Gerald Teschl
Susanne Teschl

Mathematik für Informatiker

Band 1: Diskrete Mathematik und Lineare Algebra

4. Auflage
Mit 108 Abbildungen

Springer

Gerald Teschl
Universität Wien
Fakultät für Mathematik
Oskar-Morgenstern-Platz 1
1090 Wien, Österreich
Gerald.Teschl@univie.ac.at
http://www.mat.univie.ac.at/~gerald/

Susanne Teschl
Fachhochschule Technikum Wien
Höchstädtplatz 5
1200 Wien, Österreich
Susanne.Teschl@technikum-wien.at
http://staff.technikum-wien.at/~teschl/

ISBN 978-3-540-77431-0 e-ISBN 978-3-540-77432-7

DOI 10.1007/978-3-540-77432-7

ISSN 1614-5216

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Einbandgestaltung: KünkelLopka Werbeagentur, Heidelberg

Gedruckt auf säurefreiem Papier

9 8 7 6 5 4 3 2 1

springer.com

Inhaltsverzeichnis

Grundlagen

Diskrete Mathematik

Lineare Algebra

1

Logik und Mengen

1.1 Elementare Logik

Die Logik ist ein wichtiges Hilfsmittel in der Informatik. Sie wird beim Entwurf von Programmen gebraucht oder um die Korrektheit von Algorithmen zu verifizieren. Sie hilft bei der Beantwortung von Fragen wie „Hat die Switch-Anweisung wohl nichts übersehen?“ oder „Arbeitet der Algorithmus wohl in allen Spezialfällen so, wie ich es möchte?“. Die Logik ist notwendig, um Anforderungen eindeutig und widerspruchsfrei zu formulieren. Was ist zum Beispiel die Verneinung von „Jeder Benutzer hat ein Passwort“? Es gibt in der Umgangssprache verschiedene Möglichkeiten, die nach den Regeln der Logik richtige Verneinung ist aber eindeutig: „Es gibt mindestens einen Benutzer, der kein Passwort hat“. (Nicht nur) für Informatiker ist logisch-analytisches Denkvermögen eine wichtige Anforderung, und daher steht die Logik auch am Anfang unseres Weges.

Definition 1.1 Eine **Aussage** (engl. *proposition*) ist ein Satz, von dem man eindeutig entscheiden kann, ob er wahr oder falsch ist.

Der Wahrheitswert „wahr“ wird dabei mit „w“ oder „1“ abgekürzt, der Wahrheitswert „falsch” mit „f“ oder „0“.

Unsere Definition ist etwas optimistisch. Bei einer axiomatischen Behandlung der Mathematik stellt sich leider heraus, dass nicht jede Aussage entscheidbar ist. Genau das sagt nämlich der berühmte **Unvollständigkeitssatz** des österreichischen Mathematikers Kurt Gödel (1906–1978): In jeder formalen Theorie, die mindestens so mächtig wie die Theorie der natürlichen Zahlen (Peano-Arithmetik) ist, bleiben wahre (und falsche) arithmetische Formeln übrig, die nicht innerhalb der Theorie beweisbar (widerlegbar) sind. Wir werden aber zum Glück auf keine dieser Aussagen stoßen.

Beispiel 1.2 Aussagen
Handelt es sich um eine Aussage?
a) Wien ist die Hauptstadt von Österreich.
b) $1 + 5 = 6$.
c) 5 ist kleiner als 3.
d) Guten Abend!
e) $x + 3 = 5$.

Lösung zu 1.2 a) und b) sind wahre Aussagen, c) ist eine falsche Aussage; d) ist keine Aussage, weil nicht gesagt werden kann, dass dieser Satz wahr oder falsch

ist. e) ist keine Aussage, weil x unbekannt ist. Wir können daraus aber sofort eine Aussage machen, indem wir eine Zahl für x einsetzen. Mit solchen so genannten *Aussageformen* werden wir uns etwas später genauer beschäftigen. ■

Aussagen werden in der Umgangssprache durch Wörter wie „und“, „oder“, usw. zu neuen Aussagen verknüpft. Der Gebrauch dieser Wörter ist umgangssprachlich nicht immer ganz klar geregelt und kann daher zu Missverständnissen führen. In der Logik ist die Verknüpfung von gegebenen Aussagen zu neuen Aussagen aber eindeutig festgelegt. Wir bezeichnen dazu beliebige gegebene Aussagen mit $a, b, c, \ldots$

Zunächst kann man durch die Verneinung einer Aussage eine neue Aussage bilden:

Definition 1.3 Die **Verneinung** oder **Negation** einer Aussage a ist genau dann wahr, wenn a falsch ist. Die Verneinung von a wird symbolisch mit $\overline{a}$ oder $\neg a$ bezeichnet (gelesen „nicht a“).

Sprachlich wird die Verneinung gebildet, indem man vor die zu verneinende Aussage das Wort „Nicht“ oder den Zusatz „Es trifft nicht zu, dass“ setzt und danach sinngemäß sprachlich vereinfacht.

Beispiel 1.4 Verneinung
Verneinen Sie folgende Aussagen mithilfe des Zusatzes „Nicht“ oder „Es trifft nicht zu, dass“ und finden Sie eine alternative, möglichst einfache sprachliche Formulierung:
a) Der Tank ist voll.
b) Alle Studenten sind anwesend.
c) Ich bin vor 1990 geboren.

Lösung zu 1.4
a) Die Verneinung ist „Es trifft nicht zu, dass der Tank voll ist“ bzw., etwas einfacher, „Der Tank ist nicht voll“. Achtung: Im ersten Moment möchte man als Verneinung vielleicht „Der Tank ist leer“ sagen. Das ist aber nicht gleichbedeutend mit „Der Tank ist nicht voll“, denn er könnte ja auch halb voll sein.
b) Die Verneinung ist „Nicht alle Studenten sind anwesend“ oder, anders ausgedrückt, „Mindestens ein Student fehlt“. („Kein Student ist anwesend“ ist nicht die richtige Verneinung.)
c) Die Verneinung ist „Ich bin nicht vor 1990 geboren“, was gleichbedeutend ist mit „Ich bin im Jahr 1990 oder nach 1990 geboren“. ■

Als Nächstes wollen wir die wichtigsten Möglichkeiten, zwei Aussagen miteinander zu verknüpfen, besprechen:

Definition 1.5 Seien a und b beliebige Aussagen (in diesem Zusammenhang auch als **Eingangsaussagen** bezeichnet.)

- Die **UND**-Verknüpfung oder **Konjunktion** von a und b wird symbolisch mit $a \wedge b$ bezeichnet (gelesen: „a und b“). Die neue Aussage $a \wedge b$ ist genau dann wahr, wenn sowohl a als auch b wahr ist. Ansonsten ist $a \wedge b$ falsch.

- Die **ODER**-Verknüpfung oder **Disjunktion** von a und b wird symbolisch mit $a \vee b$ bezeichnet (gelesen: „a oder b“). Die neue Aussage $a \vee b$ ist genau dann wahr, wenn mindestens eine der beiden Aussagen a bzw. b wahr ist; ansonsten ist $a \vee b$ falsch. Die Verknüpfung $a \vee b$ entspricht dem *nicht-ausschließenden* „oder“ (denn $a \vee b$ ist auch wahr, wenn sowohl a als auch b wahr ist).
- Die **ENTWEDER ... ODER**-Verknüpfung von a und b wird symbolisch mit $a \operatorname{xor} b$ (vom englischen *eXclusive OR*) oder $a \oplus b$ bezeichnet. Die neue Aussage $a \operatorname{xor} b$ ist genau dann wahr, wenn entweder a oder b (aber nicht beide gleichzeitig) wahr sind. Die Verknüpfung $a \operatorname{xor} b$ entspricht dem *ausschließenden* „oder“.

Eselsbrücke: Das Symbol $\wedge$ erinnert an den Anfangsbuchstaben des englischen **A**ND.

Verknüpfte Aussagen lassen sich am besten durch ihre **Wahrheits(werte)tabelle** beschreiben. Dabei werden die möglichen Kombinationen von Wahrheitswerten der Eingangsaussagen a und b (bzw. im Fall der Verneinung die möglichen Wahrheitswerte der Eingangsaussage a) angegeben, und dazu der entsprechende Wahrheitswert der verknüpften Aussage:

a	$\overline{a}$
0	1
1	0

a	b	$a \wedge b$	$a \vee b$	$a \operatorname{xor} b$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

Daraus kann man zum Beispiel bequem ablesen, dass die Aussage $a \wedge b$ nur dann wahr ist (d.h. Wahrheitswert 1 hat), wenn sowohl a als auch b wahr ist. Für alle anderen Kombinationen von Wahrheitswerten von a und b ist $a \wedge b$ eine falsche Aussage.

Beispiel 1.6 UND- bzw. ODER- Verknüpfung
Geben Sie jeweils die Wahrheitswerte der Aussagen $a \wedge b$, $a \vee b$ und $a \operatorname{xor} b$ an:
a) a: Wien liegt in Österreich; b: Wien liegt in Deutschland
b) a: $2 < 3$; b: $1 + 1 = 2$

Lösung zu 1.6
a) Wir stellen zunächst fest, dass a wahr ist und dass b falsch ist. Damit stehen nach den Regeln der Logik auch schon die Wahrheitswerte der verknüpften Aussagen fest (unabhängig von der inhaltlichen Bedeutung der entstehenden verknüpften Aussagen):
• $a \wedge b$ („Wien liegt in Österreich und (Wien liegt in) Deutschland“) ist eine falsche Aussage, da eine der Eingangsaussagen, nämlich b, falsch ist.
• $a \vee b$ („Wien liegt in Österreich oder Deutschland“) ist eine wahre Aussage, da zumindest eine der Eingangsaussagen wahr ist.
• $a \operatorname{xor} b$ („Wien liegt entweder in Österreich oder in Deutschland“) ist eine wahre Aussage, da genau eine der Eingangsaussagen wahr ist (nicht aber beide).
b) Da sowohl a als auch b wahr ist, folgt: $a \wedge b$ ist wahr, $a \vee b$ ist wahr, $a \operatorname{xor} b$ ist falsch. ■

Die Verwendung von „und“ bzw. „oder“ in der Aussagenlogik stimmt in den meisten Fällen mit dem überein, was wir uns erwarten würden. Manchmal gibt es aber in der Umgangssprache Formulierungen, bei denen die Bedeutung nur aus dem Zusammenhang klar ist: Wenn zum Beispiel auf einem Schild „Rauchen *und* Hantieren mit offenem Feuer verboten!“ steht, dann weiß jeder, dass man hier weder Rauchen noch mit offenem Feuer hantieren darf. Vom Standpunkt der Aussagenlogik aus bedeutet das Verbot aber, dass nur *gleichzeitiges* Rauchen und Hantieren mit offenem Feuer verboten ist, es aber zum Beispiel erlaubt wäre, mit offenem Feuer zu hantieren, solange man dabei nicht raucht. Nach den Regeln der Aussagenlogik müsste das Verbot „Rauchen *oder* Hantieren mit offenen Feuer verboten!“ lauten (eine Argumentation, die Ihnen aber wohl vor einem Richter nicht helfen würde, nachdem die Tankstelle abgebrannt ist).

Definition 1.7 Ersetzt man in einer Aussage a irgendeine Konstante durch eine Variable x, so entsteht eine **Aussageform** $a(x)$ (auch **Aussagefunktion** genannt).

Beispiel: $a(x)$: $x < 100$ ist eine Aussageform. Sie besteht aus zwei Teilen: aus der Variablen x und aus dem so genannten **Prädikat** „ist kleiner 100“. Man spricht auch von **Prädikatenlogik**. Eine Aussageform $a(x)$ wird zu einer Aussage, wenn man für x ein konkretes Objekt einsetzt. Wenn für x zum Beispiel der Wert 3 eingesetzt wird, entsteht die wahre Aussage $a(3)$: $3 < 100$.

Beispiel 1.8 Aussageform
Gegeben sind die Aussageformen $a(x)$: $x^2 < 15$ und $b(x)$: $x^2 + 1 = 5$.
a) Ist die Aussage $a(1)$ wahr oder falsch?
b) Ist $b(1)$ wahr oder falsch?

