mit $+$ bzw. $\cdot$ sei hier die Addition bzw. Multiplikation modulo m bezeichnet; vgl. auch die Bemerkung zur Schreibweise auf Seite 85.)

(i) $(\mathbb{Z}_m, +)$

(ii) $(\mathbb{Z}_m, \cdot)$

(iii) $(\mathbb{Z}_m \setminus \{0\}, \cdot)$

Zu (i) und (ii): Schauen Sie sich Feststellung 1 auf Seite 82 an, sowie obiges Beispiel 2. Dann sollten Sie die Antwort selber finden!

Zu (iii): **1. Fall**: *m ist keine Primzahl.* In diesem Fall gibt es also ganze Zahlen a, b mit $1 \leq a, b \leq m$ und $a \cdot b = m$. Es folgt $a \cdot b \equiv 0 \pmod{m}$, d.h., es gibt zwei Elemente aus $\mathbb{Z}_m \setminus \{0\}$, deren Produkt nicht in $\mathbb{Z}_m \setminus \{0\}$ ist. $\mathbb{Z}_m \setminus \{0\}$ ist also *nicht einmal abgeschlossen* bzgl. $\cdot$ und daher auch *keine Gruppe*. (Eine andere Möglichkeit zu begründen, dass keine Gruppe vorliegt, ergibt sich aus Feststellung 3, Seite 84. Welche nämlich?)

2. Fall: *m ist eine Primzahl.* Dass (G1), (G2) und (G3) erfüllt sind, ergibt sich aus den Feststellungen 1 und 3 auf den Seiten 82 und 84. Steht damit fest, dass eine Gruppe vorliegt? Noch nicht ganz, denn

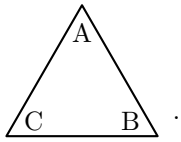
es könnte ja wie im 1. Fall die Abgeschlossenheit verletzt sein. Es bleibt also zu zeigen

$$a, b \in \mathbb{Z}_m \setminus \{0\} \Longrightarrow a \cdot b \in \mathbb{Z}_m \setminus \{0\}.$$

Wir weisen dies durch einen Widerspruchsbeweis nach: Angenommen, für $a, b \in \mathbb{Z}_m \setminus \{0\}$ gelte $a \cdot b \notin \mathbb{Z}_m \setminus \{0\}$. Es folgt $a \cdot b \equiv 0 \pmod{m}$, d.h., $m \mid (a \cdot b)$. Da m eine Primzahl ist, folgt $m \mid a$ oder $m \mid b$ (vgl. Seite 24), also $a \equiv 0 \pmod{m}$ oder $b \equiv 0 \pmod{m}$, im Widerspruch zu $a, b \in \mathbb{Z}_m \setminus \{0\}$.

Bei den obigen Beispielen 1 - 4 handelt es sich um *wichtige Standardbeispiele* von Gruppen; wirklich neu waren diese Beispiele allerdings nicht - deshalb konnten wir uns bei der Behandlung dieser Beispiele ja auch so oft auf bereits bewiesene Feststellungen berufen. Darüber hinaus gibt es aber eine Vielzahl weiterer Gruppen: Der Gruppenbegriff ist ein zentraler Begriff der Mathematik und in fast jedem Teilgebiet der Mathematik spielen Gruppen eine wichtige Rolle. Wir geben zunächst zwei weitere Beispiele an, die nicht untypisch sind, wobei die Darstellung an N. L. Biggs, Discrete Mathematics, Oxford University Press angelehnt ist.

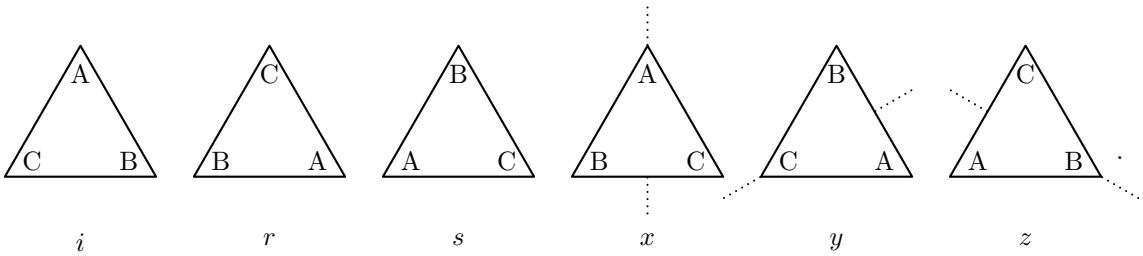
5. **Ein geometrisches Beispiel**: Wir betrachten ein gleichseitiges Dreieck, dessen Eckpunkte wir mit A, B und C bezeichnen:



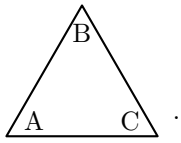
Darüber hinaus betrachten wir sechs *Symmetrietransformationen* der Ebene, die i, r, s, x, y und z genannt werden sollen:

i ist nichts weiter als die Identität, d.h., die Abbildung, die alle Punkte der Ebene fest lässt;
r ist eine Drehung der Ebene um den Mittelpunkt des Dreiecks, und zwar um 120° im Uhrzeigersinn;
s ist wie r, nur dass der Drehwinkel 240° beträgt;
x, y und z sind Spiegelungen der Ebene längs der unten in der Zeichnung angegebenen Achsen.

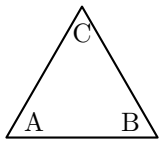
Alle diese Transformationen sind Abbildungen $\mathbb{R}^2 \longrightarrow \mathbb{R}^2$, die das Dreieck in sich selbst überführen. In der folgenden Zeichnung ist der Effekt dargestellt, den die einzelnen Transformationen auf die Eckpunkte des Dreiecks haben:



Führt man zwei der Transformationen nacheinander aus, so entsteht wiederum eine der sechs Transformationen: Führt man beispielsweise erst s und dann y aus, so erhält man z. Dies lässt sich am Effekt ablesen, den die Transformationen auf die Eckpunkte des Dreiecks haben: Nach Ausführung der Drehung s befindet sich das Dreieck in der folgenden Lage:



Spiegelt man jetzt noch zusätzlich an der Achse, die zu y gehört, so kommt das Dreieck in die Lage:



.

Man beachte dabei: Die Achsen, die jeweils zu x, y und z gehören, werden bei den Drehungen nicht mit bewegt, sondern sind fest. Insgesamt hat die Nacheinanderausführung von s und y also denselben Effekt wie z.

Für die Nacheinanderausführung von s und y schreiben wir $y * s$ (Man achte auf die Reihenfolge: $y * s$ bedeutet: „Zuerst wird s ausgeführt, danach wird y ausgeführt“.) Es gilt also

$$y * s = z.$$

Ähnlich findet man beispielsweise

$$x * s = y, r * z = x, r * s = i, x * x = i.$$

Insgesamt erhält man folgende Tabelle, die die Operation $*$ vollständig beschreibt:

	i	r	s	x	y	z
i	i	r	s	x	y	z
r	r	s	i	y	z	x
s	s	i	r	z	x	y
x	x	z	y	i	s	r
y	y	x	z	r	i	s
z	z	y	x	s	r	i

Es sei $G_\triangle = \{i, r, s, x, y, z\}$ die Menge unserer Symmetrietransformationen. Es ist nun einfach nachzuprüfen, dass es sich bei $(G_\triangle, *)$ um eine Gruppe handelt: (G1) gilt, da es sich bei den Elementen von $G_\triangle$ um Abbildungen der Menge der Punkte der Ebene auf sich selbst handelt und da die Nacheinanderausführung von Abbildungen assoziativ ist; neutrales Element ist natürlich i; die jeweiligen Inversen sind in der folgenden Tabelle angegeben:

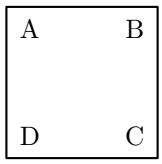
Element	i	r	s	x	y	z
Inverses	i	s	r	x	y	z

.

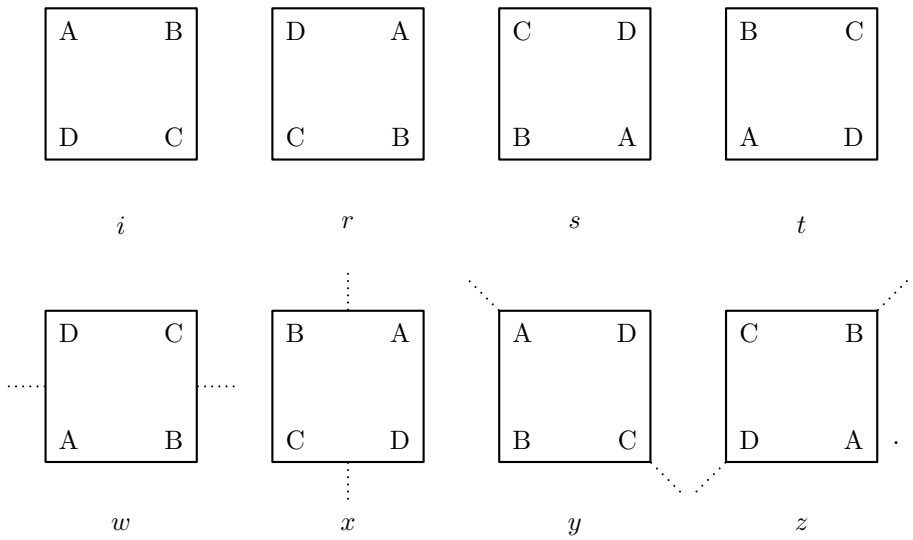
Wir wollen $G_\triangle$ (zusammen mit der Operation $*$) die *Dreiecksgruppe* nennen. Die obige Tabelle, die die Wirkung von $*$ vollständig beschreibt, nennt man die *Gruppentafel* von $G_\triangle$.

In ähnlicher Weise erhält man auch für andere geometrische Objekte zugehörige Gruppen. Wir deuten dies für die *Quadratgruppe* $G_\square$ an.

Man betrachtet ein Quadrat



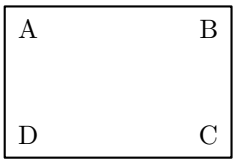
und die zugehörigen Symmetrietransformationen der Ebene, die wie folgt dargestellt werden können:



Zur Übung:

a) Man berechne $s * y$, $x * r$ sowie $x * y$ und gebe zu allen Elementen das Inverse an.

b) Entsprechend definiere man durch Betrachtung eines Rechtecks mit ungleichen Seitenlängen die *Rechteckgruppe* $G_{\square}$ und stelle die zugehörige Gruppentafel auf.



6. G_M sei die Menge der 2×2 - Matrizen der folgenden Form mit $\alpha, \beta \in \mathbb{Z}_3$ und $\alpha \neq 0$:

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}.$$

Behauptung: G_M ist eine Gruppe, wenn man als Operation die Matrizenmultiplikation wählt.

Bevor wir nachprüfen, ob (G1) - (G3) erfüllt sind, haben wir uns zunächst um die *Abgeschlossenheit* zu kümmern; d.h., wir müssen uns vergewissern, dass man die Menge G_M nicht verlässt, wenn man zwei Matrizen aus G_M miteinander multipliziert. Es seien also

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \text{ und } \begin{pmatrix} \gamma & \delta \\ 0 & 1 \end{pmatrix}$$

zwei Matrizen aus G_M, d.h., es gilt $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_3$ und $\alpha, \gamma \neq 0$. Es folgt

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha\gamma & \alpha\delta + \beta \\ 0 & 1 \end{pmatrix}.$$

Aus $\alpha, \gamma \neq 0$ folgt $\alpha\gamma \neq 0$. (Beachten Sie: Es liegt $\mathbb{Z}_3$ zugrunde und nicht etwa $\mathbb{Z}_4$ oder $\mathbb{Z}_6$! Man vergleiche hierzu auch obiges Beispiel 4 (iii).) Also ist die Abgeschlossenheit gegeben.

(G1) ist erfüllt, da die Matrizenmultiplikation assoziativ ist. (G2) ist erfüllt, da die Einheitsmatrix in G_M liegt. (Man wähle hierfür $\alpha = 1$ und $\beta = 0$.)

Zu (G3): Gegeben sei $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \in G_M$. Für ein mögliches Inverses $\begin{pmatrix} \gamma & \delta \\ 0 & 1 \end{pmatrix} \in G_M$ muss gelten:

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};$$

das bedeutet, dass $\alpha\gamma = 1$ und $\alpha\delta + \beta = 0$ gelten muss. Es folgt $\gamma = \alpha^{-1}$ und $\delta = \alpha^{-1}(-\beta)$. Folglich kann das Inverse von $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$ nur

$$\begin{pmatrix} \alpha^{-1} & \alpha^{-1}(-\beta) \\ 0 & 1 \end{pmatrix}$$

sein. Man rechnet leicht nach, dass tatsächlich gilt:

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & \alpha^{-1}(-\beta) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ und } \begin{pmatrix} \alpha^{-1} & \alpha^{-1}(-\beta) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

6.3 Einige Folgerungen aus den Gruppenaxiomen

Bislang hatten wir in Gruppen die Operation meist mit $*$, das neutrale Element mit e und das Inverse von a mit a' bezeichnet. Wir steigen nun auf die sogenannte *multiplikative Schreibweise* um, d.h., anstelle von $*$ benutzen wir den Malpunkt $\cdot$, den man wie üblich aber auch weglassen kann. Anstelle von $a * b$ schreiben wir also $a \cdot b$ bzw. ab. Ferner: Anstelle von e schreiben wir 1 und anstelle von a' benutzen wir die Schreibweise a^{-1}. Zusammengefasst

- $a * b$ wird $a \cdot b$ oder ab,
- e wird 1,
- a' wird a^{-1}.

Aufgrund der Gruppenaxiome (G1) - (G3) gilt dann in der neuen Schreibweise:

- $a(bc) = (ab)c$,
- $1a = a1 = a$,
- $aa^{-1} = a^{-1}a = 1$.