Lösung zu 1.8
a) Wir setzen in der Aussageform $a(x)$ für x den Wert 1 und erhalten damit die Aussage $a(1)$: $1 < 15$. Sie ist wahr.
b) Die Aussage $b(1)$ lautet: $1 + 1 = 5$. Sie ist falsch. ■

Aussageformen können wie Aussagen verneint bzw. mit $\wedge, \vee$, xor verknüpft werden. Es entsteht dadurch eine neue Aussageform:

Beispiel 1.9 Verknüpfungen von Aussageformen
Gegeben sind wieder $a(x)$: $x^2 < 15$ und $b(x)$: $x^2 + 1 = 5$.
a) Verneinen Sie $a(x)$. b) Verneinen Sie $b(x)$.
c) Geben Sie Beispiele für Werte von x an, für die die verknüpfte Aussageform $a(x) \wedge b(x)$ eine wahre bzw. eine falsche Aussage wird.

Lösung zu 1.9
a) Die Verneinung von $a(x)$ ist die Aussageform $\overline{a(x)}$: $x^2 \geq 15$. (Achtung: Die Verneinung ist nicht „$x^2 > 15$“. Denn „nicht kleiner“ ist gleichbedeutend mit „gleich oder größer“.)
b) Die Verneinung ist $\overline{b(x)}$: $x^2 + 1 \neq 5$.
c) Setzen wir in $a(x) \wedge b(x)$ für x den Wert 1 ein, dann erhalten wir die Aussage: $a(1) \wedge b(1)$. Sie ist falsch, weil $b(1)$ falsch ist.
Wenn wir $x = 2$ setzen, so entsteht die Aussage: $a(2) \wedge b(2)$. Da sowohl $a(2)$: $2^2 < 15$ als auch $b(2)$: $2^2 + 1 = 5$ wahr ist, ist auch $a(2) \wedge b(2)$ wahr. ■

Eine weitere Möglichkeit, um aus Aussageformen Aussagen zu erzeugen, ist die Verwendung von Quantoren. Darunter versteht man einfach die Zusätze „Für alle“ oder „Für ein“:

Definition 1.10 (All-Aussagen und Existenz-Aussagen) Gegeben ist eine Aussageform $a(x)$.

- Die Aussage „Für alle x (aus einer bestimmten Menge) gilt $a(x)$“ ist wahr genau dann, wenn $a(x)$ für alle in Frage kommenden x wahr ist. Abkürzend schreibt man für diese **All-Aussage**
$$\forall x\colon a(x),$$
wobei $\forall$ „für alle“ gelesen wird (oder „für jedes“). Das Symbol $\forall$ heißt **All-Quantor**.
- Die Aussage „Es gibt ein x (aus einer bestimmten Menge), sodass $a(x)$“ ist wahr genau dann, wenn $a(x)$ für *zumindest* eines der in Frage kommenden x wahr ist. Symbolisch schreibt man diese **Existenz-Aussage** als
$$\exists x\colon a(x),$$
wobei $\exists$ „es gibt (mindestens) ein“ gelesen wird (oder auch: „es existiert (mindestens) ein“ oder „für (mindestens) ein“). Das Symbol $\exists$ heißt **Existenz-Quantor**.

Bei der Verwendung mehrerer Quantoren ist ihre Reihenfolge wesentlich.

Beispiel 1.11 Für alle ...
a) Ist „Für alle natürlichen Zahlen x gilt: $x+1 > x$“ eine wahre oder eine falsche Aussage?
b) Ist die Aussage „Für alle natürlichen Zahlen x ist $x > 3$“ wahr oder falsch?

Lösung zu 1.11
a) Diese Aussage hat die Form „$\forall$ natürlichen x: $a(x)$“, wobei $a(x)$ die Aussageform „$x + 1 > x$“ ist. Sie ist wahr, denn welche natürliche Zahl wir auch immer für x einsetzen, $a(x)$ ist immer eine wahre Aussage: $a(1)$ ist wahr und $a(2)$ ist wahr und ... ist wahr.
b) Die Aussage hat die Form „Für alle natürlichen Zahlen x gilt: $a(x)$“, wobei $a(x)$ die Aussageform „$x > 3$“ bedeutet. Nun können wir aber (mindestens) ein natürliches x finden, für das $a(x)$ falsch ist, z. B. $x = 1$. Damit ist die gegebene All-Aussage falsch. ■

Wichtig ist also: Um nachzuweisen, dass eine All-Aussage „$\forall x$: $a(x)$“ wahr ist, muss man für *jedes einzelne* x sichergehen, dass $a(x)$ wahr ist. Um nachzuweisen, dass eine All-Aussage „$\forall x$: $a(x)$“ falsch ist, muss man *(mindestens) ein* x finden, für das $a(x)$ falsch ist.

Noch ein Beispiel: Ich möchte feststellen, ob die All-Aussage „$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ für alle natürlichen Zahlen“ wahr ist. Wie gehe ich vor? Am besten bestimme ich einmal den Wahrheitswert der Aussage für eine konkrete natürliche Zahl, z. B. für $n = 5$: $1+2+3+4+5 = 15$ ist tatsächlich dasselbe wie $\frac{5\cdot 6}{2}$. Vielleicht probiere ich die Formel auch noch für ein paar andere natürliche Zahlen. Wenn (so wie hier) auf diese Weise kein n gefunden wird, für das die Aussage falsch ist, dann spricht

so weit nichts gegen die Richtigkeit der Formel. Nun muss ich aber noch beweisen, dass sie für *alle*, also *jedes beliebige*, natürliche n gilt. Wie soll das funktionieren, dazu müsste man ja unendlich viele Zahlen probieren?! – Durch Probieren kommt man hier wirklich nicht weiter. Abhilfe kommt hier zum Beispiel durch die Beweismethode der *Vollständigen Induktion*, die wir in einem späteren Kapitel kennen lernen werden.

Beispiel 1.12 Es existiert ein ...
a) Ist „Es existiert eine ganze Zahl x mit $x^2 = 4$“ wahr oder falsch?
b) Ist die Aussage „Es gibt eine natürliche Zahl x mit $x^2 < 0$“ wahr oder falsch?

Lösung zu 1.12
a) Wir haben es mit der Existenz-Aussage „$\exists$ ganze Zahl x mit $a(x)$“ zu tun, wobei $a(x)$ die Aussageform „$x^2 = 4$“ ist. Wir können eine ganze Zahl finden, z. B. $x = 2$, für die $a(2)$ wahr ist. Daher ist die gegebene Existenz-Aussage wahr. Beachten Sie, dass „Es existiert *ein*“ immer im Sinn von *mindestens ein* gemeint ist (und nicht im Sinn von *genau ein*). Es ist also kein Problem, dass hier auch $a(-2)$ wahr ist.
b) Die Aussage hat die Form „$\exists$ natürliches x mit $a(x)$“, wobei $a(x)$ die Aussageform „$x^2 < 0$“ bedeutet. Welche natürliche Zahl x wir auch probieren, wir können keine finden, für die $a(x)$ wahr ist. Daher ist die gegebene Existenz-Aussage falsch. ■

Wichtig ist also hier: Um nachzuweisen, dass eine Existenz-Aussage „$\exists x$: $a(x)$“ wahr ist, muss man *mindestens ein* x finden, für das $a(x)$ wahr ist. Um nachzuweisen, dass eine Existenz-Aussage „$\exists x$: $a(x)$“ falsch ist, muss man *jedes einzelne* x untersuchen und sichergehen, dass $a(x)$ für alle x falsch ist.

All- und Existenzaussagen werden – wie jede Aussage – sprachlich mithilfe der Worte „Nicht“ bzw. „Es trifft nicht zu, dass“ verneint. Aus ihrer Definition folgt:

Satz 1.13 (Verneinung von All- und Existenzaussagen) Durch die Verneinung einer All-Aussage entsteht eine Existenz-Aussage, und umgekehrt entsteht durch die Verneinung einer Existenz-Aussage eine All-Aussage:

$$\begin{aligned} \overline{\text{Für alle } x \text{ gilt } a(x)} &= \text{Es existiert ein } x, \text{ sodass } \overline{a(x)} \\ \overline{\text{Es existiert ein } x \text{ mit } a(x)} &= \text{Für alle } x \text{ gilt } \overline{a(x)} \end{aligned}$$

oder kürzer:

$$\begin{aligned} \overline{\forall x\colon a(x)} &= \exists x\colon \overline{a(x)} \\ \overline{\exists x\colon a(x)} &= \forall x\colon \overline{a(x)}. \end{aligned}$$

Wenn Mathematiker lange über etwas gegrübelt haben und durch Schlussfolgerungen auf eine neue wichtige Erkenntnis gestoßen sind, dann bezeichnen sie diese Erkenntnis als **Satz** oder **Theorem**, und auch wir werden an dieser Tradition festhalten. Die Schlussfolgerungen müssen dabei aber immer absolut wasserdicht sein! Einfach eine Vermutung äußern, die dann gilt, bis jemand sie widerlegt, zählt in der Mathematik nicht! Auch die Schlussfolgerung „Weil es in allen Testfällen richtig war, ist es wohl immer richtig“ wird nicht akzeptiert. (Es muss in allen Fällen, nicht nur den getesteten Fällen, richtig sein.)

Beispiel 1.14 Verneinung von All- und Existenzaussagen
Verneinen Sie, indem Sie die All- in eine Existenzaussage umwandeln, bzw. umgekehrt, und sprachlich vereinfachen:
a) Alle Menschen mögen Mathematik.
b) Es gibt einen Studenten, der Spanisch spricht.
c) $\forall x$: $x > 3$

Lösung zu 1.14
a) Die gegebene Aussage ist „$\forall x$: x mag Mathematik“ (wobei x ein beliebiger Mensch ist). Verneinung: „$\exists x$: $\overline{x \text{ mag Mathematik}}$“, also „$\exists x$: x mag Mathematik nicht“, also „Es gibt (mindestens) einen Menschen, der Mathematik nicht mag“.
b) Die Aussage hat die Form „$\exists x$: x spricht Spanisch“ (wobei x ein beliebiger Student ist). Verneinung: „$\forall x$: $\overline{x \text{ spricht Spanisch}}$“, in Worten: „$\forall x$: x spricht nicht Spanisch“, also „Für jeden Studenten gilt: Er/sie spricht nicht Spanisch“, bzw. „Kein Student spricht Spanisch“.
c) Die Verneinung ist $\exists x$: $\overline{x > 3}$, also $\exists x$: $x \leq 3$. In Worten: Die Verneinung von „Alle x sind größer als 3“ ist „Nicht alle x sind größer als 3“ bzw. „Es gibt (zumindest) ein x, das kleiner oder gleich 3 ist.“ ■

In der Mathematik sind Schlussfolgerungen besonders wichtig. Sie werden durch die folgenden Verknüpfungen beschrieben:

Definition 1.15 Die **WENN-DANN-Verknüpfung** oder **Subjunktion** $a \to b$ (gelesen „Wenn a, dann b“) und die **GENAU-DANN-Verknüpfung** oder **Bijunktion** $a \leftrightarrow b$ (gelesen „a genau dann, wenn b“) von zwei Aussagen a bzw. b sind durch ihre Wahrheitstabellen folgendermaßen definiert:

a	b	$a \to b$	$a \leftrightarrow b$
0	0	1	1
0	1	1	0
1	0	0	0
1	1	1	1

Die neue Aussage $a \to b$ ist also nur dann falsch, wenn a wahr und b falsch ist; in allen anderen Fällen ist $a \to b$ wahr. Die neue Aussage $a \leftrightarrow b$ ist genau dann wahr, wenn beide Eingangsaussagen den gleichen Wahrheitswert haben, wenn also a und b beide wahr oder beide falsch sind.

Zunächst beschäftigen wir uns mit der Aussage $a \to b$:

Beispiel 1.16 WENN-DANN-Verknüpfung
„Wenn es neblig ist, dann ist die Sicht schlecht“ ist wahr (davon gehen wir aus). Diese Aussage hat die Form $a \to b$, wobei a: „Es ist neblig“ bzw. b: „Die Sicht ist schlecht“ bedeutet. Was kann damit über die Sicht (den Wahrheitswert von b) gesagt werden, wenn es nicht neblig ist (also wenn a falsch ist)?