Die multiplikative Schreibweise, die wir ab jetzt meistens verwenden werden, hat den Vorteil, kurz, knapp und in Rechnungen gut handhabbar zu sein; deshalb ist sie auch die allgemein übliche Schreibweise. Ein Nachteil oder besser gesagt eine *Gefahr* besteht allerdings darin, dass sie leicht mit der normalen Multiplikation von Zahlen verwechselt werden kann. Vor allem sollte man eins beachten: *Längst nicht jede Rechenregel für das Multiplizieren für Zahlen ist auch für Gruppen richtig.* Beispielsweise gilt für Zahlen das Kommutativgesetz $ab = ba$; in Gruppen braucht es aber nicht unbedingt zu gelten: Der Gruppentafel für die Dreiecksgruppe entnimmt man beispielsweise, dass

$$s * x \neq x * s$$

gilt, und das ändert sich natürlich nicht dadurch, dass man zur multiplikativen Schreibweise übergeht.

Gilt für ein gewisses Paar $a, b \in G$ aber doch $ab = ba$, so sagt man, dass a und b *kommutieren*. Eine Gruppe G, in der alle Elemente kommutieren, nennt man *kommutativ* oder *abelsch*.

Satz 1.
Es seien x, y, z, a und b irgendwelche Elemente einer Gruppe G. Dann gilt

(i) $xy = xz \Rightarrow y = z$ (*linksseitige Kürzregel*),

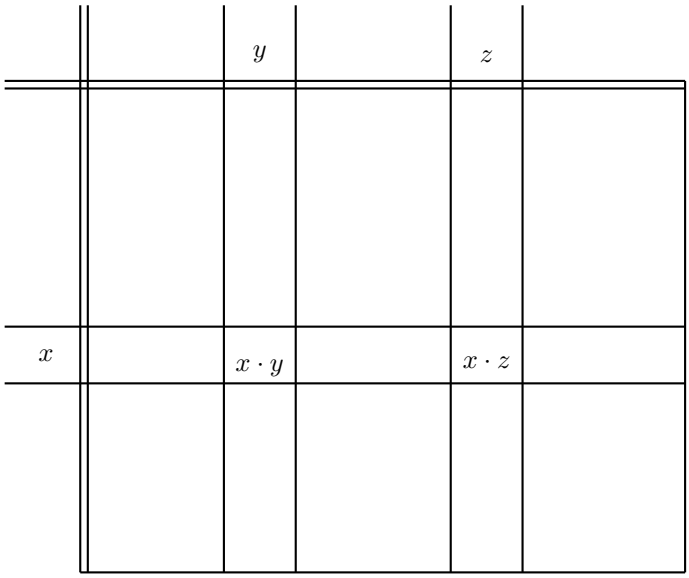
(ii) $ax = bx \Rightarrow a = b$ (*rechtsseitige Kürzregel*).

Beweis von (i). $xy = xz \Rightarrow x^{-1}(xy) = x^{-1}(xz) \overset{(G1)}{\Rightarrow} (x^{-1}x)y = (x^{-1}x)z \overset{(G3)}{\Rightarrow} 1y = 1z \overset{(G2)}{\Rightarrow} y = z$.
Der Beweis von (ii) geht entsprechend. □

Wir haben im Beweis von Satz 1 nur das verwenden können, was in den Axiomen steht. Beim Beweis weiterer Sätze sind wir schon etwas besser dran: Wir können das, was in den Axiomen steht benutzen *und den soeben bewiesenen Satz 1.*

Bevor wir zu Satz 2 kommen, wollen wir uns aber noch anschauen, welche Bedeutung die Kürzregeln für die *Gruppentafel* einer endlichen Gruppe G haben; es gelte $|G| = n$.

Die linksseitige Kürzregel besagt, dass man in jeder Zeile n verschiedene Einträge antrifft (*Erläuterung*: Dass in einer Zeile an zwei verschiedenen Stellen derselbe Eintrag zu finden ist, bedeutet, dass es x, y und z mit $y \neq z$ und $xy = xz$ gibt (vgl. Skizze); genau das wird aber durch die linksseitige Kürzregel ausgeschlossen.)



Entsprechend sagt die rechtsseitige Kürzregel aus, dass in jeder Spalte n unterschiedliche Einträge anzutreffen sind.

Satz 2.
Es seien a, b Elemente der Gruppe G. Dann besitzt die Gleichung

$$ax = b$$

eine eindeutige Lösung in G.

Beweis. Wir haben zwei Dinge zu zeigen: Eine *Existenzaussage* („Es gibt eine Lösung“) und eine *Eindeutigkeitsaussage* („Es kann nicht zwei verschiedene Lösungen geben“)

Nachweis der Eindeutigkeit: $ax_1 = b, ax_2 = b \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$ (nach Satz 1).

Nachweis der Existenz: Das Element $a^{-1}b$ ist eine Lösung von $ax = b$, da

$$a(a^{-1}b) \overset{(G1)}{=} (aa^{-1})b \overset{(G3)}{=} 1b \overset{(G2)}{=} b. \square$$

Für den *Spezialfall* $a = b$ besagt Satz 2, dass die Gleichung $ax = a$ genau eine Lösung hat. (Diese Lösung ist aufgrund von (G2) natürlich das neutrale Element 1 und wir haben insbesondere noch einmal bestätigt, dass das neutrale Element eindeutig bestimmt ist; als eine Feststellung über Monoide war uns dies allerdings bereits bekannt.)

Für den *Spezialfall* $b = 1$ besagt Satz 2, dass die Gleichung $ax = 1$ genau eine Lösung hat. (Diese Lösung ist aufgrund von (G3) natürlich das Element a^{-1}. Insbesondere haben wir noch einmal bestätigt, dass zu jedem Element das Inverse eindeutig bestimmt ist; auch dies war uns bereits bekannt, vgl. Feststellung 2 in Abschnitt 6.1)

6.4 Die Ordnung eines Gruppenelements

Gegeben sei eine Gruppe G. Dann kann man für jedes $a \in G$ und $n \in \mathbb{N}$ Potenzen a^n wie folgt rekursiv definieren:

$$a^1 := a \text{ und } a^n := aa^{n-1} \text{ für } n \geq 2.$$

Außerdem definiert man:

$$a^0 := 1.$$

Potenzen mit negativem Exponenten werden wie folgt definiert: Was a^{-1} bedeutet, ist bereits definiert, und für $n \geq 2$ definiert man:

$$a^{-n} := (a^{-1})^n.$$

Es gelten die folgenden *Potenzregeln*, auf deren Beweis verzichtet werden soll:

$$\boxed{a^m a^n = a^{m+n},\ (a^m)^n = a^{mn} \text{ für alle } m, n \in \mathbb{Z}.}$$

Wir werden von diesen beiden Potenzregeln häufig Gebrauch machen, meistens jedoch ohne diese ausdrücklich zu erwähnen.

Ist G eine *endliche* Gruppe und $a \in G$, so können die Elemente

$$a^1,\ a^2,\ a^3,\ a^4,\ \ldots$$

nicht alle verschieden sein: Es muss Potenzen a^k und a^ℓ mit $k < \ell$ geben, für die $a^\ell = a^k$ gilt. Durch Multiplikation mit a^{-k} auf beiden Seiten folgt dann (mit Hilfe der ersten Potenzregel) $a^{\ell-k} = a^0 = 1$. Dies zeigt, dass es in einer endlichen Gruppe zu jedem $a \in G$ ein $m \geq 1$ gibt mit $a^m = 1$. Damit gibt es auch eine *kleinste* Zahl $m \geq 1$ mit dieser Eigenschaft. Dies führt zu folgender Definition.

Definition.

a) Wenn G eine endliche Gruppe ist, so gibt es für jedes $a \in G$ ein kleinstes $m \geq 1$, für das

$$a^m = 1$$

gilt. Man nennt dieses $m \in \mathbb{N}$ die *Ordnung von* a in G.

b) Wenn G eine unendliche Gruppe ist, so definiert man die Ordnung m von a in G wie zuvor, vorausgesetzt, dass ein $m \geq 1$ mit $a^m = 1$ überhaupt existiert. Existiert ein solches m für ein a nicht, so sagt man, dass a *unendliche Ordnung* hat.

Beispiele:

1. In $G_\triangle$ gilt

$$r^1 = r,\ r^2 = s,\ r^3 = i.$$

Da i das neutrale Element von $G_\triangle$ ist, folgt, dass r die Ordnung 3 hat. Welche Ordnungen haben die übrigen Elemente von $G_\triangle$?

2. Wir bestimmen die Ordnung der Elemente 2 und 3 in $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$:

$$2^1 = 2,\ 2^2 = 2 \cdot 2 = 4,\ 2^3 = 2 \cdot 2^2 = 2 \cdot 4 = 1, \text{ also hat 2 die Ordnung 3;}$$

$$3^1 = 3,\ 3^2 = 3 \cdot 3 = 2,\ 3^3 = 3 \cdot 3^2 = 3 \cdot 2 = 6,$$
$$3^4 = 3 \cdot 3^3 = 3 \cdot 6 = 4,\ 3^5 = 3 \cdot 3^4 = 3 \cdot 4 = 5,$$
$$3^6 = 3 \cdot 3^5 = 3 \cdot 5 = 1, \text{ also hat 3 die Ordnung 6.}$$

3. Wir betrachten die symmetrische Gruppe S_6 und fragen nach der Ordnung der Permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 2 & 4 \end{pmatrix}$.

Es gilt

$$\begin{aligned} \pi^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 6 & 5 \end{pmatrix}, \\ \pi^3 = \pi\pi^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 4 & 2 \end{pmatrix}, \\ \pi^4 = \pi\pi^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = id. \end{aligned}$$

Also hat π die Ordnung 4.

4. Wir betrachten das Beispiel 6 aus Abschnitt 6.2: G_M sei die Menge der 2×2 - Matrizen der Form $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$ mit $\alpha, \beta \in \mathbb{Z}_3,\ \alpha \neq 0$. Wir bestimmen die Ordnung der Matrix $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$.

Es gilt

$$A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ und } A^3 = AA^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Da die Einheitsmatrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ das neutrale Element bzgl. der Matrizenmultiplikation ist, folgt, dass A die Ordnung 3 hat.

5. In $(\mathbb{Z}, +)$ ist es unüblich, auf die multiplikative Schreibweise umzusteigen, da es in $\mathbb{Z}$ ja schon die gewöhnliche Multiplikation gibt. Es bleibt hier also bei dem Operator $+$, 0 ist das neutrale Element bzgl. $+$ und $-a$ ist bzgl. $+$ das Inverse von a.

Frage: Welche Ordnung hat das Element 1 in $(\mathbb{Z}, +)$?

Antwort: 1 hat in $(\mathbb{Z}, +)$ unendliche Ordnung. Denn: In $(\mathbb{Z}, +)$ gilt $1 \neq 0$, $1 + 1 \neq 0$, $1 + 1 + 1 \neq 0$, $1 + 1 + 1 + 1 \neq 0$, ... Wir können 1 addieren soviel wir wollen, niemals erreichen wir das neutrale Element 0 der Addition.

6. Man überlege sich, welche Ordnungen die Elemente 1, -1 und 2 in $(\mathbb{Q} \setminus \{0\}, \cdot)$ haben.

Ist a ein Element der Gruppe G, das in G endliche Ordnung m hat, so wissen wir, dass

$$a^s \neq 1 \ (1 \leq s \leq m-1) \text{ und } a^m = 1.$$

Außerdem gilt natürlich $a^0 = 1$. Für Potenzen a^s mit $s > m$ und für Potenzen a^s mit negativem Exponenten wissen wir aber noch nicht, wann $a^s = 1$ gilt. Der folgende Satz gibt hierüber Auskunft.

Satz 3.
Es sei G eine Gruppe und $a \in G$ sei ein Element der Ordnung $m \in \mathbb{N}$. Dann gilt für jedes $s \in \mathbb{Z}$:

$$a^s = 1 \Leftrightarrow m \mid s.$$

Beweis. Wir haben zwei Dinge nachzuweisen:

(i) $m \mid s \Rightarrow a^s = 1$,

(ii) $a^s = 1 \Rightarrow m \mid s$.

(i) Falls $m \mid s$, so gibt es ein $k \in \mathbb{Z}$ mit $s = mk$. Es folgt

$$a^s = a^{mk} = (a^m)^k = 1^k = 1.$$

(ii) Es gelte nun $a^s = 1$. Es gibt $q, r \in \mathbb{Z}$ mit $0 \leq r < m$, so dass $s = qm + r$ („Zerlegung mit Rest“). Es folgt

$$1 = a^s = a^{qm+r} = a^{mq+r} = (a^m)^q a^r = a^r,$$

wobei die letzte Gleichung wegen $a^m = 1$ gilt.

Wir haben also $a^r = 1$ für ein r mit $0 \leq r < m$ gefunden. Da m als Ordnung von a die *kleinste* natürliche Zahl ist, für die $a^m = 1$ gilt, muss $r = 0$ sein. Es folgt $s = qm$, d.h., $m \mid s$. □

6.5 Isomorphie von Gruppen

Wir betrachten noch einmal die Beispiele 5 und 6 aus Abschnitt 6.2:
$G_\triangle = \{i, r, s, x, y, z\}$ war das geometrische Beispiel der Dreiecksgruppe, G_M war die Menge der 2×2 - Matrizen der Form $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$, wobei $\alpha, \beta \in \mathbb{Z}_3,\ \alpha \neq 0$. Man findet, dass G_M sechs Elemente enthält, denen wir die Namen I, R, S, X, Y und Z geben wollen:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad R = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

$$X = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \quad Z = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}.$$

Stellt man die Gruppentafel für G_M auf, so erhält man:

	I	R	S	X	Y	Z
I	I	R	S	X	Y	Z
R	R	S	I	Y	Z	X
S	S	I	R	Z	X	Y
X	X	Z	Y	I	S	R
Y	Y	X	Z	R	I	S
Z	Z	Y	X	S	R	I

Gruppentafel für G_M

Vergleicht man die obige Gruppentafel für G_M mit der Gruppentafel für $G_\triangle$ aus Abschnitt 6.2, so erkennt man, dass es sich *im Wesentlichen um dieselbe Gruppentafel* handelt: Die Wahl der Bezeichnungen I, R, S, Y, X und Z für die Matrizen aus G_M wurde gerade so vorgenommen, dass dies besonders deutlich wird. Man sagt, dass es sich bei $G_\triangle$ und G_M um *isomorphe Gruppen* handelt.

Allgemein nennt man zwei endliche Gruppen G_1 und G_2 *isomorph* (oder *strukturgleich*), wenn es möglich ist, die Reihenfolge ihrer Elemente so zu wählen, dass (bis auf die Bezeichnungen) gleiche Gruppentafeln entstehen. Dabei ist es natürlich nicht erforderlich, dass man wie in den obigen Beispielen kleine und große Buchstaben verwendet, sondern worauf es ankommt ist, dass es eine bijektive Abbildung

$$\beta : G_1 \longrightarrow G_2$$

zwischen den Elementen von G_1 und G_2 gibt, für die gilt: Führt innerhalb von G_1 die Multiplikation von a und b zum Ergebnis c, so führt in G_2 die Multiplikation von $\beta(a)$ und $\beta(b)$ zum Ergebnis $\beta(c)$. Es soll also für alle $a, b, c \in G_1$ gelten

$$ab = c \Longrightarrow \beta(a)\beta(b) = \beta(c).$$

Dasselbe (nur etwas kompakter ausgedrückt): Es soll für alle $a, b \in G_1$ gelten:

$$\beta(ab) = \beta(a)\beta(b).$$

Damit sind wir bei der üblichen Definition des Begriffs „isomorph“ angelangt, in der der Begriff der Gruppentafel nicht mehr auftaucht und die deshalb insbesondere auch für unendliche Gruppen brauchbar ist. (Die zunächst gegebene Definition von „isomorph“ ist für endliche Gruppen gleichbedeutend zur nachfolgenden; „Bijektion“ ist ein anderer Ausdruck für „bijektive Abbildung“.)

Definition.
Zwei Gruppen G_1 und G_2 (beide in multiplikativer Schreibweise) heißen *isomorph*, falls es eine Bijektion $\beta : G_1 \to G_2$ gibt, so dass für alle $a, b \in G_1$ gilt:

$$\beta(ab) = \beta(a)\beta(b). \tag{6.1}$$

Sind zwei Gruppen G_1 und G_2 isomorph, so schreiben wir $G_1 \cong G_2$; eine zugehörige Bijektion $\beta : G_1 \to G_2$, für die (6.1) gilt, nennt man einen *Isomorphismus*. Liegen die Gruppen nicht in multiplikativer Schreibweise vor, so definiert man ganz entsprechend, was „isomorph“ bedeutet; haben wir es etwa mit den Gruppen $(G_1, *)$ und $(G_2, \Diamond)$ zu tun, so lautet die (6.1) entsprechende Bedingung

$$\beta(a * b) = \beta(a) \Diamond \beta(b).$$

6.6 Zyklische Gruppen

Definition.
Eine Gruppe G heißt *zyklisch*, falls sie ein Element a enthält, für das gilt: Jedes Element x aus G ist eine Potenz von a. Mit anderen Worten: Für jedes $x \in G$ gibt es ein $k \in \mathbb{Z}$, so dass $x = a^k$ (also beispielsweise $x = a^3$, $x = a^5$ oder $x = a^{-7}$) gilt. Man sagt dann a *erzeugt* G (oder a ist ein *Erzeuger* von G) und schreibt

$$G = \langle a \rangle.$$

1. Fall: a erzeugt G und alle Potenzen von a sind verschieden. In diesem Fall gilt

$$G = \left\{ \ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, \ldots \right\};$$

G ist also eine *unendliche zyklische Gruppe*; unter allen Gruppen von diesem Typ wählen wir eine aus, die wir mit

$$C_\infty$$

bezeichnen wollen; für C_∞ verwenden wir, wenn nichts anderes gesagt ist, multiplikative Schreibweise. (Als C_∞ könnte man beispielsweise die folgende Gruppe $G \subseteq \mathbb{Q}$ nehmen: $G := \left\{ 2^n : n \in \mathbb{Z} \right\}$ mit der gewöhnlichen Multiplikation in $\mathbb{Q}$.)

Behauptung: Die altbekannte Gruppe $(\mathbb{Z}, +)$ fällt unter Fall 1; sie ist damit also eine unendliche zyklische Gruppe.

Zum Nachweis dieser Behauptung zeigen wir, dass $(\mathbb{Z}, +)$ isomorph zu C_∞ ist. Es sei a ein Erzeuger von C_∞, also $C_\infty = \langle a \rangle$. Wir definieren die Abbildung $\beta : \mathbb{Z} \to C_\infty$ durch

$$\beta(n) = a^n \ (n \in \mathbb{Z}).$$

Da alle Potenzen von a verschieden sind und $C_\infty = \langle a \rangle$ gilt, ist β eine Bijektion. Ferner gilt aufgrund der Potenzregeln:

$$\beta(n + m) = a^{n+m} = a^n a^m = \beta(n)\beta(m),$$

d.h., β ist ein Isomorphismus. □

2. Fall: a erzeugt G und *nicht alle Potenzen von a sind verschieden.*

In diesem Fall gibt es also $k, \ell \in \mathbb{Z},\ k < \ell$ mit $a^\ell = a^k$. Multipliziert man auf beiden Seiten mit a^{-k} (und wendet die Potenzregeln an), so folgt $a^{\ell-k} = a^0 = 1$. Es folgt, dass a endliche Ordnung in G hat. Wir bezeichnen die Ordnung von a mit m und behaupten:

(i) Die Elemente $a^0 = 1, a^1, a^2, \ldots, a^{m-1}$ sind alle verschieden.

(ii) Außer den in (i) genannten Elementen gibt es keine weiteren in G.

Nachweis von (i): Angenommen, es gilt $a^\ell = a^k$ für $0 \leq k < \ell \leq m-1$. Wie oben folgt dann $a^{\ell-k} = 1$, im Widerspruch zur Annahme, dass m die Ordnung von a ist

Nachweis von (ii): Es sei $b \in G$. Wegen $G = \langle a \rangle$ existiert dann ein $k \in \mathbb{Z}$ mit $b = a^k$. Man wähle $q, r \in \mathbb{Z}$ mit $0 \leq r \leq m-1$, so dass $k = qm + r$ („Zerlegung mit Rest"). Es folgt aufgrund der Potenzregeln: $b = a^k = a^{qm+r} = (a^m)^q a^r = a^r$ (da $a^m = 1$). Wegen $0 \leq r \leq m-1$ folgt (ii).

Aus (i) und (ii) ergibt sich also $G = \{1, a, a^2, \ldots, a^{m-1}\}$.

Ähnlich wie wir im 1. Fall C_∞ ausgewählt haben, wählen wir im 2. Fall zu jedem $m \in \mathbb{N}$ eine zyklische Gruppe der Ordnung m aus, für die wir die Bezeichnung

$$C_m$$

benutzen wollen; für C_m verwenden wir, wenn nichts anderes gesagt ist, multiplikative Schreibweise.

Behauptung: Die Gruppe $(\mathbb{Z}_m, +)$ fällt unter Fall 2, sie ist somit eine *endliche zyklische Gruppe der Ordnung m*.

Man beweist diese Behauptung ähnlich wie die entsprechende Behauptung im 1. Fall, indem man unter Benutzung der Potenzregeln zeigt, dass $\mathbb{Z}_m \cong C_m$ gilt.

Beispiel: Es sei $G = \mathbb{Z}_7 \setminus \{0\}$. Ist G bezüglich der Multiplikation modulo 7 eine zyklische Gruppe?

Wir versuchen, ein Element zu finden, das G erzeugt. Es gilt:

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 1.$$

Als ein Erzeuger (man sagt auch *Generator*) von G kommt 2 also nicht in Frage. Mit 3 funktioniert es besser:

$$3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5,\ 3^6 = 1.$$

Also gilt $G = \langle 3 \rangle$. Mit anderen Worten: G ist eine zyklische Gruppe mit 6 Elementen und ein Erzeuger dieser Gruppe ist das Element 3.

6.7 Untergruppen

Definition.
Ist G eine Gruppe und H eine Teilmenge von G, so nennt man H eine *Untergruppe von G*, falls H in Bezug auf die Operation von G selbst eine Gruppe ist.

Beispiel: Es sei $G_\triangle = \{i, r, s, x, y, z\}$ die Dreiecksgruppe. Wir betrachten Teilmengen von $G_\triangle$:

$$H_1 = \{r, s, z\},\ H_2 = \{i, r, s\},\ H_3 = \{i, r, s, x\}.$$

Sind dies Untergruppen?

Antwort: H_1 ist ganz gewiss keine Untergruppe, da H_1 ja noch nicht einmal abgeschlossen ist: Es gilt $rz = x$ und x ist nicht in H_1. Außerdem hat H_1 kein neutrales Element.

H_2 ist eine Untergruppe, da H_2 abgeschlossen ist (man beachte insbesondere, dass $rs = i$ und $sr = i$ gilt) und da außerdem (G1) - (G3) gelten: Das Assoziativgesetz (G1) „vererbt" sich natürlich von $G_\triangle$ auf H_2, (G2) gilt wegen $i \in H_2$ und außerdem hat jedes Element von H_2 ein Inverses in H_2; für i ist dies i selber, für r ist dies s und umgekehrt. Also gilt (G3).

H_3 ist keine Untergruppe. (Wieso nicht?)

Der folgende Satz erleichtert einem das Leben, wenn es darum geht, nachzuprüfen, ob eine Teilmenge H einer Gruppe G eine Untergruppe von G ist.

Satz 4.

Es sei G eine Gruppe und H sei eine nichtleere Teilmenge von G, für die die folgenden beiden Bedingungen gelten:

(U1) $a, b \in H \Rightarrow ab \in H$,

(U2) $a \in H \Rightarrow a^{-1} \in H$.

Dann ist H eine Untergruppe von G.

Zusatz (*Wichtig!*). Wenn G *endlich* ist, dann reicht es sogar aus, (U1) nachzuweisen, da dann (wie wir gleich zeigen werden) (U2) aus (U1) folgt.

Beweis des Satzes. $H \subseteq G$ sei nichtleer und erfülle sowohl (U1) als auch (U2). Um nachzuweisen, dass H dann eine Untergruppe von G ist, müssen wir zeigen, dass H abgeschlossen ist und dass für H die Gruppenaxiome gelten. Die Abgeschlossenheit von H gilt aufgrund von (U1). (G1) ist erfüllt, da die Multiplikation in G assoziativ ist. (Man kann es auch so ausdrücken: Das Assoziativgesetz „vererbt“ sich von G auf H.)

Dass (G2) für H gilt, erkennt man so: Da H nicht leer ist, können wir ein $h \in H$ wählen. Aus (U2) folgt dann, dass $h^{-1} \in H$ gilt. Aus (U1) folgt dann weiter, dass $hh^{-1} \in H$ gilt. Da $hh^{-1} = 1$ gilt, haben wir (G2) gezeigt.

Dass (G3) gilt, ergibt sich unmittelbar aus (U2). □

Beweis des Zusatzes. G sei nun endlich und es gelte (U1). Es sei $a \in H$ beliebig. (U2) ist nachgewiesen, wenn wir $a^{-1} \in H$ zeigen. Das erhält man folgendermaßen: Da G endlich ist, ist a von endlicher Ordnung; $m \in \mathbb{N}$ sei die Ordnung von a. Wir betrachten die Elemente $a, a^2, \ldots, a^{m-1}$: Iterierte Anwendung von (U1) ergibt, dass alle diese Elemente in H sind. Insbesondere gilt also

$$a^{m-1} \in H.$$

Nun ist aber a^{m-1} nichts anderes als a^{-1}, da $aa^{m-1} = a^{m-1}a = a^m = 1$ gilt. Also gilt $a^{-1} \in H$. □

Es sei G eine Gruppe und $a \in G$ ein Element endlicher Ordnung m; die Teilmenge H von G sei definiert durch:

$$H = \left\{1, a, a^2, \ldots, a^{m-1}\right\}. \tag{6.2}$$

Man zeige (Übungsaufgabe!): *H ist eine Untergruppe von G der Ordnung m.* (Anleitung: Aufgrund von Satz 4 sind (U1) und (U2) zu zeigen; außerdem ist $|H| = m$ nachzuweisen, d.h., es ist zu zeigen, dass die Elemente $1, a, a^2, \ldots, a^{m-1}$ alle verschieden sind. Dies alles lässt sich mit Schlüssen erledigen, die in ähnlicher Form schon mehrfach in den Abschnitten 6.4, 6.5 und 6.6 vorkamen.)

Man nennt die Untergruppe H aus (6.2) die *von a erzeugte zyklische Untergruppe von G* und schreibt für diese Untergruppe entweder wie bisher $H = \langle a \rangle$ oder auch $H = \langle a \rangle_G$.

6.8 Nebenklassen und der Satz von Lagrange

Definition.

Es sei H eine Untergruppe einer Gruppe G und a sei ein Element von G. Mit Hilfe von a und H definieren wir eine Teilmenge von G wie folgt:

$$aH := \left\{g \in G : \text{ Es gibt ein } h \in H \text{ mit } g = ah\right\}.$$

Man nennt eine solche Teilmenge aH eine *Linksnebenklasse* von H in G.

Wir beschreiben die obige Definition von aH noch einmal mit Worten: Man erhält die Elemente von aH dadurch, dass man alle Elemente von H von links mit a multipliziert. Falls H endlich ist, etwa $|H| = m$

und $H = \{h_1, h_2, \ldots, h_m\}$, so sind also

$$ah_1,\ ah_2,\ \ldots,\ ah_m$$

die Elemente von aH. Diese Elemente sind tatsächlich alle verschieden, wie man mit Hilfe der Linkskürzregel sofort einsieht: Für $h_i \neq h_j$ muss $ah_i \neq ah_j$ gelten, denn wäre $ah_i = ah_j$, so würde sich mit der Linkskürzregel $h_i = h_j$ ergeben. Es gilt also $|aH| = m$, d.h., H und aH haben gleich viele Elemente.