Lösung zu 1.16 Laut Wahrheitstabelle ist $a \to b$ für folgende Kombinationen wahr: a wahr, b wahr (also Nebel, schlechte Sicht); a falsch, b wahr (also kein Nebel,

schlechte Sicht); a falsch, b falsch (also kein Nebel, gute Sicht). Wir sehen insbesondere, dass, wenn a falsch ist, b falsch oder wahr sein kann. Das heißt, wenn es nicht neblig ist (a falsch), so kann die Sicht gut oder schlecht (weil es z. B. dunkel ist oder stark regnet) sein. Wir wissen also, wenn es nicht neblig ist, nichts über die Sicht. (Wir haben hier einfachheitshalber „gute Sicht“ als Verneinung von „schlechte Sicht” verwendet.) ■

Wichtig ist nun vor allem folgende Schreibweise, der Sie immer wieder begegnen werden:

Definition 1.17 Ist die verknüpfte Aussage $a \to b$ wahr, so spricht man von einem **logischen Schluss** (oder einer **Implikation**) und schreibt

$$a \Rightarrow b.$$

Für $a \Rightarrow b$ sagt man: „**Aus** a **folgt** b“ oder „a **impliziert** b“, oder **„Wenn** a**, dann** b“ oder „a **ist hinreichend für** b“ oder „b **ist notwendig für** a“.

Wenn Sie also $a \Rightarrow b$ sehen, so bedeutet das: *Wenn a wahr ist, so ist auch b wahr. Wenn a falsch ist, so kann b wahr oder falsch sein.* Für Aussageformen bedeutet $a(x) \Rightarrow b(x)$, dass $a(x) \to b(x)$ für alle x wahr ist.

Wir können insbesondere im obigen Beispiel schreiben: „Es ist neblig $\Rightarrow$ Die Sicht ist schlecht“ und dazu in Worten sagen: „Aus Nebel folgt schlechte Sicht“ oder „Nebel impliziert schlechte Sicht“ oder „Wenn es neblig ist, ist die Sicht schlecht“ oder „Nebel ist hinreichend für schlechte Sicht“ oder „Schlechte Sicht ist notwendig für Nebel“.

Zwei verknüpfte Aussagen werden als **gleich** (oder **logisch äquivalent**) bezeichnet, wenn sie für jede Kombination der Wahrheitswerte der Eingangsaussagen die gleichen Wahrheitswerte annehmen. Aus der folgenden Tabelle

a	b	$\overline{a}$	$\overline{b}$	$a \to b$	$\overline{b} \to \overline{a}$	$b \to a$	$a \leftrightarrow b$	$(a \to b) \wedge (b \to a)$
0	0	1	1	1	1	1	1	1
0	1	1	0	1	1	0	0	0
1	0	0	1	0	0	1	0	0
1	1	0	0	1	1	1	1	1

sehen wir zum Beispiel, dass $a \to b = \overline{b} \to \overline{a}$, da die fünfte und sechste Spalte dieselben Wahrheitswerte haben. Daraus folgt die wichtige Tatsache:

Satz 1.18 $a \Rightarrow b$ bedeutet dasselbe wie $\overline{b} \Rightarrow \overline{a}$.

Aber Achtung: Wir sehen auch, dass $a \to b \neq b \to a$. Mit anderen Worten: $a \Rightarrow b$ ist gleichbedeutend mit $\overline{b} \Rightarrow \overline{a}$, jedoch nicht gleichbedeutend mit $b \Rightarrow a$.

Beispiel 1.19 Richtige Schlussfolgerung

a) Es gilt: „Nebel $\Rightarrow$ schlechte Sicht“. Gilt auch „keine schlechte Sicht $\Rightarrow$ kein Nebel“?
b) Es gilt: „Nebel $\Rightarrow$ schlechte Sicht“. Gilt auch „schlechte Sicht $\Rightarrow$ Nebel“?

c) Es gilt (für jedes x): „$x > 3 \Rightarrow x > 0$“. Gilt auch „$x \leq 0 \Rightarrow x \leq 3$“?
d) Es gilt (für jedes x): „$x > 3 \Rightarrow x > 0$“. Gilt auch „$x > 0 \Rightarrow x > 3$“?

Lösung zu 1.19

a) Ja, denn $a \Rightarrow b$ ist gleich(bedeutend wie) $\overline{b} \Rightarrow \overline{a}$.
b) Zunächst ist uns bewusst, dass grundsätzlich $a \Rightarrow b$ etwas anderes bedeutet als $b \Rightarrow a$. Überlegen wir, ob auch $b \Rightarrow a$ gilt, also „schlechte Sicht $\Rightarrow$ Nebel“? Nein, denn: Wenn die Sicht schlecht ist, dann folgt daraus nicht notwendigerweise Nebel (es könnte ja auch kein Nebel, dafür aber Dunkelheit sein).
c) Gleichbedeutend mit „$x > 3 \Rightarrow x > 0$“ ist: „$\overline{x > 0} \Rightarrow \overline{x > 3}$“, also „$x \leq 0 \Rightarrow x \leq 3$“.
d) Wieder ist uns bewusst, dass $a \Rightarrow b$ nicht gleichbedeutend mit $b \Rightarrow a$ ist. Gilt aber vielleicht auch „$x > 0 \Rightarrow x > 3$“? D.h., ist „$x > 0 \to x > 3$“ wahr für alle x? Nein, denn für $x = 2$ ist $x > 0$ wahr, aber $x > 3$ falsch. Also haben wir $x > 0 \not\Rightarrow x > 3$ gezeigt. ■

Durch Blick auf die letzte Wahrheitstabelle sehen wir, dass $a \leftrightarrow b$ immer dann wahr ist, wenn $(a \to b) \wedge (b \to a)$ wahr ist; wenn also sowohl $a \Rightarrow b$ als auch $b \Rightarrow a$ gilt; d.h., wenn a hinreichend und notwendig für b ist. Dafür verwendet man nahe liegend folgende Schreibweise:

Definition 1.20 Wenn $a \leftrightarrow b$ wahr ist, dann spricht man von **Äquivalenz** und schreibt

$$a \Leftrightarrow b.$$

Die Äquivalenz $a \Leftrightarrow b$ bedeutet, dass sowohl $a \Rightarrow b$ als auch $b \Rightarrow a$ gilt. Man sagt: „a **genau dann, wenn** b“ oder „a **dann und nur dann, wenn** b“ oder „a **ist notwendig und hinreichend für** b“.

Wenn Sie also $a \Leftrightarrow b$ sehen, so bedeutet das: *Die Aussagen a und b haben denselben Wahrheitswert.*

Beispiel 1.21 Genau dann, wenn ...

a) „x ist eine gerade Zahl $\leftrightarrow$ x ist durch 2 teilbar“ ist (für jedes x) eine wahre Aussage. Daher: „x gerade $\Leftrightarrow$ x durch 2 teilbar“. Gelesen: „x ist gerade genau dann, wenn x durch 2 teilbar ist“ oder „x ist gerade dann und nur dann, wenn x durch 2 teilbar ist“.
b) Wir haben im letzten Beispiel gezeigt, dass zwar „$x > 3 \Rightarrow x > 0$“, aber „$x > 0 \not\Rightarrow x > 3$“ gilt. Also „$x > 3 \not\Rightarrow x > 0$“.

In der Mathematik wird großer Wert auf richtige Schlussfolgerungen gelegt, wie auch folgende kleine Anekdote zeigt: Ein Chemiker, ein Physiker und ein Mathematiker reisen in einem Zug durch Schottland. Als sie aus dem Fenster sehen, erblicken sie ein schwarzes Schaf auf der Weide. Der Chemiker bemerkt: „Aha, in Schottland sind die Schafe also schwarz“. Der Physiker bessert ihn sofort aus: „Nein, in Schottland gibt es ein schwarzes Schaf“. Der Mathematiker schüttelt nur den Kopf und meint: „In Schottland gibt es ein Schaf, das auf der uns zugewandten Seite schwarz ist“.

In der Logik geht es unter anderem darum, aus wahren Aussagen logisch richtige Schlussfolgerungen zu ziehen und somit zu neuen wahren Aussagen zu kommen.

Man spricht in diesem Zusammenhang von einem **Beweis**. Aus der letzten Wahrheitstabelle kann man einige mögliche Beweistechniken ablesen:

- $(a \to b) \wedge (b \to a) = a \leftrightarrow b$: Um $a \Leftrightarrow b$ zu zeigen, kann man zeigen, dass sowohl $a \Rightarrow b$ als auch $b \Rightarrow a$ gilt.
- $\overline{b} \to \overline{a} = a \to b$: Um $a \Rightarrow b$ zu zeigen, kann man auch $\overline{b} \Rightarrow \overline{a}$ zeigen. Diese Vorgehensweise wird auch **indirekter Beweis** genannt.
  Um $a \Rightarrow b$ zu zeigen, kann man aber auch den Fall „a wahr und b falsch“ ausschließen (das ist ja der einzige Fall, für den $a \to b$ falsch ist). Dies macht man, indem man die Annahme „a wahr und b falsch“ zu einem Widerspruch führt (**Beweis durch Widerspruch**).

Das soll an dieser Stelle einfach nur erwähnt sein, Beispiele werden folgen.

1.2 Elementare Mengenlehre

Mengentheoretische Ausdrücke sind ein wesentlicher Teil der mathematischen „Umgangssprache“. Der mathematische Mengenbegriff wird oft auch im Alltag verwendet, nämlich immer dann, wenn wir mit einer Menge eine *Zusammenfassung* meinen, wie z. B. die Menge der Einwohner von Wien, alle Dateien in einem Verzeichnis, usw. Georg Cantor, der Begründer der Mengenlehre, hat im Jahr 1895 eine anschauliche Definition einer Menge gegeben:

Definition 1.22 Eine **Menge** ist eine Zusammenfassung von bestimmten und wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.

Streng genommen ist diese Definition etwas unbefriedigend, da z. B. der Ausdruck „Zusammenfassung von Objekten“ zwar intuitiv klar, aber nicht definiert ist. Dieses Problem ist aber unumgänglich: In der axiomatischen Mengenlehre gibt es einfach undefinierte Begriffe. Aber es kommt noch schlimmer, unsere Definition kann sogar zu Widersprüchen führen (Russell'sches Paradoxon – nach dem britischen Mathematiker und Philosophen Bertrand Russell (1872–1970)): Wenn ein Barbier behauptet alle Männer eines Dorfes zu rasieren, die sich nicht selbst rasieren, rasiert er sich dann selbst (d.h., ist er in dieser Menge enthalten oder nicht)? Durch ausgefeiltere Axiomensysteme lassen sich solche einfachen Widersprüche zwar vermeiden, aber ob man damit *alle* Widersprüche ausgeräumt hat, bleibt trotzdem unklar. Kurt Gödel hat gezeigt, dass ein System nicht zum Beweis seiner eigenen Widerspruchsfreiheit verwendet werden kann. Wir werden aber einfach unserem Barbier verbieten widersprüchliche Aussagen zu machen und uns mit obiger Definition begnügen.

Die Objekte einer Menge M werden die **Elemente** von M genannt. Wir schreiben $a \in M$, wenn a ein Element von M ist. Ist a kein Element von M, so schreiben wir dafür $a \notin M$. Mengen werden üblicherweise mit Großbuchstaben wie A, B, M etc. bezeichnet. Beispiel: $M = \{1, 2, 3, 4, 5\}$ ist die Menge, die aus den Zahlen 1, 2, 3, 4, und 5 besteht. Es ist $1 \in M$, aber $7 \notin M$.

Zwei Mengen sind **gleich**, wenn sie dieselben Elemente haben. Auf die Reihenfolge der Elemente kommt es also nicht an. Auch wird jedes Element nur *einmal* gezählt (braucht also nur einmal angeschrieben zu werden). So können wir die Menge $A = \{i, n, f, o, r, m, a, t, i, k\}$ ohne weiteres auch schreiben als $A = \{a, f, i, k, m, n, o, r, t\}$.