Da dies eine wichtige Beobachtung ist, halten wir sie ausdrücklich fest:

Feststellung 1.
Ist H eine endliche Untergruppe von G, so gilt für jede Linksnebenklasse aH von H:

$$|aH| = |H|\,.$$

Beispiele:

1. Es sei $G = \mathbb{Z}_7 \setminus \{0\} = \{1, 2, \ldots, 6\}$, wobei die Multiplikation die übliche Multiplikation modulo 7 ist. Es sei $H = \langle 6 \rangle$, d.h., H ist die von 6 erzeugte zyklische Untergruppe von G. Da $6^2 = 36 \equiv 1 \pmod 7$ gilt, besteht H nur aus den Elementen 1 und 6, also

$$H = \{1, 6\}.$$

Die Gruppentafel („Multiplikationstabelle“) von H sieht so aus:

	1	6
1	1	6
6	6	1

Wir bestimmen die Linksnebenklasse aH für $a = 3$; es gilt in $\mathbb{Z}_7 \setminus \{0\}$:

$$3 \cdot 1 = 3,\ 3 \cdot 6 = 4.$$

Also haben wir $3H = \{3, 4\}$.

Ganz entsprechend können wir *sämtliche Linksnebenklassen* aH bestimmen, es ergibt sich

$$1H = \{1, 6\} \quad 2H = \{2, 5\} \quad 3H = \{3, 4\}$$
$$4H = \{3, 4\} \quad 5H = \{2, 5\} \quad 6H = \{1, 6\}.$$

Manche dieser Nebenklassen sind gleich (etwa $2H = 5H$); es kann also durchaus passieren, dass $aH = bH$ gilt, obwohl $a \neq b$ ist. Ein und dieselbe Menge kann also unter verschiedenen Namen auftreten.

2. Es sei $G = \mathbb{Z}_{13} \setminus \{0\} = \{1, 2, \ldots, 12\}$ mit Multiplikation modulo 13 und H sei durch $H = \langle 3 \rangle$ gegeben. In $\mathbb{Z}_{13} \setminus \{0\}$ gilt: $3^1 = 3,\ 3^2 = 9,\ 3^3 = 1$; also:

$$H = \{1, 3, 9\}.$$

Linksnebenklassen von H sind dann beispielsweise

$$2H = \{2, 5, 6\} \quad \text{und} \quad 4H = \{4, 10, 12\}.$$

3. Wir betrachten die symmetrische Gruppe S_3, die aus den Permutationen der Menge $M = \{1, 2, 3\}$ besteht; es gibt $3! = 6$ Permutationen von M:

- die identische Permutation: id,

- drei Transpositionen: $(1,2),\ (1,3),\ (2,3)$,
- zwei Permutationen der Ordnung 3: $(1,2,3)$ und $(1,3,2)$.

$H = \langle (1,2)\rangle = \{id, (1,2)\}$ sei die von $(1,2)$ erzeugte zyklische Untergruppe von S_3.

Wir berechnen die Linksnebenklasse $(1,3)H$: Es gilt selbstverständlich $(1,3)id = (1,3)$; für das Produkt $\pi = (1,3)(1,2)$ gilt: $\pi(1) = 2$, da durch $(1,2)$ die 1 auf 2 abgebildet wird und da 2 von der Permutation $(1,3)$ festgelassen wird. Ähnlich überlegt man sich, dass $\pi(2) = 3$ und $\pi(3) = 1$ gilt. Also $\pi = (1,2,3)$.

Damit ergibt sich:

$$(1,3)H = \Big\{(1,3)id,\ (1,3)(1,2)\Big\} = \Big\{(1,3),\ (1,2,3)\Big\}.$$

Bestimmt man entsprechend sämtliche Linksnebenklassen von H, so erhält man

$$idH = \Big\{id,\ (1,2)\Big\} \qquad (1,2)H = \Big\{id,\ (1,2)\Big\} \qquad (1,3)H = \Big\{(1,3),\ (1,2,3)\Big\}$$
$$(2,3)H = \Big\{(2,3),\ (1,3,2)\Big\} \quad (1,2,3)H = \Big\{(1,3),\ (1,2,3)\Big\} \quad (1,3,2)H = \Big\{(2,3),\ (1,3,2)\Big\}.$$

Betrachtet man in den obigen Beispielen 1 und 3 die jeweils *verschiedenen* unter den Linksnebenklassen von H, so fällt auf, dass diese eine Zerlegung von $\mathbb{Z}_7 \setminus \{0\}$ bzw. S_3 in disjunkte Klassen bilden, etwa ergab sich in Beispiel 3 eine Zerlegung von

$$S_3 = \Big\{id,\ (1,2),\ (1,3),\ (2,3),\ (1,2,3),\ (1,3,2)\Big\}$$

in die drei Klassen

$$\Big\{id,\ (1,2)\Big\}, \quad \Big\{(1,3),\ (1,2,3)\Big\} \quad \text{und} \quad \Big\{(2,3),\ (1,3,2)\Big\}.$$

Wir zeigen nun, dass Entsprechendes allgemein gilt.

Feststellung 2.
Ist H eine Untergruppe von G, so bilden die verschiedenen unter den Linksnebenklassen von H eine Zerlegung von G in disjunkte Mengen.

Beweis. Zunächst einmal stellen wir fest, dass jedes Element $a \in G$ tatsächlich in einer Linksnebenklasse von H vorkommt: Das ist klar, da $1 \in H$ gilt, und somit $a \in aH$. Es bleibt zu zeigen:

$(*)$ Haben zwei Linksnebenklassen a_1H und a_2H ein Element x gemeinsam, so sind a_1H und a_2H gleich.

Zum Nachweis von $(*)$ sei ein $x \in a_1H \cap a_2H$. Zu zeigen ist $a_1H = a_2H$.

Aus $x \in a_1H$ folgt, dass $x = a_1h_1$ für ein $h_1 \in H$, und aus $x \in a_2H$ folgt, dass $x = a_2h_2$ für ein $h_2 \in H$ gilt.

Wir wollen zunächst $a_1H \subseteq a_2H$ zeigen. Hierzu sei $y \in a_1H$, zu zeigen ist, dass daraus $y \in a_2H$ folgt. Wegen $y \in a_1H$ gilt $y = a_1h$ für ein $h \in H$.

Man beachte, dass aus $x = a_1h_1$ folgt: $xh_1^{-1} = (a_1h_1)h_1^{-1} = a_1(h_1h_1^{-1}) = a_1$. Es ergibt sich nun:

$$y = a_1h = (xh_1^{-1})h = x(h_1^{-1}h) = a_2\underbrace{h_2(h_1^{-1}h)}_{\in H}.$$

Da $h_2\big(h_1^{-1}h\big) \in H$ gilt, folgt $y \in a_2H$. Also gilt $a_1H \subseteq a_2H$. Analog erhält man, wenn man die Rollen von a_1 und a_2 vertauscht, dass $a_2H \subseteq a_1H$ gilt. Insgesamt folgt daher $a_1H = a_2H$. $\square$

Wir benutzen nun die Feststellungen 1 und 2, um das Hauptergebnis dieses Abschnitts zu beweisen.

Satz 5 (Lagrange).
G sei eine endliche Gruppe der Ordnung n (d.h. $|G| = n$) und H sei eine Untergruppe von G der Ordnung m (d.h. $|H| = m$). Dann ist m ein Teiler von n.

Beweis. Aufgrund der Feststellungen 1 und 2 bilden die verschiedenen unter den Linksnebenklassen von H eine Zerlegung von G in disjunkte Mengen, sagen wir in k disjunkte Mengen $M_1, \ldots, M_k$, für die $|M_1| = \ldots = |M_k| = |H| = m$ gilt. Es folgt $n = k \cdot m$, d.h., m ist ein Teiler von n. □

Der Satz von Lagrange besagt also: *Hat G die Ordnung n, so kommen als Ordnung einer Untergruppe von G nur Teiler von n in Frage.* Gilt also beispielsweise $|G| = 10$, so kann es nur Untergruppen der Ordnungen 1, 2, 5 und 10 geben, niemals aber Untergruppen der Ordnungen 3, 4, 6, 7, 8 oder 9. (Ob es nun in G mit $|G| = 10$ tatsächlich eine Untergruppe etwa der Ordnung 5 gibt, darüber sagt der Satz nichts aus.)

Einige Folgerungen aus dem Satz von Lagrange:

Folgerung 1. Es sei G eine endliche Gruppe mit $|G| = n$ und a sei ein Element von G. Dann gilt:

(i) die Ordnung von a teilt n,

(ii) $a^n = 1$.

Beweis.

(i) Hat a die Ordnung m, so hat die von a in G erzeugte zyklische Untergruppe

$$\langle a \rangle = \left\{1, a, a^2, \ldots, a^{m-1}\right\}$$

die Ordnung m. Also gilt nach dem Satz von Lagrange: $m \mid n$.

(ii) Nach (i) gilt $m \mid n$ für die Ordnung m von a, d.h., $n = m \cdot k$ für ein $k \in \mathbb{N}$. Es folgt

$$a^n = a^{m \cdot k} = (a^m)^k = 1^k = 1. \quad \square$$

Beispiele:

1. Für eine Gruppe G gelte $|G| = 42$ und es sei $a \in G$. Für die Ordnung von a kommt dann nur in Frage: 1, 2, 3, 6, 7, 14, 21 oder 42.

2. Wir betrachten die Gruppe $\mathbb{Z}_{13} \setminus \{0\}$, wobei die Operation die Multiplikation modulo 13 ist.

Wir wollen die Ordnung von 2 bestimmen. Es gilt in $\mathbb{Z}_{13} \setminus \{0\}$: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 3$. Also: 2 hat keine der Ordnungen 1, 2, 3 oder 4.

Wenn wir nicht (i) aus Folgerung 1 kennen würden, würden wir vermutlich im gleichen Stil fortfahren und $2^5, 2^6, 2^7, \ldots$ berechnen.

Da wir jedoch Folgerung 1 kennen, wissen wir, dass als mögliche weitere Ordnungen nur noch 6 und 12 in Frage kommen. Es gilt $2^6 = 64 \equiv 12 \pmod{13}$, also hat 2 auch nicht die Ordnung 6.

Folglich hat 2 die Ordnung 12.

Folgerung 2. G sei eine Gruppe mit Primzahlordnung, d.h., $|G| = p$ für eine Primzahl p. Dann ist G zyklisch.

Beweis. Es gilt $|G| = p \geq 2$. Also können wir ein Element $a \in G$ mit $a \neq 1$ wählen. Da p eine Primzahl ist, kommen als Ordnung von a nur 1 und p in Frage (nach Folgerung 1). Wegen $a \neq 1$ scheidet 1 als mögliche Ordnung von a aus.

Also: a hat die Ordnung p. Wir betrachten die von a in G erzeugte zyklische Gruppe

$$\langle a \rangle = \left\{1, a, a^2, \ldots, a^{p-1}\right\}.$$

Wegen $|\langle a \rangle| = p = |G|$ folgt:

$$G = \langle a \rangle,$$

d.h., G ist zyklisch. $\square$

Also: *Jede Gruppe von Primzahlordnung ist zyklisch.*

Beispiele:

1. Wir betrachten die symmetrische Gruppe S_3 und wollen alle Untergruppen von S_3 bestimmen. Die $3! = 6$ Elemente von S_3 sind: id, $(1,2)$, $(1,3)$, $(2,3)$, $(1,2,3)$ und $(1,3,2)$.

Wir bestimmen *zunächst die zyklischen Untergruppen*, d.h., die Untergruppen der Form $\langle a \rangle$, die also von einem einzigen Element erzeugt werden; es ergibt sich:

$$\begin{aligned} \langle id \rangle &= \Big\{ id \Big\} \\ \langle (1,2) \rangle &= \Big\{ id,\ (1,2) \Big\}. \end{aligned}$$

Analog:

$$\begin{aligned} \langle (1,3) \rangle &= \Big\{ id,\ (1,3) \Big\} \\ \langle (2,3) \rangle &= \Big\{ id,\ (2,3) \Big\}. \end{aligned}$$

Und schließlich (man beachte $(1,2,3)^2 = (1,3,2)$, $(1,2,3)^3 = id$ sowie $(1,3,2)^2 = (1,2,3)$, $(1,3,2)^3 = id$):

$$\langle (1,2,3) \rangle = \Big\{ id,\ (1,2,3),\ (1,3,2) \Big\} = \langle (1,3,2) \rangle.$$

Wir haben bisher fünf Teilmengen von S_3 bestimmt, von denen feststeht: Diese Teilmengen sind Untergruppen von S_3. Eine weitere Untergruppe können wir sofort angeben: S_3 selbst.

Insgesamt gibt es aber $2^6 = 64$ Teilmengen von S_3, unter denen sich weitere Untergruppen befinden könnten. Müssen wir nun alle verbliebenen Teilmengen eine nach der anderen unter die Lupe nehmen, um herauszufinden, ob es noch weitere Untergruppen gibt?

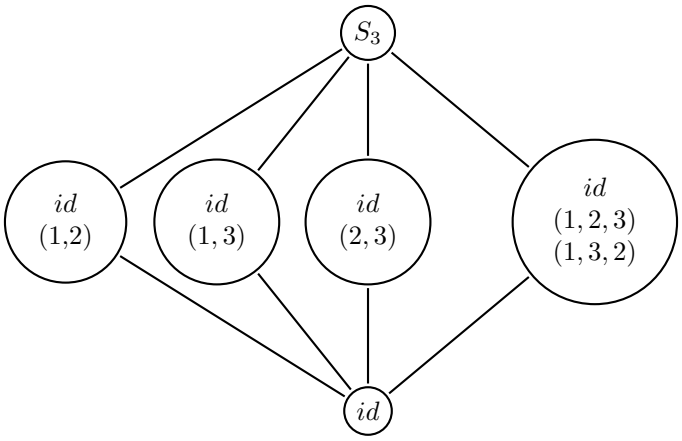
Zum Glück nicht! Aufgrund des Satzes von Lagrange wissen wir, dass als Untergruppenordnungen außer 1 und 6 nur noch 2 und 3 in Frage kommen. Nach Folgerung 2 müssen Untergruppen der Ordnung 2 und 3 jedoch zyklische Untergruppen sein; die zyklischen Untergruppen von S_3 haben wir aber schon vollständig bestimmt. *Wir können also sicher sein, dass wir bereits alle Untergruppen gefunden haben.*

Zusammenfassend können wir feststellen:

Außer den Untergruppen $\{id\}$ und G selbst (die gibt es ja immer!) existieren genau vier weitere Untergruppen von $G = S_3$, nämlich

- die zyklischen Untergruppen der Ordnung 2: $\{id,\ (1,2)\}$, $\{id,\ (1,3)\}$, $\{id,\ (2,3)\}$,
- eine zyklische Untergruppe der Ordnung 3: $\{id,\ (1,2,3),\ (1,3,2)\}$.

Bezüglich der Relation $\subseteq$ bilden die Untergruppen einer Gruppe G eine *partiell geordnete Menge*, die man, falls G endlich ist, durch ihr *Hasse-Diagramm* darstellen kann. In unserem Beispiel $G = S_3$ ergibt sich das folgende Hasse-Diagramm:



2. Die symmetrische Gruppe S_3 hat nur wenige Elemente und ist deshalb relativ leicht zu überschauen. Im Lehrbuch von N. L. Biggs, Discrete Mathematics wird ein etwas komplizierteres Beispiel diskutiert: Es wird dort für *eine bestimmte Gruppe A der Ordnung 12* ermittelt, welches die Untergruppen von A sind. Wir geben hier nur das Ergebnis wieder.

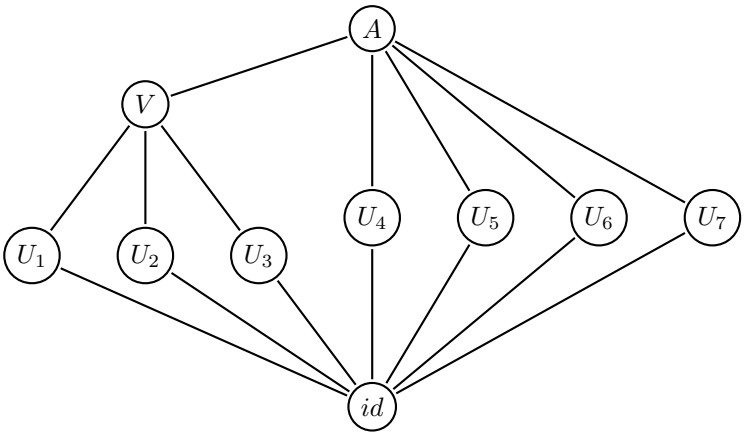
Zunächst wissen wir nach dem Satz von Lagrange, dass es nur Untergruppen der Ordnungen

$$1,\ 2,\ 3,\ 4,\ 6 \text{ oder } 12$$

geben kann. Das Ergebnis ist, dass es genau folgende Untergruppen gibt:

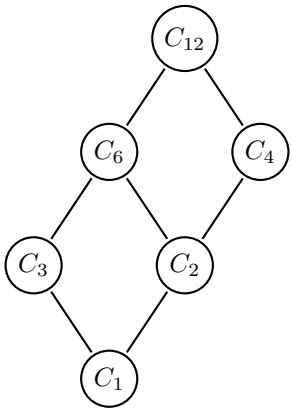
- eine Untergruppe der Ordnung 1, nämlich $\{id\}$ (Das ist sowieso klar!)
- drei Untergruppen U_1, U_2, U_3 der Ordnung 2
- vier Untergruppen U_4, U_5, U_6, U_7 der Ordnung 3
- eine Untergruppe V der Ordnung 4; diese Untergruppe enthält die Untergruppen U_1, U_2, U_3 und ist *nicht zyklisch*
- *keine* Untergruppe der Ordnung 6
- eine Untergruppe der Ordnung 12, nämlich A selbst. (Das war wieder klar!)

Das zugehörige Hasse-Diagramm sieht so aus:



3. Wir erwähnen (ohne Beweis), dass es auch andere Gruppen der Ordnung 12 gibt, für die die Untergruppenstruktur völlig anders aussieht als für die Gruppe A aus Beispiel 2. Ist beispielsweise C_{12} eine

zyklische Gruppe der Ordnung 12, so gilt: Zu jeder der möglichen Untergruppenordnungen 1, 2, 3, 4, 6, 12 gibt es *genau eine Untergruppe*; außerdem sind alle diese Untergruppen selber wieder zyklisch. Wenn wir die Untergruppen von C_{12} mit C_1, C_2, C_3, C_4, C_6 und C_{12} bezeichnen, wobei $|C_i| = i$ gilt, so sieht das Hasse-Diagramm wie folgt aus:



Dieses Hasse-Diagramm hat dieselbe Struktur wie das Hasse-Diagramm, das zur Teilbarkeitsrelation $|$ gehört, wobei die Grundmenge die Menge $\{1, 2, 3, 4, 6, 12\}$ aller positiven Teiler von 12 ist.

Die im Beispiel 3 erwähnten Tatsachen gelten übrigens entsprechend für jede endliche zyklische Gruppe. Dies ist der Inhalt des folgenden Satzes, den wir ohne Beweis angeben. Einen Beweis sowie Details zu Beispiel 3 findet man im Buch von Biggs, das im Übrigen sehr empfohlen werden kann und dem wir in Abschnitt 6 teilweise gefolgt sind.

Satz 6.
G sei eine endliche zyklische Gruppe der Ordnung n, und d sei ein Teiler von n. Dann hat G genau eine Untergruppe der Ordnung d, und diese Untergruppe ist ebenfalls zyklisch.

Für das zugehörige Hasse-Diagramm ergibt sich aus Satz 6, dass es dieselbe Struktur hat wie das Hasse-Diagramm, das zur Teilbarkeitsrelation gehört, wobei die Grundmenge die Menge aller positiven Teiler von n ist.

Anmerkungen zu Links- und Rechtsnebenklassen

Wir haben im Abschnitt 6.8 unsere Überlegungen auf dem Begriff der Linksnebenklasse aufgebaut. Ebenso gut hätten wir Rechtsnebenklassen nehmen können, die wie folgt definiert werden:

Definition.
Für eine Untergruppe H einer Gruppe G und ein Element $a \in G$ sei

$$Ha := \Big\{ g \in G : \text{ Es gibt ein } h \in H \text{ mit } g = ha \Big\}.$$

Man nennt die Teilmenge Ha von G eine *Rechtsnebenklasse* von H in G.

Ist die betrachtete Gruppe G abelsch, so gilt offenbar $aH = Ha$; man braucht dann nicht zwischen Links- und Rechtsnebenklassen zu unterscheiden und spricht nur von *Nebenklassen*.

Ist G nicht abelsch, so kann durchaus $aH \neq Ha$ gelten. Ebenso wie wir mit Hilfe der Linkskürzregel $|aH| = |H|$ erhalten haben, kann man mit der Rechtskürzregel

$$|Ha| = |H|$$

erhalten (vgl. Feststellung 1). Für Rechtsnebenklassen gilt auch analog zu Feststellung 2:

Feststellung 2'.

Ist H eine Untergruppe von G, so bilden die verschiedenen unter den Rechtsnebenklassen von H eine Zerlegung von G in disjunkte Mengen.

Unter den Rechtsnebenklassen von H in G kann es durchaus welche geben, die keine Linksnebenklassen von H in G sind (und umgekehrt)[1]; wegen $|aH| = |H| = |Ha|$ gilt aber:

Ist G endlich, so ist die Anzahl der Rechtsnebenklassen von H in G gleich der Anzahl der Linksnebenklassen von H in G, nämlich $\frac{|G|}{|H|}$. Man nennt diese Anzahl den *Index* von H in G.

[1] Um dies einzusehen bilde man in Beispiel 3 auf Seite 113 die Rechtsnebenklassen von $H = \langle (1,2) \rangle$.

7 Ringe, Körper und Polynome

7.1 Ringe

Definition.
Eine Menge R, auf der zwei binäre Operationen $+$ und $\cdot$ definiert sind, heißt ein *Ring*, falls die folgenden Axiome gelten:

(R1) Assoziativgesetze:
- $a + \big(b + c\big) = \big(a + b\big) + c$
- $a \cdot \big(b \cdot c\big) = \big(a \cdot b\big) \cdot c$

(R2) Kommutativgesetz der Addition:
- $a + b = b + a$

(R3) Distributivgesetze:
- $a \cdot \big(b + c\big) = a \cdot b + a \cdot c$
- $\big(b + c\big) \cdot a = b \cdot a + c \cdot a$

(R4) Existenz neutraler Elemente:
Es gibt in R Elemente 0 und 1, welche die Eigenschaft haben, dass für jedes $a \in R$ gilt:
- $a + 0 = a$
- $a \cdot 1 = 1 \cdot a = a$

(R5) Existenz inverser Elemente der Addition:
Zu jedem a aus R gibt es ein Element $-a$ aus R, für das gilt:
- $a + (-a) = 0$

Mit Hilfe der Begriffe „Monoid“ und „Gruppe“ kann man die Definition eines Ringes auch in der folgenden kompakten Form aussprechen.

Definition.
Eine Menge R, auf der zwei binäre Operationen $+$ und $\cdot$ gegeben sind, heißt ein *Ring*, falls die folgenden Axiome gelten:

(RI) $(R, +)$ ist eine kommutative Gruppe.

(RII) $(R, \cdot)$ ist ein Monoid.

(RIII) Es gelten die Distributivgesetze, d.h., für alle $a, b, c \in R$ gilt:
- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(b + c) \cdot a = b \cdot a + c \cdot a$

In der kommutativen Gruppe $(R, +)$ bezeichnet man das neutrale Element mit 0. Das Inverse von a bezüglich $+$ wird mit $-a$ bezeichnet. Anstelle von „das Inverse von a bezüglich $+$“ sagt man meistens „das Negative von a“. (RI) bedeutet im Einzelnen, dass der Operator $+$ folgende Eigenschaften hat:

- $(a + b) + c = a + (b + c)$

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

Im Monoid $(R, \cdot)$ bezeichnet man das neutrale Element mit 1.

(RII) bedeutet im Einzelnen, dass die Multiplikation folgende Eigenschaften hat:

- $(ab)c = a(bc)$,
- $a \cdot 1 = 1 \cdot a = a$.

Wir geben **Beispiele** für Ringe:

1. Der *Ring der ganzen Zahlen* $(\mathbb{Z}, +, \cdot)$, wobei $+$ und $\cdot$ die übliche Addition und Multiplikation sind. Dieser Ring besitzt außer den in den Axiomen genannten Eigenschaften *zusätzliche Eigenschaften*, die längst nicht in jedem Ring gelten:

(i) Die Multiplikation ist *kommutativ*, d.h., es gilt stets $ab = ba$.

(ii) Es gilt die *Kürzregel*, d.h., für a, b, c mit $a \neq 0$ gilt stets $ab = ac \Rightarrow b = c$.

2. $(\mathbb{Z}_m, +, \cdot)$ für $m \geq 2$, wobei $+$ und $\cdot$ die Addition bzw. Multiplikation modulo m sind.

Dass es sich hierbei tatsächlich um einen Ring handelt, für den außerdem (i) gilt, entnimmt man Feststellung 1, Seite 82. Zusatzeigenschaft (ii) gilt aber im Allgemeinen nicht. (Ein Beispiel hierfür: In $\mathbb{Z}_6$ gilt $4 \cdot 5 = 4 \cdot 2$, aber nicht $5 = 2$.)

3. Ist R ein Ring mit Operationen $+$ und $\cdot$, so sei $M(n \times n, R)$ die Menge aller $n \times n$ - Matrizen über R. Nimmt man als Operationen die Addition und Multiplikation von Matrizen, so wird $M(n \times n, R)$ zu einem Ring.

Man nennt derartige Ringe $M(n \times n, R)$ *Matrizenringe*.

Da die Matrizenmuliplikation im Allgemeinen nicht kommutativ ist, ist es leicht, Ringe anzugeben, für die (i) nicht gilt, die also *nicht kommutativ* sind. Zum Beispiel ist $M(2 \times 2, \mathbb{R})$ ein solcher Ring: Für $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ gilt $AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ und $BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, also $AB \neq BA$.

Auf weitere Standardbeispiele für Ringe wie etwa *Körper* und *Polynomringe* kommen wir später zu sprechen.

7.2 Die Einheitengruppe eines Ringes

Es sei $(R, +, \cdot)$ ein Ring. In diesem Abschnitt befassen wir uns weniger mit der Addition $+$, sondern wir richten unser Augenmerk auf das Monoid $(R, \cdot)$. Vor allem interessieren uns die *invertierbaren Elemente von* $(R, \cdot)$, also diejenigen Elemente $a \in R$, die ein inverses Element bezüglich der Multiplikation besitzen.

Zur Erinnerung: Es sei $a \in R$. Dann heißt ein Element $x \in R$ *inverses Element von a bezüglich der Multiplikation*, wenn

$$xa = ax = 1.$$

Ebenfalls zur Erinnerung schaue man sich noch einmal an, was wir bereits in Abschnitt 6.1 über invertierbare Elemente in Monoiden gesagt haben (insbesondere die dort gegebenen Beispiele). Aus Abschnitt 6.1 wissen wir bereits, dass ein Element $a \in R$ niemals zwei verschiedene inverse Elemente bezüglich der Multiplikation haben kann. Wenn a ein Inverses der Multiplikation besitzt, so bezeichnen wir es mit

$$a^{-1}$$

und sprechen von *dem* Inversen von a.