Einige häufig auftretende Zahlenmengen werden mit eigenen Symbolen bezeichnet, z. B.

$$\begin{aligned} \mathbb{N} &= \{1, 2, 3, 4, \ldots\} \qquad \text{Menge der natürlichen Zahlen} \\ \mathbb{Z} &= \{\ldots, -2, -1, 0, 1, 2, \ldots\} \qquad \text{Menge der ganzen Zahlen} \end{aligned}$$

Sie sind Beispiele für **unendliche Mengen**, d.h. Mengen mit unendlich vielen Elementen (im Gegensatz zu **endlichen Mengen**). Die Anzahl der Elemente einer Menge A wird als $|A|$ abgekürzt und **Mächtigkeit** genannt. Zum Beispiel ist die Anzahl der Elemente von $A = \{a, f, i, k, m, n, o, r, t\}$ gleich $|A| = 9$.

Oft ist es umständlich oder unmöglich, eine Menge durch *Aufzählung* ihrer Elemente anzugeben. Dann gibt man eine gemeinsame *Eigenschaft* der Elemente an: $M = \{x \in \mathbb{N} \mid x < 6\}$ ist eine andere Schreibweise für die Menge $M = \{1, 2, 3, 4, 5\}$. Der senkrechte Strich „|“ wird dabei gelesen als „für die gilt“. Anstelle von „|“ kann man auch einen Doppelpunkt „:“ schreiben, also $M = \{x \in \mathbb{N} : x < 6\}$. Gelesen: „$M$ ist die Menge aller natürlichen Zahlen x, für die gilt: x ist kleiner als 6“. Ihnen ist vielleicht eine andere Möglichkeit eingefallen, um die Elemente von M zu beschreiben. So hätten wir natürlich auch $M = \{x \in \mathbb{N} \mid x \leq 5\}$ oder $M = \{x \in \mathbb{Z} \mid 1 \leq x \leq 5\}$ etc. schreiben können.

Beispiel 1.23 Angabe von Mengen
a) Zählen Sie die Elemente der Menge $A = \{x \in \mathbb{Z} : x^2 = 4\}$ auf.
b) Geben Sie die Menge $B = \{3, 4, 5\}$ in einer anderen Form an.

Lösung zu 1.23
a) $A = \{-2, 2\}$
b) $B = \{x \in \mathbb{N} \mid 3 \leq x \leq 5\}$ wäre eine Möglichkeit. ■

Es hat sich als nützlich herausgestellt eine Menge einzuführen, die *keine Elemente* enthält. Diese Menge heißt **leere Menge**. Man schreibt sie mit dem Symbol $\{\}$ oder auch mit $\emptyset$.

Beispiel 1.24 Leere Menge
$S = \{x \in \mathbb{N} \mid x = x+1\} = \{\}$, denn es gibt keine natürliche Zahl, die gleich bleibt, wenn man zu ihr 1 addiert.

Die Einführung der leeren Menge macht den Umgang mit Mengen einfacher. Gäbe es sie nicht, so könnte man zum Beispiel nicht von der Menge aller roten Autos auf einem Parkplatz sprechen, wenn man sich nicht vorher vergewissert hätte, dass es dort auch tatsächlich solche gibt.

Definition 1.25 Eine Menge A heißt **Teilmenge** von B, wenn gilt: $x \in A \Rightarrow x \in B$. Das bedeutet also, dass jedes Element von A auch in B enthalten ist. Man schreibt in diesem Fall: $A \subseteq B$.

Die Tatsache, dass A Teilmenge von B ist, $A \subseteq B$, beinhaltet auch den Fall, dass A und B gleich sind. Wenn betont werden soll, dass A Teilmenge von B ist, aber $A \neq B$, so schreibt man $A \subset B$ oder $A \subsetneq B$.

Die Menge aller Teilmengen einer gegebenen Menge A wird als **Potenzmenge** von A bezeichnet.

Abbildung 1.1 veranschaulicht die Beziehung $A \subseteq B$. Solche grafische Darstellungen werden als **Venn-Diagramme** bezeichnet.

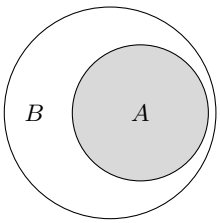


Abbildung 1.1. A ist Teilmenge von B

Beispiel 1.26 Teilmenge
a) $\{1,2,3\} \subseteq \{0,1,2,3\}$ b) $\{1,2,3\} \subseteq \mathbb{N}$ c) $\{1,2,3\} \subseteq \{1,2,3\}$
d) $A = \{0,2,4\}$ ist keine Teilmenge von $B = \{2,4,6,8\}$, weil $0 \notin B$.
e) Aus der Definition der leeren Menge folgt: $\{\} \subseteq A$ für jede Menge A.

Wenn wir zwei Mengen A und B gegeben haben, dann könnten wir uns für jene Elemente interessieren, die *sowohl* in A *als auch* in B vorkommen:

Definition 1.27 Die Menge

$$A \cap B = \{x \mid x \in A \text{ und } x \in B\}$$

nennt man den **Durchschnitt** von A und B.

Abbildung 1.2 veranschaulicht den Durchschnitt von Mengen.

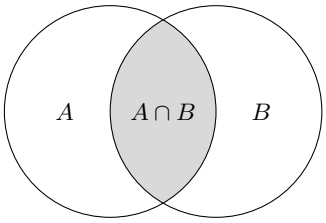


Abbildung 1.2. Durchschnitt von Mengen

Beispiel 1.28 Durchschnitt
a) $\{2,3,4\} \cap \{3,4,7\} = \{3,4\}$ b) $\{1,2,3\} \cap \mathbb{N} = \{1,2,3\}$
c) $\{u,v\} \cap \{x,y\} = \{\}$

Besitzen zwei Mengen kein gemeinsames Element, so heißen diese Mengen **disjunkt** (oder auch **elementfremd**).

Wir könnten auch alle Elemente zu einer neuen Menge zusammenfassen, die in A oder in B (oder in beiden) vorkommen:

Definition 1.29 Die Menge

$$A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$$

nennt man **Vereinigung** von A und B.

Eselsbrücke: Das Symbol $\cup$ für Vereinigung erinnert an eine Schüssel – in ihr wird alles vereinigt.

Abbildung 1.3 veranschaulicht die Vereinigung von zwei Mengen.

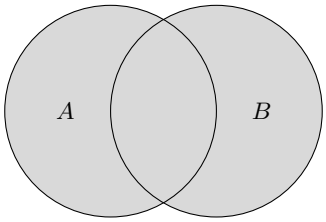


Abbildung 1.3. Vereinigung von A und B

Beispiel 1.30 Vereinigung

a) $\{1,2,3\} \cup \{3,4\} = \{1,2,3,4\}$. Die Zahl 3, die in beiden Mengen vorkommt, wird in der Vereinigungsmenge (wie bei Mengen üblich) nur einmal angeschrieben.
b) $\{u,v\} \cup \{x,y\} = \{u,v,x,y\}$
c) $\{1,2,3\} \cup \mathbb{N} = \mathbb{N}$

Die Mengenoperationen erfüllen die folgenden Gesetze:

Satz 1.31 (Rechengesetze für Mengen)
Kommutativgesetze:

$$A \cup B = B \cup A, \qquad A \cap B = B \cap A.$$

Assoziativgesetze:

$$A \cup (B \cup C) = (A \cup B) \cup C, \qquad A \cap (B \cap C) = (A \cap B) \cap C.$$

Bei der Vereinigung mehrerer Mengen kann also auf Klammern verzichtet werden. Analoges gilt für den Durchschnitt.

Distributivgesetze:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Für die Vereinigung mehrerer Mengen $A_1, \ldots, A_n$ schreibt man abkürzend

$$\bigcup_{j=1}^{n} A_j = A_1 \cup \cdots \cup A_n = \{x \mid x \in A_j \text{ für mindestens ein } j, j = 1, \ldots, n\}$$

und liest diesen Ausdruck: „Vereinigung aller Mengen A_j für $j = 1$ bis $j = n$“. Analoges gilt für den Durchschnitt:

$$\bigcap_{j=1}^{n} A_j = A_1 \cap \cdots \cap A_n = \{x \mid x \in A_j \text{ für alle } j = 1, \ldots, n\}.$$

Manchmal möchte man aus einer Menge bestimmte Elemente entfernen. Dazu gibt es folgende Mengenoperation:

Definition 1.32 Die **Differenz** zweier Mengen

$$A \backslash B = \{x \mid x \in A \text{ und } x \notin B\}$$

ist die Menge der Elemente von A ohne die Elemente von B. Ist speziell B eine Teilmenge von A, so nennt man $A \backslash B$ auch das **Komplement** von B in A und schreibt dafür $\overline{B}$. In diesem Zusammenhang bezeichnet man A als die **Grundmenge**.

Abbildung 1.4 veranschaulicht die Differenz von Mengen.

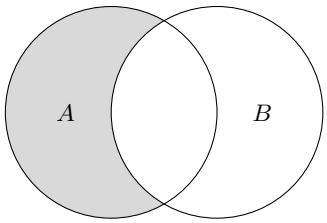


Abbildung 1.4. Differenz $A \backslash B$ von Mengen: Der grau schattierte Bereich enthält alle Elemente von A, die nicht in B liegen.

Beispiel 1.33 Differenz
a) $\{1,2,3\}\backslash\{3,4\} = \{1,2\}$. Hier haben wir aus der Menge $\{1,2,3\}$ alle Elemente entfernt, die auch in $\{3,4\}$ vorkommen. Es macht nichts, dass die Zahl 4 in der ersten Menge überhaupt nicht vorkommt.
b) $\{u,v\}\backslash\{x,y\} = \{u,v\}$
c) $\mathbb{N}\backslash\{1\} = \{x \in \mathbb{N} \mid x \geq 2\}$

Vereinigung, Durchschnitt und Differenz werden über die folgenden Rechenregeln in Bezug zueinander gesetzt:

Satz 1.34 Sind A, B Teilmengen einer Menge M (Grundmenge), so gelten für die Komplemente die **de Morgan'schen Regeln**

$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \qquad \overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Sie sind nach dem schottischen Mathematiker Augustus de Morgan (1806–1871) benannt.

Erinnern Sie sich daran, dass bei einer Menge die Reihenfolge, in der ihre Elemente aufgezählt werden, keine Rolle spielt. Es ist also zum Beispiel $\{1,2\} = \{2,1\}$. Oft ist aber auch die Reihenfolge von Objekten wichtig:

Wenn Sie ins Kino gehen, so könnte Ihr Sitzplatz im Kinosaal durch das Zahlenpaar $(3,7)$ eindeutig bestimmt werden: Reihe 3, Sitz 7. Das Zahlenpaar $(7,3)$ würde einen anderen Sitzplatz bezeichnen.

Definition 1.35 Man bezeichnet (a,b) als **geordnetes Paar** (auch: **Tupel**). Zwei geordnete Paare (a,b) und (a',b') sind genau dann **gleich**, wenn $a = a'$ und $b = b'$ ist.

Ein geordnetes Paar wird zum Unterschied zu einer Menge mit *runden* Klammern geschrieben. Nun ist die Reihenfolge von Bedeutung und mehrfach auftretende Elemente werden angeführt. (Es gibt ja auch Reihe 3, Sitz 3 im Kino.)

Beispiel 1.36 Geordnetes Paar
a) $(1,2) \neq (2,1)$ b) $(2,2) \neq (2)$

Definition 1.37 Die Menge aller geordneten Paare zweier Mengen A und B wird **kartesisches Produkt von A und B** genannt und als $A \times B$ geschrieben:

$$A \times B = \{(a,b) \mid a \in A \text{ und } b \in B\} \quad \text{gelesen: „}A \text{ kreuz } B\text{“.}$$

$A \times B$ enthält also alle geordneten Paare (a,b), wobei das erste Element im geordneten Paar immer aus der Menge A und das zweite Element immer aus der Menge B kommt.

Beispiel 1.38 Kartesisches Produkt
a) $\{1,2\} \times \{3,4\} = \{(1,3),(1,4),(2,3),(2,4)\}$
b) $\{1\} \times \{3,4\} = \{(1,3),(1,4)\}$
c) $\{3,4\} \times \{1\} = \{(3,1),(4,1)\}$. Es ist also $A \times B$ nicht gleich $B \times A$.
d) Die Elemente von $\mathbb{N}^2$ (= abkürzende Schreibweise für $\mathbb{N} \times \mathbb{N}$) sind alle geordneten natürliche Zahlenpaare.