Diejenigen Elemente $a \in R$, für die das Inverse a^{-1} existiert, nennt man die *Einheiten* von R. Die Menge aller Einheiten von R bezeichnet man mit

$$E(R).$$

Beispiele:

1. Für $R = \mathbb{Z}$ (mit der gewöhnlichen Addition und Multiplikation) gilt $E(R) = \{1, -1\}$. (Wieso?)
2. Für $R = \mathbb{Z}_6$ (mit der Addition und Multiplikation modulo 6) gilt $E(R) = \{1, 5\}$. (Wieso? Wenn Sie es nicht mehr so genau wissen: Schauen Sie sich noch einmal Feststellung 3 auf Seite 84 an!)
3. Bestimmen Sie $E(R)$ für $R = \mathbb{Z}_8$ und für $R = \mathbb{Z}_{11}$ (mit + und · modulo 8 bzw. 11).
4. Es sei p eine Primzahl und $R = \mathbb{Z}_p$ (mit + und · modulo p). Welche Elemente enthält dann $E(R)$?

Wir zeigen nun, dass $E(R)$ bzgl. der Multiplikation immer eine Gruppe ist. Man nennt $E(R)$ deshalb die *Einheitengruppe* des Rings R.

Satz 1.
Die Menge $E(R)$ der invertierbaren Elemente („Einheiten“) von R ist bzgl. der Multiplikation des Ringes R eine Gruppe.

Beweis. Bevor wir die Gruppenaxiome (G1), (G2) und (G3) nachprüfen, müssen wir zeigen, dass $E(R)$ bzgl. $\cdot$ *abgeschlossen* ist: Hierzu seien $a, b \in E(R)$; wir haben zu zeigen, dass dann auch $a \cdot b \in E(R)$ gilt.

Aus $a, b \in E(R)$ folgt, dass die inversen Elemente a^{-1} und b^{-1} existieren. Um zu erkennen, dass $a \cdot b \in E(R)$ gilt, müssen wir zeigen, dass auch $a \cdot b$ ein Inverses hat. Wie könnte das Inverse von $a \cdot b$ aussehen?

Mögliche Kandidaten sind $a^{-1}b^{-1}$ und $b^{-1}a^{-1}$. Möchte man nachweisen, dass $a^{-1}b^{-1}$ das Inverse von $a \cdot b$ ist, so müsste man $(ab)(a^{-1}b^{-1}) = 1$ zeigen. Das klappt aber nicht, da die Multiplikation *nicht kommutativ zu sein braucht*. Die zweite Möglichkeit funktioniert:

$$(ab)(b^{-1}a^{-1}) \overset{*}{=} abb^{-1}a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1.$$

Ebenso erhält man $(b^{-1}a^{-1})(ab) = 1$. Zur mit * bezeichneten Stelle geben wir weiter unten noch eine zusätzliche Erklärung.

Nachprüfen der Gruppenaxiome:

(G1): (G1) gilt, da $(R, \cdot)$ ein Monoid ist und in einem Monoid definitionsgemäß das Assoziativgesetz gilt; für $E(R)$ braucht das Assoziativgesetz also gar nicht nachgeprüft zu werden, es „vererbt“ sich von R auf $E(R)$.

(G2): Es gilt $1 \in E(R)$, da 1 ein Inverses besitzt. (Was ist nämlich das Inverse von 1?)

(G3): Es ist zu zeigen, dass Folgendes gilt:

$$x \in E(R) \Rightarrow x^{-1} \in E(R).$$

Das ist aber klar: Wenn x^{-1} das Inverse von x ist, so ist wegen $xx^{-1} = x^{-1}x = 1$ auch x das Inverse von x^{-1}. □

Bemerkung zur mit * gekennzeichneten Stelle:

Wir haben die Klammern einfach weggelassen. Warum durften wir das tun?

Antwort: In $(R, \cdot)$ gilt das Assoziativgesetz $x(yz) = (xy)z$ und deshalb sind die Klammern überflüssig.

Allgemein gilt nämlich Folgendes: Es liege eine *Halbgruppe* $(H, \cdot)$ vor; das bedeutet, dass $\cdot$ ein binärer Operator ist, für den das Assoziativgesetz $x(yz) = (xy)z$ gilt. Dann folgt (und das ist der eigentliche Sinn des Assoziativgesetzes), dass *in Produkten mit drei oder mehr Faktoren keine Klammern gesetzt werden müssen*. Man nennt dies auch das *allgemeine Assoziativgesetz*; beweisen kann man es mit vollständiger Induktion, was aber hier nicht durchgeführt werden soll. Stattdessen wollen wir das allgemeine Assoziativgesetz an Beispielen erläutern. Für den Fall von drei und vier Faktoren besagt dieses Gesetz, dass in jeder Halbgruppe $(H, \cdot)$ gilt:

- $x(yz)$ und $(xy)z$ führen zu demselben Ergebnis; deshalb kann man die Klammern weglassen und einfach xyz schreiben;
- die Ausdrücke $w(x(yz))$, $w((xy)z)$, $((wx)y)z$, $(w(xy))z$ und $(wx)(yz)$ liefern alle dasselbe Ergebnis und deshalb kann man die Klammern weglassen und einfach $wxyz$ schreiben.

Nach dem allgemeinen Assoziativgesetz gilt Entsprechendes auch für Ausdrücke mit 5, 6 oder mehr Faktoren; beispielsweise bedeuten die Ausdrücke $u(v(w(x(yz))))$ und $((((uv)w)x)y)z$ dasselbe wie alle anderen Möglichkeiten, diese Faktoren sinnvoll zu beklammern und deshalb kann man die Klammern weglassen und einfach $uvwxyz$ schreiben.

Definition.
Ist $n \in \mathbb{N}$, so sei $\varphi(n)$ die Anzahl der Elemente $a \in \{1, \ldots, n\}$, die teilerfremd zu n sind, also $\mathrm{ggT}(a, n) = 1$ erfüllen. Man nennt φ die *Euler-Funktion*.

Einige Werte der Euler-Funktion:

n	$\varphi(n)$	Elemente $a \in \{1, \ldots, n\}$ mit $\mathrm{ggT}(a, n) = 1$
1	1	1
2	1	1
3	2	1, 2
4	2	1, 3
5	4	1, 2, 3, 4
6	2	1, 5
7	6	1, 2, 3, 4, 5, 6
8	4	1, 3, 5, 7
9		
10		
11		

Zur Übung vervollständige man die Tabelle!

Wir haben bereits früher festgestellt (vgl. Seite 84), dass ein Element $a \in \mathbb{Z}_n$ genau dann invertierbar ist, wenn a und n teilerfremd sind. Es folgt für den Ring $\mathbb{Z}_n$ (mit Addition und Multiplikation modulo n):

Feststellung.
Die Einheitengruppe $E(\mathbb{Z}_n)$ des Ringes $\mathbb{Z}_n$ ist eine Gruppe der Ordnung $\varphi(n)$.

Beispiele:

1. $E(\mathbb{Z}_8) = \{1, 3, 5, 7\}$ ist eine Gruppe der Ordnung $\varphi(8) = 4$. In dieser Gruppe gilt $3^2 = 1$, $5^2 = 1$, $7^2 = 1$; es gibt also kein Element der Ordnung 4. Deshalb ist diese Gruppe nicht zyklisch.
2. $E(\mathbb{Z}_5) = \{1, 2, 3, 4\}$ ist ebenfalls eine Gruppe der Ordnung 4. Wegen $E(\mathbb{Z}_5) = \langle 2 \rangle$ ist diese Gruppe zyklisch und damit insbesondere nicht isomorph zur Gruppe aus Beispiel 1.

Wer noch etwas mehr über die Euler-Funktion wissen möchte, schaue in die Lehrbücher von A. Steger (Diskrete Strukturen, Band 1) und N. L. Biggs (Discrete Mathematics). Wir zeigen hier nur noch den folgenden Satz, der auf den berühmten Schweizer Mathematiker Leonhard Euler (1707 - 1783) zurückgeht.

Satz 2 (L. Euler).
Für alle $n \in \mathbb{N}$ und alle $a \in E(\mathbb{Z}_n)$ gilt:

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \tag{7.1}$$

Mit Hilfe der im vorhergehenden Abschnitt bereitgestellten Ergebnisse über Gruppen fällt der Beweis leicht: Wendet man Folgerung 1 aus dem Satz von Lagrange (vgl. Abschnitt 6.8) auf die Gruppe $E(\mathbb{Z}_n)$

an und berücksichtigt man $|E(\mathbb{Z}_n)| = \varphi(n)$, so erhält man

$$a^{\varphi(n)} = 1.$$

Dies ist eine Gleichung in $\mathbb{Z}_n$, die dasselbe wie (7.1) bedeutet, nur in anderer Schreibweise. □

Ist p eine Primzahl, so gilt $E(\mathbb{Z}_p) = \{1, \ldots, p-1\}$ und $\varphi(p) = p - 1$. Aus dem obigen Satz von Euler erhält man also für jede Primzahl p:

$$a^{p-1} \equiv 1 \pmod{p} \text{ für alle } a \in \{1, \ldots, p-1\}. \tag{7.2}$$

Dies ist im Wesentlichen der Inhalt des Satzes von Fermat, den wir bereits auf Seite 84 formuliert und dort auf eine ganz andere Weise bewiesen haben. Wir wiederholen den Satz noch einmal und zeigen, dass er tatsächlich unmittelbar aus (7.2) folgt.

Satz von Fermat[1].
Es sei p eine Primzahl und n eine natürliche Zahl, für die $p \nmid n$ gilt. Dann folgt $n^{p-1} \equiv 1 \pmod{p}$.

Beweis. Wegen $p \nmid n$ gibt es ein $a \in \{1, \ldots, p-1\}$ mit $n \equiv a \pmod{p}$. Es folgt (durch Anwendung der Regel (5) für das Rechnen mit Kongruenzen, Seite 79) $n^{p-1} \equiv a^{p-1} \pmod{p}$. Also ergibt sich mit (7.2)

$$n^{p-1} \equiv a^{p-1} \equiv 1 \pmod{p}. \quad \square$$

Wir haben bereits auf Seite 20 definiert, was ein *Körper* ist. Aus der dort gegebenen Definition wird klar, dass ein Körper nichts anderes als ein Ring ist, für den neben (RI), (RII) und (RIII) die folgenden zusätzlichen Bedingungen erfüllt sind:

a) Die Multiplikation ist kommutativ.

b) Jedes Element $\neq 0$ ist invertierbar.

c) Es muss $0 \neq 1$ gelten.

Gegeben sei ein Körper K. Wir stellen uns die Frage: Welche Elemente von K gehören zur Einheitengruppe $E(K)$ des Körpers K?

Antwort: $E(K) = K \setminus \{0\}$.

Begründung: Wegen b) gilt $K \setminus \{0\} \subseteq E(K)$. Es bleibt also zu zeigen: $0 \notin E(K)$. Dies ist nachgewiesen, wenn wir zeigen, dass $0 \cdot a \neq 1$ für alle $a \in K$ gilt. Dies lässt sich so erschließen: Es sei $a \in K$. Dann gilt $0 \cdot a = (0+0)a = 0 \cdot a + 0 \cdot a$. Addiert man auf beiden Seiten der erhaltenen Gleichung das Negative von $0 \cdot a$, so folgt $0 = 0 \cdot a$ Wegen c) ergibt sich $0 \cdot a = 0 \neq 1$. □

Zu einem Körper K gehören also immer *zwei kommutative Gruppen*, nämlich

- die kommutative Gruppe $(K, +)$, die in jedem Ring vorhanden ist,
- die kommutative Gruppe $(K \setminus \{0\}, \cdot)$.

Man nennt diese Gruppen die *additive* und die *multiplikative Gruppe* des Körpers K.

7.3 Der Polynomring K[x]

Aus der Schule sind Ihnen Polynome wie beispielsweise

$$5x^3 + 2x^2 + 3x + 7 \text{ oder } x^2 + 5$$

bekannt; allgemein ist ein Polynom ein Ausdruck der Form

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \tag{7.3}$$

[1] Nach dem Franzosen Pierre Fermat (1601 - 1665). Der Satz wird auch „kleiner Satz von Fermat“ genannt. Interessante historische Bemerkungen zu diesem Satz findet man in A. Steger, Diskrete Strukturen, Band 1.

wobei x eine Unbestimmte ist und $a_0, a_1, \ldots, a_n$ $(n \geq 0)$ die *Koeffizienten* des Polynoms (7.3) heißen.

In der Schule stammen die Koeffizienten meist aus dem Körper $\mathbb{R}$ der reellen Zahlen. In diesem Fall spricht man von einem *reellen Polynom*. Stammen die Koeffizienten aus dem Körper $\mathbb{C}$ der komplexen Zahlen, so spricht man von einem *komplexen Polynom*. Komplexe Polynome werden gemeinsam mit dem Körper $\mathbb{C}$ der komplexen Zahlen im 2. Semester behandelt werden.

Hier wollen wir den allgemeineren Fall studieren, dass die Koeffizienten aus einem beliebigen Körper K stammen, also etwa aus dem Körper $K = \mathbb{Z}_2$ oder aus dem Körper $K = \mathbb{Z}_3$; man spricht in diesem Fall von einem *Polynom über K*.

Die Menge sämtlicher Polynome über einem Körper K bezeichnet man mit

$$K[x];$$

Polynome aus $K[x]$ werden meist mit Ausdrücken wie $a(x)$, $b(x)$, $p(x)$, $q(x)$ bezeichnet[2].

Wie Sie aus der Schule sicherlich wissen, kann man Polynome addieren, multiplizieren und man kann eine Division mit Rest ausführen. Diese Operationen mit Polynomen werden weiter unten besprochen. Zunächst sollen einige Begriffe eingeführt werden.