Wir können natürlich auch mehrere Elemente, deren Reihenfolge von Bedeutung ist, betrachten. Wenn n die Anzahl dieser Elemente ist, so spricht man von einem **n-Tupel**. So ist $(1,4,0)$ ein Beispiel für ein 3-Tupel. Das **kartesische Produkt der Mengen** $A_1, A_2, ..., A_n$ ist in diesem Sinn definiert als

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, ..., a_n) \mid a_1 \in A_1, ..., a_n \in A_n\}.$$

Man schreibt für das **n-fache Produkt** $A \times A \times ... \times A$ einer Menge A oft auch abkürzend A^n. Ist $\mathbb{R}$ die Menge der reellen Zahlen, so ist z. B. $\mathbb{R}^3$ die Menge aller reellen 3-Tupel (die als „Punkte“ im 3-dimensionalen Raum veranschaulicht werden können).

Mengen kommen zum Beispiel als Definitions- oder Wertebereiche von *Funktionen* vor, daher an dieser Stelle schon folgende Definition:

Definition 1.39 Eine **Abbildung** oder **Funktion** f von einer Menge D in eine Menge M ist eine Vorschrift, die jedem Element $x \in D$ genau ein Element $f(x) \in M$ zuordnet. Man schreibt dafür kurz: $f : D \to M$, $x \mapsto f(x)$ und sagt: „x wird auf $f(x)$ abgebildet“.

Beispiel 1.40 Abbildungen
a) Die Abbildung $f : \mathbb{N} \to \mathbb{N}$ mit $n \mapsto n^2$ ordnet jeder natürlichen Zahl ihr Quadrat zu. Also z. B. $f(1) = 1$, $f(2) = 4$, $f(3) = 9$, usw.
b) Der ASCII-Code ist eine Abbildung, die den Zahlen 0 bis 127 bestimmte Steuerzeichen, Ziffern, Buchstaben und Sonderzeichen zuordnet: z. B. $f(36) =$ \$ oder $f(65) = A$.

Wir werden darauf noch im Abschnitt 5.2 über Funktionen zurückkommen.

1.3 Schaltalgebra

Außer in der Aussagenlogik gibt es noch viele andere Situationen, in denen man es mit Größen zu tun hat, die nur zwei verschiedene Werte annehmen können. Das wohl wichtigste Beispiel ist der Computer, der alles auf die beiden Werte 0 und 1 reduziert. Mithilfe der Schaltalgebra kann man logische Schaltungen beschreiben und untersuchen.

Wir gehen davon aus, dass wir zwei Werte, 0 (falsch) und 1 (wahr), zur Verfügung haben. Eine Variable a kann nur diese beiden Werte annehmen, man spricht daher auch von einer **binären Variablen** oder **Schaltvariablen**. Wie in der Aussagenlogik definieren wir die Negation $\overline{a}$, die Konjunktion $a \cdot b$ und die Disjunktion $a + b$ gemäß folgender Wertetabelle:

a	b	$\overline{a}$	$a \cdot b$	$a + b$
0	0	1	0	0
0	1	1	0	1
1	0	0	0	1
1	1	0	1	1

Man verwendet hier anstelle der Symbole $\wedge$ und $\vee$ oft $\cdot$ bzw. $+$ und spricht auch von einer Multiplikation bzw. Addition. Das hat einen einfachen Grund: Das Verknüpfungsergebnis von $a \cdot b$ laut obiger Tabelle entspricht dem jeweiligen Produkt der reellen Zahlen 0 und 1: $0 \cdot 0 = 0$, $1 \cdot 0 = 0$, $0 \cdot 1 = 0$, $1 \cdot 1 = 1$. Ebenso kann man bei $a + b$ wie gewohnt mit 0 und 1 rechnen, mit einer Ausnahme: Man muss berücksichtigen, dass per Definition $1 + 1 = 1$ gesetzt wird.

Wie schon in der Aussagenlogik sind zwei verknüpfte Ausdrücke **gleich**, wenn sie bei derselben Belegung der Eingangsvariablen gleiche Werte annehmen.

Beispiel 1.41 Gleichheit von verknüpften Ausdrücken
Zeigen Sie mithilfe einer Wertetabelle, dass $\overline{\overline{a}} = a$.

Lösung zu 1.41 Die Verneinung $\overline{\overline{a}}$ von $\overline{a}$ hat genau den entgegengesetzten Wahrheitswert von $\overline{a}$,

a	$\overline{a}$	$\overline{\overline{a}}$
0	1	0
1	0	1

also immer denselben Wahrheitswert wie a. ■

Es ist also

$$a = \overline{\overline{a}}.$$

Auf die gleiche Weise können wir nachweisen, dass

$$a \cdot 0 = 0, \quad a \cdot 1 = a, \quad a \cdot a = a, \quad a \cdot \overline{a} = 0$$

und

$$a + 1 = 1, \quad a + 0 = a, \quad a + a = a, \quad a + \overline{a} = 1.$$

Wenn wir uns das genauer ansehen, dann erkennen wir, dass jede Formel in eine andere gültige Formel übergeht, wenn man in ihr die Symbole $\cdot$ und $+$ sowie 0 und 1 vertauscht: Zum Beispiel erhält man aus $a \cdot 0 = 0$ auf diese Weise die Formel $a + 1 = 1$ (in $a \cdot 0 = 0$ wurde $\cdot$ durch $+$ ersetzt und 0 durch 1). Man bezeichnet dies als **Dualitätsprinzip**.

Eine Begründung, warum das Dualitätsprinzip gilt, kommt etwas später.

Allgemeiner kann man auch Ausdrücke betrachten, die mehr als eine Variable enthalten. Sind a, b und c Variable, die die Werte 0 und 1 annehmen können, so können wir durch Aufstellen der zugehörigen Wertetabellen leicht folgende Regeln zeigen, die wir schon analog bei den Mengen kennen gelernt haben. (Beachten Sie, dass wieder nach dem Dualitätsprinzip je zwei Formeln einander entsprechen.)

Satz 1.42 (Logikgesetze)
Kommutativgesetze:

$$a + b = b + a, \qquad a \cdot b = b \cdot a.$$

Assoziativgesetze:

$$a + (b + c) = (a + b) + c, \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

Distributivgesetze:

$$a + (b \cdot c) = (a + b) \cdot (a + c), \qquad a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

Absorptionsgesetze:

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

De Morgan'sche Regeln:

$$\overline{a \cdot b} = \overline{a} + \overline{b}, \qquad \overline{a + b} = \overline{a} \cdot \overline{b}.$$

Die Kommutativgesetze sind uns vom Rechnen mit reellen Zahlen vertraut und besagen nichts anderes, als dass zum Beispiel $0 \cdot 1$ dasselbe ist wie $1 \cdot 0$ oder $0 + 1$ dasselbe ist wie $1 + 0$.

Auch die Assoziativgesetze sind uns vertraut. Sie sagen, dass man in einem längeren Ausdruck, der nur *eine* Verknüpfungsart enthält (also nur „+“ oder nur „·“), keine Klammern setzen muss, weil es auf die Reihenfolge nicht ankommt. Es ist z. B. $1 \cdot (0 \cdot 1)$ dasselbe wie $(1 \cdot 0) \cdot 1$, daher kann man die Klammern hier gleich weglassen und $1 \cdot 0 \cdot 1$ schreiben.

Wenn ein Ausdruck sowohl $\cdot$ also auch $+$ enthält, dann müssen Klammern gesetzt werden, um die Reihenfolge der Auswertung klarzustellen. Gibt es keine Klammern, dann gilt die Konvention, dass zuerst die Verneinung, dann $\cdot$ und dann $+$ ausgewertet wird. Der Ausdruck $\overline{a} \cdot b + b$ ist also als $((\overline{a}) \cdot b) + b$ zu verstehen.

Bei den reellen Zahlen gibt es analog die Regel „Punkt vor Strich“.

Das zweite (rechte) Distributivgesetz ist uns ebenfalls vom Rechnen mit reellen Zahlen vertraut („Ausmultiplizieren“ bzw., wenn es von rechts nach links gelesen wird, „Herausheben“). Das erste (linke) Distributivgesetz würde einem „Ausaddieren“ entsprechen, es gibt aber kein entsprechendes Gesetz für das Rechnen mit reellen Zahlen.

Es gelten also insbesondere alle Rechenregeln, die für die Multiplikation und Addition von reellen Zahlen gelten. Da uns diese Rechenregeln vertraut sind, ist es auch sinnvoll, die gleichen Symbole $\cdot$ und $+$ zu verwenden.

Dieses *Rechnen* mit 0 und 1 geht auf den englischen Mathematiker George Boole (1815–1864) zurück, dem es gelang, eine Algebra der Aussagen zu entwickeln und damit die über 2000 Jahre alte Aussagenlogik zu formalisieren. Eine **Boole'sche Algebra** ist allgemein eine Menge (die mindestens 2 Elemente, 0 und 1, enthält) mit zwei Verknüpfungen, $\cdot$ und $+$, die die obigen Ge-

setze erfüllen. Die grundlegenden Schaltungen in Computern folgen diesen Gesetzen, daher ist die Schaltalgebra ein wichtiges Anwendungsgebiet der Boole'schen Algebra.

Beispiel 1.43 (→CAS) De Morgan'sche Regeln
Zeigen Sie die Gültigkeit der de Morgan'schen Regeln mithilfe einer Wertetabelle.

Lösung zu 1.43 Für die erste Regel müssen wir zeigen, dass für jede Kombination der Werte der Eingangsvariablen a und b die Ausdrücke $\overline{a \cdot b}$ und $\overline{a} + \overline{b}$ die gleichen Werte haben:

a	b	$a \cdot b$	$\overline{a \cdot b}$	$a + b$	$\overline{a + b}$	$\overline{a}$	$\overline{b}$	$\overline{a} + \overline{b}$	$\overline{a} \cdot \overline{b}$
0	0	0	1	0	1	1	1	1	1
0	1	0	1	1	0	1	0	1	0
1	0	0	1	1	0	0	1	1	0
1	1	1	0	1	0	0	0	0	0

Tatsächlich sind in der vierten und der neunten Spalte dieselben Werte, daher ist $\overline{a \cdot b} = \overline{a} + \overline{b}$. Analog folgt aus Gleichheit der sechsten und zehnten Spalte $\overline{a + b} = \overline{a} \cdot \overline{b}$. Da das Aufstellen solcher Wertetabellen recht mühsam ist, bietet es sich an den Computer zu bemühen (siehe Abschnitt 1.4). ■

Aus den de Morgan'schen Regeln folgt auch sofort das Dualitätsprinzip: Negieren wir zum Beispiel das erste Absorptionsgesetz, so folgt aus $\overline{a \cdot (a + b)} = \overline{a} + (\overline{a + b}) = \overline{a} + (\overline{a} \cdot \overline{b})$, dass $\overline{a} + (\overline{a} \cdot \overline{b}) = \overline{a}$. Da diese Gleichung für beliebige a, b gilt, gilt sie auch, wenn wir a durch $\overline{a}$ und b durch $\overline{b}$ ersetzen: $a + (a \cdot b) = a$. Das ist aber genau das zweite Absorptionsgesetz.

Natürlich hat es wenig Sinn all diese Regeln aufzustellen, wenn sie nicht auch zu etwas gut wären. In der Tat können sie in der Praxis dazu verwendet werden, um zum Beispiel komplizierte Ausdrücke zu vereinfachen und damit Schaltungen auf möglichst wenige Schaltelemente zu reduzieren.

Beispiel 1.44 (→CAS) Vereinfachung einer Schaltung
Vereinfachen Sie den Ausdruck $\overline{a} \cdot \overline{b} + \overline{a} \cdot b + a \cdot b$.

Lösung zu 1.44 Wir wenden Schritt für Schritt Rechenregeln an:

$$\begin{aligned} \overline{a} \cdot \overline{b} + \overline{a} \cdot b + a \cdot b &= \overline{a} \cdot (\overline{b} + b) + a \cdot b = \overline{a} \cdot 1 + a \cdot b = \overline{a} + a \cdot b = \\ &= (\overline{a} + a) \cdot (\overline{a} + b) = 1 \cdot (\overline{a} + b) = \overline{a} + b, \end{aligned}$$

wobei wir im ersten Schritt das zweite Distributivgesetz (Herausheben eines Faktors), danach $b + \overline{b} = 1$, weiter $\overline{a} \cdot 1 = \overline{a}$ und zuletzt noch das erste Distributivgesetz („Ausaddieren") verwendet haben. ■

Eine Abbildung $f : B^n \to B$, mit $B = \{0, 1\}$, wird als eine **Logikfunktion** in n Variablen bezeichnet. Speziell im Fall $n = 2$ (d.h. 2 Eingangsvariablen) spricht man auch von einer **binären Logikfunktion**. Die oben eingeführten Verknüpfungen $\cdot$ und $+$ von zwei Variablen sind also Beispiele binärer Logikfunktionen. Das sind aber bei weitem nicht alle denkbaren. Bereits in der Aussagenlogik haben wir neben Dis- und Konjunktion eine Reihe weiterer Verknüpfungsmöglichkeiten kennen gelernt. Wenn man alle Kombinationen von Wahrheitswerten für a und b anführt, so kommt man insgesamt auf 16 mögliche binäre Logikfunktionen:

a	b	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

Natürlich finden wir hier alle bekannten Verknüpfungen wieder: $f_8(a,b) = a \cdot b$, $f_{14}(a,b) = a + b$, $f_{11}(a,b) = a \to b$. Die Logikfunktion $f_7(a,b) = \overline{a \cdot b}$ heißt **NAND**-Verknüpfung und $f_1(a,b) = \overline{a + b}$ wird als **NOR**-Verknüpfung bezeichnet.

Man kann nun zeigen, dass sich alle diese 16 Verknüpfungen mithilfe der Konjunktion, Disjunktion und Negation ausdrücken lassen. Das ist besonders bei der Umsetzung von elektronischen Schaltungen von großer Bedeutung: Es müssen dann nur diese drei Basistypen gebaut werden, und alle anderen lassen sich durch sie erzeugen. Um zu sehen, dass diese 3 Basistypen ausreichen, betrachten wir zunächst jene vier Logikfunktionen aus obiger Tabelle, die für genau eine Kombination der Eingabewerte den Wert 1 annehmen (und sonst immer 0 sind). Es sind das f_1, f_2, f_4 und f_8. Diese vier Verknüpfungen heißen **Minterme**, oder **Vollkonjunktionen** und werden auch mit m_0, m_1, m_2 und m_3 bezeichnet. Es ist also m_0 jene Logikfunktion, die nur bei der Kombination $(a,b) = (0,0)$ den Wert 1 annimmt, m_1 hat Wahrheitswert 1 nur für $(a,b) = (0,1)$, m_2 hat Wahrheitswert 1 nur für $(a,b) = (1,0)$ und m_3 hat Wahrheitswert 1 nur bei $(a,b) = (1,1)$.

Weiters ist leicht zu sehen:

Satz 1.45 Die Minterme können als Produkte dargestellt werden:

$$m_0(a,b) = \overline{a} \cdot \overline{b}, \quad m_1(a,b) = \overline{a} \cdot b, \quad m_2(a,b) = a \cdot \overline{b}, \quad m_3(a,b) = a \cdot b.$$

Das kann mithilfe der zugehörigen Wahrheitstabelle gezeigt werden:

Beispiel 1.46 Darstellung eines Minterms als Produkt
Zeigen Sie mithilfe einer Wahrheitstabelle, dass $m_0 = \overline{a} \cdot \overline{b}$.

Lösung zu 1.46

a	b	$\overline{a}$	$\overline{b}$	$\overline{a} \cdot \overline{b}$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	0	0	0

Tatsächlich ist also $\overline{a} \cdot \overline{b} = f_1(a,b) = m_0(a,b)$. ■

In der Praxis ist oft die Wertetabelle einer Verknüpfung vorgegeben und man möchte sie durch möglichst wenige Schaltelemente (Disjunktion, Konjunktion oder Negation) realisieren. Gehen wir von der Wertetabelle einer Verknüpfung f (f steht hier für eine der möglichen binären Logikfunktionen $f_0, \ldots, f_{15}$) aus,

a	b	$f(a,b)$
0	0	$f(0,0)$
0	1	$f(0,1)$
1	0	$f(1,0)$
1	1	$f(1,1)$

dann kann f folgendermaßen als Summe von Mintermen geschrieben werden:

$$f = f(0,0) \cdot m_0 + f(0,1) \cdot m_1 + f(1,0) \cdot m_2 + f(1,1) \cdot m_3.$$

Das lässt sich durch Aufstellen einer Wertetabelle nachweisen (siehe Übungen).

Satz 1.47 (Normalformen) Jede Logikfunktion $f : B^2 \to B$ lässt sich in **disjunktiver Normalform** (DNF)

$$f(a,b) = f(0,0) \cdot \overline{a} \cdot \overline{b} + f(0,1) \cdot \overline{a} \cdot b + f(1,0) \cdot a \cdot \overline{b} + f(1,1) \cdot a \cdot b$$

schreiben. Alternativ kann f auch in **konjunktiver Normalform** (KNF)

$$f(a,b) = (f(0,0) + a + b) \cdot (f(0,1) + a + \overline{b}) \cdot (f(1,0) + \overline{a} + b) \cdot (f(1,1) + \overline{a} + \overline{b})$$

dargestellt werden.

Die Ausdrücke $M_0(a,b) = a + b$, $M_1(a,b) = a + \overline{b}$, $M_2(a,b) = \overline{a} + b$, $M_3(a,b) = \overline{a} + \overline{b}$, die in der KNF vorkommen, heißen **Maxterme** oder **Volldisjunktionen**. Maxterme nehmen nur für eine Kombination der Eingangsvariablen den Wert 0, sonst immer den Wert 1 an (sind also in diesem Sinn „maximal“).

Beispiel 1.48 Disjunktive Normalform
Bringen Sie die Verknüpfung $f_{11}(a,b) = a \to b$ auf DNF.

Lösung zu 1.48 Wir schreiben in der Wertetabelle rechts neben den Funktionswerten von f_{11} die entsprechenden Minterme, die gerade für diese Eingangsvariablen den Wert 1 annehmen, an:

a	b	$f_{11}(a,b)$	
0	0	1	m_0
0	1	1	m_1
1	0	0	m_2
1	1	1	m_3

Nun setzen wir in die Formel für die DNF ein:

$$\begin{aligned} f_{11}(a,b) &= m_0(a,b) f_{11}(0,0) + \ldots + m_3(a,b) f_{11}(1,1) \\ &= \overline{a} \cdot \overline{b} \cdot 1 + \overline{a} \cdot b \cdot 1 + a \cdot \overline{b} \cdot 0 + a \cdot b \cdot 1. \end{aligned}$$

Es wird also genau über jene Minterme summiert, für die der zugehörige Funktionswert den Wert 1 hat:

$$f_{11}(a,b) = m_0(a,b) + m_1(a,b) + m_3(a,b) = \overline{a} \cdot \overline{b} + \overline{a} \cdot b + a \cdot b.$$

Das ist die gesuchte DNF. (Aus Beispiel 1.44 wissen wir, dass sich dieser Ausdruck noch weiter umformen lässt: $a \to b = \overline{a} + b$.) ■

Eine beliebige Verknüpfung kann also leicht alleine durch Konjunktion, Disjunktion und Negation dargestellt werden, indem man die Summe über alle Minterme bildet, für die die Verknüpfung den Wert 1 hat. Analog wird für die KNF das Produkt aller Maxterme gebildet, für die die Verknüpfung den Wert 0 hat:

Beispiel 1.49 Konjunktive Normalform
Bringen Sie die Verknüpfung $f_{11}(a,b) = a \to b$ auf KNF.

Lösung zu 1.49 Wieder schreiben wir in der Wertetabelle rechts neben den Funktionswerten von f_{11} die entsprechenden Maxterme, die gerade für diese Eingangsvariablen den Wert 0 annehmen, an:

a	b	$f_{11}(a,b)$	
0	0	1	M_0
0	1	1	M_1
1	0	0	M_2
1	1	1	M_3

Dann setzen wir in die Formel für die KNF ein:

$$\begin{aligned} f_{11}(a,b) &= (f_{11}(0,0) + M_0(a,b)) \cdot \ldots \cdot (f_{11}(1,1) + M_3(a,b)) \\ &= (1+a+b) \cdot (1+a+\overline{b}) \cdot (0+\overline{a}+b) \cdot (1+\overline{a}+\overline{b}) \\ &= 1 \cdot 1 \cdot (\overline{a}+b) \cdot 1 = \overline{a}+b. \end{aligned}$$

Es werden also für die KNF genau jene Maxterme multipliziert, für die der zugehörige Funktionswert den Wert 0 hat. ■

Zusammenfassend können wir also sagen: Hat die Verknüpfung öfter den Wert 0, so ist die DNF effektiver, hat sie öfter den Wert 1, so ist die KNF effektiver. Das sehen wir z. B. durch Vergleich der Rechenwege der Beispiele 1.48 und 1.49.

Mithilfe der de Morgan'schen Regeln $a \cdot b = \overline{\overline{a} + \overline{b}}$ bzw. $a + b = \overline{\overline{a} \cdot \overline{b}}$ kann man noch die Konjunktion durch die Negation und Disjunktion bzw. die Disjunktion durch die Negation und Konjunktion ausdrücken. Es reichen also Negation und Disjunktion bzw. Negation und Konjunktion aus, um eine beliebige Verknüpfung darzustellen. Wegen $\overline{a} = \overline{a \cdot a}$ reicht sogar die NAND-Verknüpfung $\overline{a \cdot b}$ alleine aus. Alternativ reicht wegen $\overline{a} = \overline{a + a}$ die NOR-Verknüpfung $\overline{a + b}$ alleine aus.

Analoge Überlegungen gelten natürlich auch für Logikfunktionen mit mehr als zwei Variablen. Hat man n Variable, so gibt es 2^{2^n} mögliche Logikfunktionen, die sich mithilfe der DNF (bzw. KNF) auf Negation, Disjunktion und Konjunktion zurückführen lassen.

1.3.1 Anwendung: Entwurf von Schaltkreisen

Die Überlegungen aus dem letzten Abschnitt bilden die Grundlage für den Entwurf von Schaltkreisen. Eine der wichtigsten Operationen, die ein Computer beherrschen muss, ist die Addition zweier Zahlen. Wie können wir eine zugehörige Schaltung entwerfen?

Da Schaltungen (und damit auch Computer) nur Nullen und Einsen verarbeiten können, müssen die beiden Zahlen als Dualzahlen, das heißt, als eine Folge

$(a_n \dots a_1 a_0)_2$ von Nullen und Einsen, gegeben sein. Die einzelnen Stellen a_j können dabei nur die Werte 0 oder 1 annehmen, und die Dualzahl $(a_n \dots a_1 a_0)_2$ entspricht der Dezimalzahl $2^n a_n \dot{+} 2^{n-1} a_{n-1} \dot{+} \dots \dot{+} 8a_3 \dot{+} 4a_2 \dot{+} 2a_1 \dot{+} a_0$ (dabei haben wir die Addition von Zahlen zur Unterscheidung von der Disjunktion mit $\dot{+}$ bezeichnet). Alle zweistelligen Dualzahlen sind zum Beispiel $(00)_2 = 2 \cdot 0 \dot{+} 0 = 0$, $(01)_2 = 2 \cdot 0 \dot{+} 1 = 1$, $(10)_2 = 2 \cdot 1 \dot{+} 0 = 2$ und $(11)_2 = 2 \cdot 1 \dot{+} 1 = 3$. (Mehr über Dualzahlen werden wir in Abschnitt 2.4 erfahren.)