Im Folgenden sei K immer ein beliebiger Körper; Sie können jedoch zunächst einmal immer an den Fall $K = \mathbb{R}$ denken, und sich nur hin und wieder daran erinnern, dass K auch ein anderer Körper sein kann, z.B. der endliche Körper $\mathbb{Z}_2$ oder $\mathbb{Z}_3$ (oder allgemeiner: der endliche Körper $\mathbb{Z}_p$ der ganzen Zahlen modulo p für eine Primzahl p).

Ist $p(x) \in K[x]$ ein Polynom mit $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ $(n \geq 0)$, so definiert man den *Grad* von $p(x)$ als die größte Zahl i, für die $a_i \neq 0$ gilt. Dies setzt allerdings voraus, dass es mindestens einen Koeffizienten von $p(x)$ gibt, der von 0 verschieden ist. Im „Ausnahmefall“, dass alle Koeffizienten gleich 0 sind, nennt man $p(x)$ das *Nullpolynom*; dem Nullpolynom geben wir den Grad 0.

Beispiele: Es sei $K = \mathbb{R}$. Dann hat $5x^3 + 2x + 1$ den Grad 3, $x^2 + 5$ hat den Grad 2, $x + 4$ hat den Grad 1. Den Grad 0 haben die konstanten Polynome $p(x) = a_0$ (einschließlich des Nullpolynoms $p(x) = 0$).

Den Grad eines Polynoms p bezeichnen wir auch mit

$$\operatorname{grad}(p).$$

Ist $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ $(n \geq 0)$ nicht das Nullpolynom, so bezeichnet man den Koeffizienten a_m mit $m = \operatorname{grad}(p)$ als den *Leitkoeffizienten* von p.

Beispiel: Es sei $K = \mathbb{R}$. Dann hat das Polynom $p(x) = 5x^3 + 2x + 1$ den Leitkoeffizienten 5.

Ein Polynom, das den Leitkoeffizienten 1 hat, nennt man *normiert*.

Wie zuvor schon erwähnt, nennt man Polynome vom Grad 0 *konstante Polynome*.

Einige **Konventionen**, die Ihnen sicherlich größtenteils sowieso klar sind und die wir teilweise stillschweigend auch schon verwendet haben:

Ist ein Koeffizient gleich 0, so braucht man den zugehörigen Term $0 \cdot x^k$ nicht mit hinzuschreiben; ist ein Koeffizient gleich 1, so schreibt man statt $1 \cdot x^k$ einfach x^k; ähnliche, fast selbstverständliche Dinge gelten für Koeffizienten mit einem Minuszeichen: Statt

$$3x^3 + (-5)x^2 + 7$$

schreibt man meistens

$$3x^3 - 5x^2 + 7.$$

Außerdem schreibt man die Terme eines Polynoms ab und zu auch in veränderter Reihenfolge auf, z.B. $p(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + a_n x^n$.

[2] Ist die Unbestimmte nicht mit x sondern (etwa) mit t bezeichnet, so schreibt man entsprechend $K[t]$ bzw. $a(t)$, $b(t)$, $p(t)$, $q(t)$; man kann aber auch einfach nur a, b, p, q schreiben.

7.3.1 Addition von Polynomen

Gegeben: $a(x), b(x) \in K[x]$ mit $a(x) = a_0+a_1x+a_2x^2+\ldots+a_nx^n$ und $b(x) = b_0+b_1x+b_2x^2+\ldots+b_mx^m$.
Wir dürfen $n \geq m$ annehmen; und wenn $n > m$ gilt, so setzen wir $b_{m+1} = b_{m+2} = \ldots = b_n = 0$.
Man definiert nun ein Polynom aus $K[x]$, das man mit $(a+b)(x)$ oder auch mit $a(x)+b(x)$ bezeichnet und die *Summe* von $a(x)$ und $b(x)$ nennt, durch die Festsetzung:

$$(a+b)(x) = (a_0+b_0) + (a_1+b_1)x + (a_2+b_2)x^2 + \ldots + (a_n+b_n)x^n.$$

Es seien $a(x), b(x) \in K[x]$. Für den Grad der Summe $(a+b)(x)$ gilt dann:

$$\operatorname{grad}(a+b) \leq \max\Big\{\operatorname{grad}(a),\ \operatorname{grad}(b)\Big\}.$$

Beispiele:

- Es sei $K = \mathbb{R}$. Für $a(x) = 3+7x+5x^3$, $b(x) = 2-4x+3x^2+2x^3$ gilt $(a+b)(x) = 5+3x+3x^2+7x^3$.
- Für $a(x)$ wie oben und $b(x) = 2+5x$ gilt $(a+b)(x) = 5+12x+5x^3$.
- Für $a(x)$ wie oben und $b(x) = 2-5x^3$ gilt $(a+b)(x) = 5+7x$.

Man beachte: Es kann vorkommen, dass $\operatorname{grad}(a+b) < \max\big\{\operatorname{grad}(a), \operatorname{grad}(b)\big\}$ gilt (wie das letzte Beispiel zeigt).

7.3.2 Multiplikation von Polynomen

Gegeben: $a(x), b(x) \in K[x]$ mit $a(x) = a_0+a_1x+a_2x^2+\ldots+a_nx^n$ und $b(x) = b_0+b_1x+b_2x^2+\ldots+b_mx^m$.
Das *Produkt* $(a \cdot b)(x) \in K[x]$ (für das man auch $a(x)b(x)$ schreibt) erhält man, indem man

$$(a_0+a_1x+a_2x^2+\ldots+a_nx^n)(b_0+b_1x+b_2x^2+\ldots+b_mx^m)$$

auf die übliche Art ausmultipliziert und anschließend die erhaltenen Terme „sortiert“. Dies kann man genauer wie folgt beschreiben:

$$(a \cdot b)(x) := c_0 + c_1x + c_2x^2 + \ldots + c_{n+m}x^{n+m},$$

wobei für $0 \leq i \leq n+m$ gilt:

$$c_i = a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \ldots + a_ib_0.$$

Mit dem Summenzeichen geschrieben lautet diese Formel:

$$c_i = \sum_{j=0}^{i} a_jb_{i-j} \quad ,$$

wobei die in dieser Formel möglicherweise auftretenden Koeffizienten a_{n+1}, a_{n+2}, …, a_{n+m} und b_{m+1}, b_{m+2}, …, b_{n+m} alle gleich 0 sein sollen.
Zur Verdeutlichung:

$$\begin{aligned}(a \cdot b)(x) \quad = \quad & \underbrace{a_0b_0}_{c_0} + \underbrace{(a_0b_1+a_1b_0)}_{c_1}x + \underbrace{(a_0b_2+a_1b_1+a_2b_0)}_{c_2}x^2 + \\ & \underbrace{(a_0b_3+a_1b_2+a_2b_1+a_3b_0)}_{c_3}x^3 + \ldots + \underbrace{a_nb_m}_{c_{n+m}}x^{n+m}.\end{aligned}$$

Zur Übung: Schreiben Sie die entsprechenden Formeln für c_4 und c_5 auf!

Beispiele:

1. Es gelte $a(x), b(x) \in \mathbb{R}[x]$ mit $a(x) = 2 + 3x + 5x^2$ und $b(x) = 1 + 2x + 2x^2$. Es ergibt sich:

$$\begin{aligned}(a \cdot b)(x) &= 2 \cdot 1 + (2 \cdot 2 + 3 \cdot 1)x + (2 \cdot 2 + 3 \cdot 2 + 5 \cdot 1)x^2 + \\ &\quad (3 \cdot 2 + 5 \cdot 2)x^3 + (5 \cdot 2)x^4 \\ &= 2 + 7x + 15x^2 + 16x^3 + 10x^4.\end{aligned}$$

2. Es gelte $a(x), b(x) \in \mathbb{R}[x]$ mit $a(x) = 3 + 2x + x^2 - 2x^3 + 5x^4 + 2x^5 + x^6$ und $b(x) = 2 + 4x + 2x^2 + 5x^3 + 2x^4 + 3x^5 + 2x^6$.

Wie lautet der Koeffizient von x^6 in $(a \cdot b)(x)$?

Antwort: $3 \cdot 2 + 2 \cdot 3 + 1 \cdot 2 - 2 \cdot 5 + 5 \cdot 2 + 2 \cdot 4 + 1 \cdot 2 = 24$.

Es seien $a(x), b(x) \in K[x]$. Weder $a(x)$ noch $b(x)$ sei das Nullpolynom. Für den Grad des Produkts $(a \cdot b)(x)$ gilt dann[3]:

$$\operatorname{grad}(a \cdot b) = \operatorname{grad}(a) + \operatorname{grad}(b).$$

Bisher haben wir nur Beispiele für $K = \mathbb{R}$ angeschaut. Nun sei K ein endlicher Körper, etwa $K = \mathbb{Z}_3$. Dadurch ändert sich im Prinzip nichts, man muss in konkreten Rechnungen nur daran denken, dass wir uns eben nicht mehr in $\mathbb{R}$, sondern in $\mathbb{Z}_3$ befinden. Das bedeutet beispielsweise, dass $1 + 2 = 0$ gilt, da die Operationen $+$ und $\cdot$ ja die Addition und Multiplikation modulo 3 sind.

Beispiele: Es gelte $a(x), b(x) \in \mathbb{Z}_3[x]$ mit $a(x) = 1 + 2x + 2x^2$ und $b(x) = 2 + x$.

Wir wollen $(a + b)(x)$ und $(a \cdot b)(x)$ berechnen und schreiben der Deutlichkeit halber:

$$a(x) = 1 + 2x + 2x^2 + 0x^3,$$

$$b(x) = 2 + 1x + 0x^2 + 0x^3.$$

Es folgt:

$$\begin{aligned}(a + b)(x) &= (1 + 2) + (2 + 1)x + (2 + 0)x^2 \\ &= 2x^2\end{aligned}$$

und

$$\begin{aligned}(a \cdot b)(x) &= 1 \cdot 2 + (1 \cdot 1 + 2 \cdot 2)x + (1 \cdot 0 + 2 \cdot 1 + 2 \cdot 2)x^2 + \\ &\quad (1 \cdot 0 + 2 \cdot 0 + 2 \cdot 1 + 0 \cdot 2)x^3 \\ &= 2 + 2x + 2x^3.\end{aligned}$$

Satz 3.

Bezüglich der zuvor definierten Addition und Multiplikation für Polynome ist $K[x]$ ein Ring, in dem zusätzlich das Kommutativgesetz der Multiplikation gilt.

Auf den Beweis dieses Satzes wollen wir verzichten, da es sich um reine Routinearbeit handelt. Wir erwähnen nur Folgendes:

- Das *Nullpolynom* ist das neutrale Element der Addition.
- Das *konstante Polynom* $a(x) = 1$ ist das neutrale Element der Multiplikation.
- Zu $a(x) = a_0 + a_1x + \ldots + a_nx^n$ ist das Inverse der Addition gegeben durch $-a_0 - a_1x - \ldots - a_nx^n$; man bezeichnet dieses Polynom mit $-a(x)$ und nennt es *das Negative* von $a(x)$.

Man nennt einen Ring, in dem zusätzlich das Kommutativgesetz der Multiplikation gilt, einen *kommutativen Ring*. Man spricht außerdem von dem *Polynomring* $K[x]$ über dem Körper K. Wir können (etwas verkürzt) Satz 3 auch so aussprechen: $K[x]$ *ist ein kommutativer Ring.*

Frage: Wieso steht im vorangegangenen Absatz „Kommutativgesetz der *Multiplikation*“ und nicht etwa „Kommutativgesetz der Addition“?

Wenn Sie die Antwort nicht wissen, schauen Sie sich am besten noch einmal an, wie der Begriff „Ring“ definiert ist.

[3]Beweis als Übungsaufgabe. Hinweis: In einem Körper K ist $K \setminus \{0\}$ eine Gruppe bzgl. der Multiplikation; deshalb gilt insbesondere: $K \setminus \{0\}$ ist bzgl. $\cdot$ abgeschlossen.

7.3.3 Polynomdivision

Die aus der Schule bekannte Polynomdivision für reelle Polynome funktioniert nach demselben Schema auch für Polynome über einem beliebigen Körper K. Grundlegend ist folgender Satz über die *Existenz und Eindeutigkeit der Zerlegung mit Rest* für Polynome. (Einen Beweis dieses Satzes findet man im Lehrbuch von A. Steger, Diskrete Strukturen, Band 1.)

Satz 4.
Zu je zwei Polynomen $a(x), b(x) \in K[x]$ mit $b(x) \neq 0$ gibt es eindeutig bestimmte Polynome $q(x)$ und $r(x)$ aus $K[x]$ mit $\text{grad}(r) < \text{grad}(b)$ oder $r(x) = 0$, so dass

$$a(x) = q(x)b(x) + r(x).$$

Man nennt dies *Zerlegung mit Rest von a(x) bezüglich b(x).*

Wie findet man zu gegebenen $a(x)$ und $b(x) \in K[x]$ mit $b(x) \neq 0$ die zugehörigen Polynome $q(x)$ und $r(x)$? **Antwort**: Mit Hilfe des üblichen Verfahrens der „Polynomdivision“, das analog zum „schriftlichen Dividieren“ von ganzen Zahlen funktioniert.