Beginnen wir mit dem einfachsten Fall, der Addition von zwei einstelligen Dualzahlen mit Überlauf:

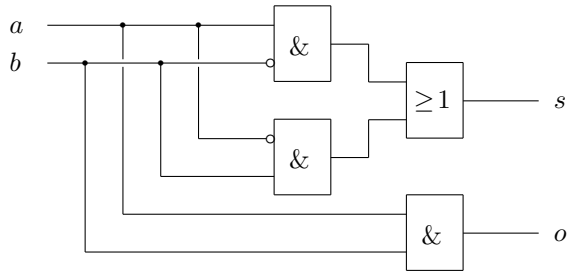
a	b	$s(a,b)$	$o(a,b)$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Hier ist s die Summe und o gibt an, ob ein Überlauf aufgetreten ist. Das Ergebnis ist also im Allgemeinen eine zweistellige Dualzahl und es gilt $a \dot{+} b = (os)_2 = s \dot{+} 2o$.

Stellen wir s und o mithilfe der DNF dar und vereinfachen das Ergebnis, so erhalten wir

$$s(a,b) = \overline{a} \cdot b + a \cdot \overline{b} = a \operatorname{xor} b \quad \text{und} \quad o(a,b) = a \cdot b.$$

Die zugehörige Schaltung wird wie folgt dargestellt:



Eine Konjunktion wird dabei mit „&“ und eine Disjunktion mit „≥ 1“ gekennzeichnet. Die Negation wird durch einen Kreis vor dem Eingang dargestellt.

Nun kommen wir zur Addition von mehrstelligen Dualzahlen. Wie im Dezimalsystem kann die Addition im Dualsystem stellenweise durchgeführt werden. Dabei werden für jede Stelle die beiden entsprechenden Stellen der zu addierenden Zahlen plus der Überlauf (Übertrag) von der vorhergehenden Stelle addiert. Wenn also $(a_n \dots a_1 a_0)_2$ und $(b_n \dots b_1 b_0)_2$ die zu addierenden Zahlen sind, so ergibt sich für die j-te Stelle der Summe $(s_n \dots s_1 s_0)_2$ und den zugehörigen Überlauf o_j:

$$(o_j s_j)_2 = s_j \dot{+} 2o_j = a_j \dot{+} b_j \dot{+} o_{j-1},$$

wobei o_j der Überlauf in der j-ten Stelle ist. Dabei ist $o_{-1} = 0$ zu setzen (denn im nullten Schritt gibt es noch keinen Überlauf) und o_n gibt an, ob insgesamt ein Überlauf aufgetreten ist.

Wir benötigen für die Addition von zwei n-stelligen Dualzahlen also noch eine Schaltung für die Addition von drei einstelligen Dualzahlen

a	b	c	$s(a,b,c)$	$o(a,b,c)$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

wobei s die Summe der drei einstelligen Dualzahlen a, b und c ist und o angibt, ob ein Überlauf aufgetreten ist. Damit lautet bei der Addition von zwei n-stelligen Dualzahlen die Formel für die j-te Stelle der Summe bzw. des Überlaufs

$$s_j = s(a_j, b_j, o_{j-1}) \quad \text{und} \quad o_j = o(a_j, b_j, o_{j-1}).$$

Hier haben wir es jeweils mit einer Verknüpfung $f = f(a,b,c)$ dreier Variablen a, b und c zu tun. Analog wie im Fall zweier Variablen kann sie mithilfe der DNF

$$\begin{aligned} f \quad = \quad & \overline{a} \cdot \overline{b} \cdot \overline{c} \cdot f(0,0,0) + \overline{a} \cdot \overline{b} \cdot c \cdot f(0,0,1) + \overline{a} \cdot b \cdot \overline{c} \cdot f(0,1,0) + \\ & \overline{a} \cdot b \cdot c \cdot f(0,1,1) + a \cdot \overline{b} \cdot \overline{c} \cdot f(1,0,0) + a \cdot \overline{b} \cdot c \cdot f(1,0,1) + \\ & a \cdot b \cdot \overline{c} \cdot f(1,1,0) + a \cdot b \cdot c \cdot f(1,1,1) \end{aligned}$$

geschrieben werden. Damit ergibt sich

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

Nun können wir die Summe zwar berechnen, wie können wir das Ergebnis aber ausgeben? Im einfachsten Fall verwenden wir für jede Stelle s_j eine Leuchtdiode. Man kann dann die Summe in Dualdarstellung ablesen und der Benutzer kann leicht selbst die zugehörige Dezimaldarstellung ausrechnen;-) Wer es doch etwas komfortabler haben möchte, kann natürlich auch das Ergebnis mittels LCD-Anzeige darstellen. Die zugehörige Schaltung können Sie in Übungsaufgabe 9 entwerfen.

Nun brauchen Sie nur noch in den nächsten Elektronikladen schlendern, um sich ein paar NAND-Gatter und Leuchtdioden zu kaufen, und schon können Sie Ihren eigenen Hochleistungstaschenrechner zusammenlöten.

Etwas fehlt unserem Computer allerdings noch: Er berechnet *statisch* aus einer Eingabe die Ausgabe, kann aber nicht mit dem Ergebnis weiterrechnen. Dazu sind noch zwei weitere Bausteine notwendig: ein Element zur Zwischenspeicherung von Ergebnissen (Flip-Flop) und ein Taktgeber zur zeitlichen Synchronisation des Ablaufes.

1.4 Mit dem digitalen Rechenmeister

Schaltalgebra

Das Aufstellen von Wertetabellen ist recht mühsam und es bietet sich daher der Einsatz eines kleinen Programms an. `Mathematica` verwendet `False`, `True` für $0, 1$ und

kennt eine Reihe logischer Verknüpfungen: Negation `Not[a]` (oder `!a`), Und `And[a, b]` (oder `a&&b`), Oder `Or[a, b]` (oder `a||b`). Mit folgendem Programm können wir leicht Wertetabellen erstellen:

```
In[1]:= LogicTable[f_, v_List] := Module[{n = Length[v], tabl, vals, rule},
           tabl = Flatten[{v, f}];
           Do[
              vals = IntegerDigits[i, 2, n] /. {0 → False, 1 → True};
              rule = Table[Rule[v[[i]], vals[[i]] ], {i, n}];
              tabl = Append[tabl, Flatten[{vals, f /. rule}]];
           , {i, 0, 2^n - 1}];
           TableForm[tabl]
           ]
```

Grübeln Sie nicht darüber, wie dieses Programm funktioniert, sondern rufen Sie es einfach mit einem logischem Ausdruck (oder einer Liste von logischen Ausdrücken) und einer Liste der Variablen auf:

```
In[2]:= LogicTable[{!(a||b), !a&&!b}, {a, b}]
Out[2]//TableForm=
        a      b      !(a||b)  !a&&!b
        False  False  True     True
        False  True   False    False
        True   False  False    False
        True   True   False    False
```

`Mathematica` kann übrigens auch logische Ausdrücke vereinfachen:

```
In[3]:= LogicalExpand[!a&&!b||!a&&b||a&&b]
Out[3]= b||!a
```

1.5 Kontrollfragen

Fragen zu Abschnitt 1.1: Elementare Logik

Erklären Sie folgende Begriffe: Aussage, Wahrheitstabelle, Negation, AND-, OR-, XOR-Verknüpfung, Aussageform, All-Aussage, All-Quantor, Existenz-Aussage, Existenz-Quantor, Implikation, notwendig/hinreichend, Äquivalenz.

1. Liegt eine Aussage vor?
   a) Österreich liegt am Meer. b) Wie spät ist es? c) $4 + 3 = 7$
2. Verneinen Sie und vereinfachen Sie sprachlich:
   a) Das Glas ist voll. b) Er ist der Älteste der Familie.
   c) 7 ist eine gerade Zahl.
3. Ist in den folgenden Sätzen vermutlich ein einschließendes oder ein ausschließendes „oder“ gemeint?
   a) Du kommst vor Mitternacht nach Hause oder du hast eine Woche Fernsehverbot.
   b) Morgen oder übermorgen kann es schneien.

c) Morgen oder übermorgen ist Montag.
d) Kopf oder Zahl?

4. Wie müsste „Betreten des Rasens und Blumenpflücken verboten“ nach den Regeln der Aussagenlogik formuliert werden?
5. Aussage a: „Die Erde hat zwei Monde“; Aussage b: „München liegt in Deutschland“. Welche Aussagen sind wahr? a) $a \wedge b$ b) $a \vee b$ c) a xor b
6. Angenommen, das Wetter würde sich an die Regel „Ist es an einem Tag sonnig, so auch am nächsten“ halten. Wenn es heute sonnig ist, was folgt dann?
   a) Es ist immer sonnig.
   b) Gestern war es sonnig.
   c) Morgen ist es sonnig.
   d) Es wird nie mehr sonnig sein.
   e) Ab heute wird es immer sonnig sein.
7. Liegt eine Aussage vor?
   a) $x + 5 = 8$ b) Es gibt ein x mit $x + 5 = 8$.
   c) Für alle x gilt: $x + 5 = 8$.
8. Welche Aussage ist wahr?
   a) Für alle natürlichen Zahlen x ist $x < 3$.
   b) Es gibt eine natürliche Zahl x mit $x < 3$.
9. Richtig oder falsch:
   Die Verneinung von „Für alle x gilt $a(x)$“ ist: „Es gibt ein x mit $\overline{a(x)}$“.
10. Verneinen Sie:
    a) Alle Tigerkatzen sind gute Mäusejäger.
    b) Es gibt einen Matrosen, der schwimmen kann.
    c) Für alle x gilt: $x < 3$.
    d) Für alle x, y gilt: $x^2 + y^2 = 4$.
11. Aussage a: „Das Auto ist ein Golf“; Aussage b: „Das Auto ist ein VW“. Was trifft zu: a) Golf $\Rightarrow$ VW b) VW $\Rightarrow$ Golf c) kein VW $\Rightarrow$ kein Golf
    d) VW $\Leftrightarrow$ Golf
12. Sei n eine natürliche Zahl. Aussageform $a(n)$: „n ist durch 4 teilbar“; Aussageform $b(n)$: „n ist eine gerade Zahl“. Was trifft für alle natürlichen Zahlen n zu?
    a) $a(n) \Rightarrow b(n)$ b) $b(n) \Rightarrow a(n)$ c) $a(n) \Leftrightarrow b(n)$ d) $\overline{b(n)} \Rightarrow \overline{a(n)}$
13. Aussage a: „Der Student hat einen Notendurchschnitt < 2“; Aussage b: „Der Student erhält ein Leistungsstipendium“. Die Richtlinie der Stipendienvergabestelle enthält folgenden Satz: „Ein Notendurchschnitt < 2 ist notwendig, aber nicht hinreichend für ein Leistungsstipendium“.
    a) Formulieren Sie diesen Satz symbolisch mit $\Rightarrow$.
    b) Gilt $\overline{a} \Rightarrow \overline{b}$? Formulieren Sie in Worten.

Fragen zu Abschnitt 1.2: Elementare Mengenlehre

Erklären Sie folgende Begriffe: Menge, Element, Mächtigkeit einer Menge, leere Menge, Teilmenge, Durchschnitt, Vereinigung, Differenz, Komplement, geordnetes Paar, kartesisches Produkt, n-Tupel, Abbildung.

1. Sind die Mengen $A = \{1, 2, 3, 4\}$ und $B = \{3, 4, 1, 2\}$ gleich?

2. Zählen Sie alle Elemente der Menge auf:
   a) $A = \{x \in \mathbb{N} \mid x^2 = 16\}$ b) $B = \{x \in \mathbb{Z} \mid x^2 = 16\}$
   c) $C = \{x \in \mathbb{N} \mid x \leq 4\}$ d) $D = \{x \in \mathbb{N} \mid 3x = 1\}$
3. $A = \{1, 2\}$ und $B = \{2, 3, 4\}$:
   a) $A \cup B =$? b) $A \cap B =$? c) Ist $2 \in A$? d) Ist $A \subseteq B$?
4. Sei N die Menge der Nobelpreisträger, O die Menge der österreichischen Nobelpreisträger, W die Menge der weiblichen Nobelpreisträger und L die Menge der Literaturnobelpreisträger. Was bedeutet: a) $O \cup L$ b) $O \cap \overline{W}$
5. Richtig oder falsch?
   a) $\{\} = \{0\}$ b) $\{3, 5, 7\} \subseteq \{1, 3, 5, 7\}$ c) $\{1\} \cup \{1\} = \{2\}$
   d) $\{1\} \cap \{1\} = \{1\}$ e) $\{1, 3\} = \{3, 1\}$ f) $(1, 3) = (3, 1)$
   g) $\{2, 5, 7\} = (2, 5, 7)$ h) $(2, 5, 5) = (2, 5)$
6. $A = \{1, 2\}$, $B = \{2, 3, 4\}$:
   a) $A \times B =$? b) $B \times A =$? c) Ist $\{1, 2\} \subseteq A \times B$?
   d) Ist $(1, 2) \in A \times B$? e) $A \backslash B =$? f) $B \backslash A =$?