Beispiel: Es seien $a(x), b(x) \in \mathbb{R}[x]$ mit $a(x) = 2x^4 + x^3 + x + 3$ und $b(x) = x^2 + x - 1$. Die durchzuführenden Rechnungen notiert man meist wie folgt. (Wir sprechen das Beispiel in der Vorlesung kurz durch; schriftliche Erläuterungen zu diesem Beispiel findet man im Buch von A. Steger. Wenn Sie sich in Bezug auf die Polynomdivision unsicher fühlen, sollten Sie sich im Tutorium „fit machen lassen“.)

$$\begin{array}{rllll} & (2x^4 & +x^3 & +x & +3) \quad : (x^2+x-1) = 2x^2 - x + 3, \text{ Rest: } -3x+6 \\ - & (2x^4 & +2x^3 & -2x^2) & \\ \hline & & -x^3 & +2x^2 & +x \quad +3 \\ & - & (-x^3 & -x^2 & +x) \\ \hline & & & 3x^2 & +3 \\ & & - & (3x^2 & +3x \quad -3) \\ \hline & & & & -3x \quad +6 \end{array}$$

Als *Ergebnis* erhält man hieraus folgende *Zerlegung mit Rest*:

$$\underbrace{2x^4 + x^3 + x + 3}_{a(x)} = \underbrace{(2x^2 - x + 3)}_{q(x)}\underbrace{(x^2 + x - 1)}_{b(x)} + \underbrace{(-3x + 6)}_{r(x)}.$$

Das Ergebnis lässt sich auch wie folgt schreiben:

$$\big(2x^4 + x^3 + x + 3\big) : \big(x^2 + x - 1\big) = 2x^2 - x + 3 + \frac{-3x + 6}{x^2 + x - 1}\ .$$

7.3.4 Der Euklidische Algorithmus für Polynome

Es sei ein Körper K fest gegeben. Mit $f(x)$, $g(x)$, $h(x)$, $a(x)$, $b(x)$, ... seien Polynome bezeichnet; alle betrachteten Polynome sollen aus $K[x]$ stammen. Man nennt $g(x)$ einen *Teiler* (oder *Faktor*) von $f(x)$, falls es ein $h(x) \in K[x]$ gibt mit

$$f(x) = g(x)h(x).$$

Man sagt auch, $f(x)$ ist ein *Vielfaches* von $g(x)$ oder auch $g(x)$ *teilt* $f(x)$ in $K[x]$. (Zusätze wie „in $K[x]$“ werden wir im Folgenden weglassen, da ja wie bereits gesagt, alle betrachteten Polynome aus $K[x]$ stammen sollen.)

Es seien nun zwei Polynome $a(x)$ und $b(x)$ gegeben. Ist $g(x)$ ein Teiler sowohl von $a(x)$ als auch von $b(x)$, so nennt man $g(x)$ einen *gemeinsamen Teiler* von $a(x)$ und $b(x)$. Ein Polynom $d(x) \in K[x]$ heißt ein *größter gemeinsamer Teiler* von $a(x)$ und $b(x)$, falls $d(x)$ ein gemeinsamer Teiler von $a(x)$ und $b(x)$ ist und falls für jeden gemeinsamen Teiler $t(x)$ von $a(x)$ und $b(x)$ gilt: $t(x)$ ist ein Teiler von $d(x)$.

Mitteilung: Es gibt im Allgemeinen nicht nur einen, sondern mehrere größte gemeinsame Teiler zweier Polynome $a(x)$ und $b(x)$; deshalb sprechen wir auch nicht von *dem* größten gemeinsamen Teiler, sondern nur von *einem* größten gemeinsamen Teiler: Ist beispielsweise für $K = \mathbb{R}$ das Polynom $d(x) = x + 4$ ein größter gemeinsamer Teiler zweier Polynome, so ist auch $2x + 8$ oder $11x + 44$ ein größter gemeinsamer Teiler dieser beiden Polynome.

Ist $d(x)$ ein größter gemeinsamer Teiler von $a(x)$ und $b(x)$ in $K[x]$, so besteht die Menge aller größten gemeinsamen Teiler aus den Polynomen der Form $k \cdot d(x)$ mit $k \in K \setminus \{0\}$. Also: *Verschiedene größte gemeinsame Teiler von $a(x)$ und $b(x)$ unterscheiden sich immer nur leicht, nämlich nur um einen konstanten Faktor $k \in K \setminus \{0\}$.*

Fordert man zusätzlich, dass $d(x)$ ein normiertes Polynom (d.h. mit Leitkoeffizient 1) ist, so ist $d(x)$ eindeutig bestimmt und man spricht vom *normierten größten gemeinsamen Teiler*.

Einen größten gemeinsamen Teiler $d(x)$ zweier Polynome kann man mit dem „Euklidischen Algorithmus für Polynome“ finden, der ganz ähnlich wie der Euklidische Algorithmus für ganze Zahlen abläuft.

Euklidischer Algorithmus zur Bestimmung eines größten gemeinsamen Teilers in K[x]

Eingabe: $a(x), b(x) \in K[x]$ mit $b(x) \neq 0$.

Ausgabe: ein größter gemeinsamer Teiler $d(x)$ von $a(x)$ und $b(x)$.

Man geht vor wie für ganzen Zahlen und bildet wiederholt *Zerlegungen mit Rest* solange, bis der Rest 0 auftritt; dann ist der letzte Rest, der ungleich 0 war (also der „vorletzte“ Rest) ein $d(x)$ wie gewünscht. Das Verfahren läuft so ab:

$a(x) = q_0(x)b(x) + r_0(x)$, mit $r_0(x) \neq 0$,
$b(x) = q_1(x)r_0(x) + r_1(x)$, mit $r_1(x) \neq 0$,
$r_0(x) = q_2(x)r_1(x) + r_2(x)$, mit $r_2(x) \neq 0$,
$r_1(x) = q_3(x)r_2(x) + r_3(x)$;

ist jetzt beispielsweise $r_3(x) = 0$, so ist $r_2(x)$ das ersehnte $d(x)$. (Ergibt sich gleich im ersten Schritt $r_0(x) = 0$, so ist $d(x) = b(x)$.)

Beispiel: Es seien $a(x), b(x) \in \mathbb{R}[x]$ mit $a(x) = x^3 - 1$ und $b(x) = x^2 - 2x + 1$. Es ergibt sich:

$x^3 - 1 = (x + 2)(x^2 - 2x + 1) + 3x - 3$,
$x^2 - 2x + 1 = (\frac{1}{3}x - \frac{1}{3})(3x - 3) + 0$.

Also ist $d(x) = 3x - 3$ ein größter gemeinsamer Teiler von $a(x)$ und $b(x)$ in $\mathbb{R}[x]$; der *normierte* größte gemeinsame Teiler von $a(x)$ und $b(x)$ ist $\frac{1}{3}d(x) = x - 1$.

7.3.5 Gleichheit von Polynomen

In manchen Situationen ist es nützlich, genau definiert zu haben, wann zwei Polynome aus $K[x]$ gleich sind. Zu diesem Zweck definieren wir zunächst, was wir unter der Koeffizientenfolge eines Polynoms verstehen wollen. Es sei $a(x)$ ein Polynom aus $K[x]$ mit $a(x) = a_0 + a_1x + \ldots + a_nx^n$; für alle $i \in \mathbb{N}$ mit $i > n$ setzen wir $a_i = 0$. Dann verstehen wir unter der *Koeffizientenfolge* von $a(x)$ die unendliche Folge

$$a_0,\ a_1,\ a_2,\ \ldots.$$

Man nennt nun zwei Polynome aus $K[x]$ *gleich*, wenn sie die gleiche Koeffizientenfolge besitzen. Das bedeutet:

Sind $a(x) = a_0 + a_1x + \ldots + a_nx^n$ und $b(x) = b_0 + b_1x + \ldots + b_mx^m$ Polynome aus $K[x]$, so sind $a(x)$ und $b(x)$ gleich, falls für die zugehörigen Koeffizientenfolgen $a_0, a_1, a_2, \ldots$ bzw. $b_0, b_1, b_2, \ldots$ gilt:

$$a_i = b_i \text{ für alle } i = 0, 1, 2, \ldots.$$

7.3.6 Polynomfunktionen

Wir wollen abschließend definieren, was die zu einem Polynom $a(x) = a_0 + a_1x + \ldots + a_nx^n$ aus $K[x]$ gehörige *Polynomfunktion* ist. Wir erläutern dies zunächst an Beispielen. Es sei $K = \mathbb{Z}_3$, d.h., K enthält nur die drei Elemente 0, 1 und 2 und gerechnet wird modulo 3. Es sei $a(x) = x^3 + x^2 + 2$. Setzt man für x nacheinander 0, 1 und 2 in $x^3 + x^2 + 2$ ein, so erhält man als Ergebnisse $0^3 + 0^2 + 2 = 2$, $1^3 + 1^2 + 2 = 1$ und $2^3 + 2^2 + 2 = 2$ (in $K = \mathbb{Z}_3$).

Zu dem Polynom $a(x) = x^3 + x^2 + 2 \in K[x]$ gehört also eine Funktion $f : \mathbb{Z}_3 \to \mathbb{Z}_3$, die durch folgende Tabelle beschrieben werden kann:

x	$f(x)$
0	2
1	1
2	2

In derselben Weise erhält man beispielsweise für das Polynom $b(x) = x^3 + x + 1$ eine zugehörige Funktion $g : \mathbb{Z}_3 \to \mathbb{Z}_3$:

x	$g(x)$
0	1
1	0
2	2

Es sei nun wieder K ein beliebiger Körper. Die obigen Beispiele dienten zur Vorbereitung der folgenden Definition.

Definition.

Gegeben sei ein Polynom $a(x) = a_0 + a_1x + \ldots + a_nx^n$ aus $K[x]$. Unter der zu $a(x)$ gehörigen *Polynomfunktion* versteht man die Funktion $K \to K$, die durch

$$k \longmapsto a_0 + a_1k + a_2k^2 + \ldots + a_nk^n$$

gegeben ist (für $k \in K$). (Um das Bild von $k \in K$ zu ermitteln, setzt man also k für x in das Polynom ein und rechnet das Ergebnis aus.)

Der Grund, weshalb zwischen einem Polynom und der zugehörigen Polynomfunktion unterschieden werden muss, ist folgender: Ist der zugrunde liegende Körper K ein endlicher Körper, so kann es durchaus vorkommen, dass zu zwei verschiedenen Polynomen dieselbe Polynomfunktion gehört. Hierzu ein **Beispiel**:

Es sei wie oben $K = \mathbb{Z}_3$ und das Polynom $c(x) \in K[x]$ sei gegeben durch

$$c(x) = x^4 + x + 2.$$

Die zugehörige Polynomfunktion $\mathbb{Z}_3 \to \mathbb{Z}_3$ ist dann dieselbe wie für das zuvor betrachtete Polynom

$$a(x) = x^3 + x^2 + 2.$$

Prüfen Sie durch Einsetzen nach, dass dies tatsächlich so ist!

Es sind also $a(x)$ und $c(x)$ verschiedene Polynome aus $\mathbb{Z}_3[x]$, die dieselbe Polynomfunktion besitzen:

$$a(x) = x^3 + x^2 + 2 \qquad\qquad c(x) = x^4 + x + 2$$
$$\searrow \qquad\qquad \swarrow$$
$$\text{dieselbe Polynomfunktion } f : \mathbb{Z}_3 \to \mathbb{Z}_3$$

Dass es für endliche Körper K unterschiedliche Polynome mit derselben Polynomfunktion geben muss, ist übrigens nicht verwunderlich, da es unendlich viele verschiedene Polynome in $K[x]$ gibt, aber nur endlich viele verschiedene Abbildungen $K \to K$.

Man kann im Übrigen beweisen, dass für unendliche Körper K (wie $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$) Derartiges nicht passieren kann: Ist K unendlich, so gehören zu zwei verschiedenen Polynomen auch immer verschiedene Funktionen $K \to K$ (vgl. etwa H. Heuser, Lehrbuch der Analysis, Teil 1 oder K. Jänich, Lineare Algebra).

Zur Übung: Es sei $K = \mathbb{Z}_2$.

a) Man bestimme die zugehörigen Polynomfunktionen: $a(x) = x$, $b(x) = x + 1$, $c(x) = x^2$, $d(x) = x^2 + x + 1$.

b) Man gebe drei verschiedene Polynome aus $\mathbb{Z}_2[x]$ an, für deren Polynomfunktionen f gilt: $f(0) = f(1) = 0$.

8 Literatur

- M. Aigner:
  Diskrete Mathematik. Vieweg-Verlag.
- A. Beutelspacher:
  Lineare Algebra. Vieweg-Verlag.
- A. Beutelspacher, M.-A. Zschiegner:
  Diskrete Mathematik für Einsteiger. Vieweg-Verlag.
- N. L. Biggs:
  Discrete Mathematics. Oxford University Press.
- R. Diestel:
  Graphentheorie. Springer-Verlag.
- S. Even:
  Algorithmic Combinatorics. MacMillan.
- G. Fischer:
  Lineare Algebra. Vieweg-Verlag.
- R. Graham, D. Knuth, O. Patashnik:
  Concrete Mathematics. Addison-Wesley.
- G. M. Gramlich:
  Lineare Algebra. Hanser.
- D. Hachenberger:
  Mathematik für Informatiker. Pearson.
- W. Hochstättler:
  Algorithmische Mathematik. Springer-Verlag.
- Th. Ihringer:
  Diskrete Mathematik. Heldermann-Verlag.
- K. Jänich:
  Lineare Algebra. Springer-Verlag.
- D. Jungnickel:
  Graphen, Netzwerke und Algorithmen. BI-Wissenschaftsverlag.
- B. Kreußler, G. Pfister:
  Mathematik für Informatiker. Springer.
- L. Lovász, J. Pelikán, K. Vesztergombi:
  Diskrete Mathematik. Springer-Verlag.
- J. Matoušek, J. Nešetril:
  Diskrete Mathematik, eine Entdeckungsreise. Springer-Verlag.

- E. R. Scheinerman:
  Mathematics - A Discrete Introduction. Brooks/Cole.
- A. Steger:
  Diskrete Strukturen, Band 1. Springer-Verlag.
- G. Teschl, S. Teschl:
  Mathematik für Informatiker. Band 1 (Diskrete Mathematik und Lineare Algebra). Springer.
- P. Tittmann:
  Einführung in die Kombinatorik. Spektrum.
- J. K. Truss:
  Discrete Mathematics for Computer Scientists. Addison-Wesley.
- R. J. Wilson:
  Einführung in die Graphentheorie. Vandenhoeck und Ruprecht.

Index