Fragen zu Abschnitt 1.3: Schaltalgebra

Erklären Sie folgende Begriffe: Schaltvariable, Dualitätsprinzip, Logikgesetze, Logikfunktion, binäre Logikfunktion, NOR-Funktion, NAND-Funktion, Minterm, Maxterm, disjunktive bzw. konjunktive Normalform.

1. Richtig oder falsch? (Überprüfen Sie mithilfe einer Wertetabelle.)
   a) $a \cdot 0 = 1$ b) $a + \overline{a} = 1$ c) $a \cdot \overline{a} = 0$ d) $\overline{\overline{a} \cdot b} = a \cdot \overline{b}$ e) $\overline{\overline{a} \cdot b} = a + \overline{b}$
2. Bilden Sie mithilfe des Dualitätsprinzips aus folgenden gültigen Regeln weitere gültige Regeln:
   a) $a \cdot 1 = a$ b) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ c) $a \cdot (a + b) = a$
3. Richtig oder falsch: Die Assoziativgesetze $a + (b + c) = (a + b) + c$ bzw. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ bedeuten, dass man bei *beliebigen* Ausdrücken der Schaltalgebra auf Klammern verzichten kann.
4. In vielen Programmiersprachen werden UND, ODER bzw. Negation als „&&“, „||“ bzw. „!“ geschrieben. Welche Abfragen sind äquivalent?
   a) $!(a \,\&\&\, b) == (!a) \,||\, (!b)$ b) $a \,||\, (b \,\&\&\, c) == (a \,\&\&\, b) \,||\, c$
5. Vereinfachen Sie folgende Ausdrücke: a) $a + (a + \overline{a})$ b) $a \cdot \overline{a} \cdot a$
6. Wie viele Minterme gibt es bei der Verknüpfung von 2 Schaltvariablen? Geben Sie sie an.
7. Kann eine beliebige Verknüpfung von zwei Schaltvariablen a und b alleine mithilfe von Negation und Konjunktion geschrieben werden?

Lösungen zu den Kontrollfragen

Lösungen zu Abschnitt 1.1

1. a) falsche Aussage
   b) keine Aussage (man kann nicht sagen, dass dieser Satz entweder wahr oder falsch ist)
   c) wahre Aussage

2. a) „Das Glas ist nicht voll“. („Das Glas ist leer“ wäre eine falsche Verneinung, denn ein Glas, das nicht voll ist, muss nicht notwendigerweise leer sein – es könnte z. B. auch halb voll sein.)
   b) „Er ist nicht der Älteste der Familie“. („Er ist der Jüngste der Familie“ wäre eine falsche Verneinung.)
   c) „7 ist keine gerade Zahl“ oder gleichbedeutend: „7 ist eine ungerade Zahl“.
3. a) ausschließend (der Satz ist im Sinn von „entweder – oder“ gemeint)
   b) einschließend (es kann morgen oder übermorgen oder auch an beiden Tagen schneien)
   c) ausschließend d) ausschließend
4. Das Verbot müsste lauten: „Betreten des Rasens oder Blumenpflücken verboten“ (da bereits Betreten des Rasens allein unerwünscht ist, auch wenn man dabei nicht Blumen pflückt).
5. a) $a \wedge b$ ist falsch, weil nicht sowohl Aussage a als auch Aussage b wahr ist.
   b) $a \vee b$ ist wahr, weil (zumindest) eine der beiden Aussagen a bzw. b wahr ist.
   c) a xor b ist wahr, weil genau eine der beiden Aussagen a bzw. b wahr ist.
6. a) falsch (gestern könnte es geregnet haben)
   b) falsch c) richtig d) falsch e) richtig
7. a) nein (Aussageform) b) wahre (Existenz-)Aussage c) falsche (All-)Aussage
8. a) falsche Aussage; nicht alle natürlichen Zahlen sind kleiner als 3
   b) wahre Aussage; es gibt (zumindest) eine natürliche Zahl, die kleiner als 3 ist
9. richtig
10. a) Nicht alle Tigerkatzen sind gute Mäusejäger (= Es gibt (mindestens) eine Tigerkatze, die kein guter Mäusejäger ist).
    b) Es gibt keinen Matrosen, der schwimmen kann (= Alle Matrosen sind Nichtschwimmer).
    c) Es gibt (zumindest) ein x mit $x \geq 3$.
    d) Es gibt (zumindest) ein x und ein y mit $x^2 + y^2 \neq 4$.
11. a) richtig b) falsch (es kann auch ein Passat sein)
    c) richtig (denn $a \Rightarrow b$ ist gleichbedeutend wie $\overline{b} \Rightarrow \overline{a}$)
    d) falsch
12. a) „n durch 4 teilbar $\Rightarrow$ n gerade“ trifft zu, denn „n durch 4 teilbar $\rightarrow$ n gerade“ ist für alle natürlichen n eine wahre Aussage. (Der Fall $a(n)$ wahr und $b(n)$ falsch (d.h., n durch 4 teilbar, aber n nicht gerade) ist nicht möglich.)
    b) „n gerade $\Rightarrow$ n durch 4 teilbar“ trifft nicht zu, denn „n gerade $\rightarrow$ n durch 4 teilbar“ ist nicht für alle n richtig.
    c) $a(n) \Leftrightarrow b(n)$ trifft nicht zu (weil zwar $a(n) \Rightarrow b(n)$, nicht aber $b(n) \Rightarrow a(n)$ zutrifft).
    d) $\overline{b(n)} \Rightarrow \overline{a(n)}$ trifft zu (da $a(n) \Rightarrow b(n)$ zutrifft).
13. a) $b \Rightarrow a$, aber $a \not\Rightarrow b$ (Ein Notendurchschnitt < 2 ist eine notwendige Voraussetzung für ein Leistungsstipendium; um eines zu bekommen, reicht dieser Notendurchschnitt aber nicht aus. Zum Beispiel muss man zusätzlich die Prüfungen innerhalb einer bestimmten Zeit abgelegt haben.)
    b) ja (da das gleichbedeutend ist zu $b \Rightarrow a$); „kein Notendurchschnitt $< 2 \Rightarrow$ kein Leistungsstipendium“

Lösungen zu Abschnitt 1.2

1. Ja, denn es kommt nicht auf die Reihenfolge der Elemente an.
2. a) $A = \{4\}$ b) $B = \{-4, 4\}$ c) $C = \{1, 2, 3, 4\}$ d) $D = \{\}$
3. a) $A \cup B = \{1, 2, 3, 4\}$ b) $A \cap B = \{2\}$ c) ja d) nein, weil $1 \notin B$
4. a) Menge der Nobelpreisträger, die Österreicher sind oder für Literatur ausgezeichnet wurden (einschließendes „oder“)
   b) Menge der männlichen österreichischen Nobelpreisträger
5. a) falsch; $\{\}$ ist die leere Menge, die Menge $\{0\}$ enthält aber die Zahl 0
   b) richtig c) falsch; $\{1\} \cup \{1\} = \{1\}$ d) richtig e) richtig
   f) falsch; bei Tupeln spielt die Reihenfolge der Elemente eine Rolle
   g) falsch; $\{2, 5, 7\}$ ist eine Menge und $(2, 5, 7)$ ist ein 3-Tupel
   h) falsch; bei Tupeln sind mehrfach auftretende Elemente von Bedeutung
6. a) $A \times B = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\}$
   b) $B \times A = \{(2, 1), (2, 2), (3, 1), (3, 2), (4, 1), (4, 2)\}$
   c) nein d) ja e) $\{1\}$ f) $\{3, 4\}$

Lösungen zu Abschnitt 1.3

1. a) falsch b) richtig c) richtig d) falsch e) richtig
2. Durch Vertauschen von 0 und 1 bzw. von + und · erhalten wir:
   a) $a + 0 = a$ b) $a + (b \cdot c) = (a + b) \cdot (a + c)$ c) $a + (a \cdot b) = a$
3. falsch; die Assoziativgesetze bedeuten, dass man bei Ausdrücken, die nur + oder nur · enthalten, auf Klammern verzichten kann. Bei gemischten Ausdrücken hängt das Ergebnis sehr wohl davon ab, ob man zuerst + oder · durchführt; man kann in diesem Fall nur deshalb auf Klammern verzichten, weil man vereinbart, dass · vor + ausgewertet wird.
4. a) richtig (de Morgan'sche Regel) b) falsch
5. a) $a + (a + \overline{a}) = a + 1 = 1$
   b) Wir werten zunächst $a \cdot \overline{a} = 0$ aus, und damit erhalten wir $a \cdot \overline{a} \cdot a = 0 \cdot a = 0$.
6. Es gibt in diesem Fall 4 Minterme:

a	b	$m_0(a,b) = \overline{a} \cdot \overline{b}$	$m_1(a,b) = \overline{a} \cdot b$	$m_2(a,b) = a \cdot \overline{b}$	$m_3(a,b) = a \cdot b$
0	0	1	0	0	0
0	1	0	1	0	0
1	0	0	0	1	0
1	1	0	0	0	1

7. Ja, denn jede Verknüpfung kann mithilfe der DNF nur mit Disjunktion, Konjunktion und Negation dargestellt werden; mithilfe der de Morgan'schen Regel $a + b = \overline{\overline{a} \cdot \overline{b}}$ kann dann noch jede Disjunktion durch eine Konjunktion ausgedrückt werden.

1.6 Übungen

Aufwärmübungen

1. Ist „Ein Barbier rasiert alle, die sich nicht selbst rasieren“ eine Aussage? (Versuchen Sie, einen Wahrheitswert zuzuordnen.)
2. Aussage a: „Österreich gehört zur EU“; Aussage b: „Österreich grenzt an Spanien“. Welche der folgenden Aussagen sind wahr:
   a) $a \wedge b$ b) $a \vee b$ c) a xor b d) $\overline{b}$
3. Verneinen Sie:
   a) Zu jedem Schloss passt ein Schlüssel.
   b) Es gibt einen Mitarbeiter, der C++ kann.
   c) Für alle x gilt: $f(x) \neq 0$.
   d) Es gibt ein $C > 0$, sodass $f(x) \leq C$ für alle x.
4. Was ist die Verneinung von „In der Nacht sind alle Katzen grau“?
   a) In der Nacht sind nicht alle Katzen grau.
   b) Am Tag ist keine Katze grau.
   c) Es gibt eine Katze, die in der Nacht nicht grau ist.
   d) In der Nacht ist keine Katze grau.
5. Gilt $\Rightarrow$ oder sogar $\Leftrightarrow$? Setzen Sie ein und formulieren Sie sprachlich:
   a) x durch 4 teilbar $\ldots$ x durch 2 teilbar.
   b) x gerade Zahl $\ldots$ $x+1$ ungerade Zahl.
6. Aussage a: „Ich bestehe die Prüfung“; Aussage b: „Ich feiere.“ Für mich gilt: $a \Rightarrow b$, also „Wenn ich die Prüfung bestehe, dann feiere ich“. Was lässt sich daraus über mein Feierverhalten sagen, wenn ich die Prüfung nicht bestehe?
7. Geben Sie die Menge in beschreibender Form an:
   a) $A = \{4, 5, 6\}$ b) $B = \{-1, 0, 1\}$
   c) $C = \{\ldots, -3, -2, -1, 0, 1\}$ d) $D = \{0, 1, 2, \ldots\}$
8. Zählen Sie jeweils die Elemente der Menge auf:
   $A = \{x \in \mathbb{N} \mid 1 < x \leq 5\}$ $B = \{x \in \mathbb{Z} \mid x^2 = 25\}$
   $C = \{x \in \mathbb{Z} \mid x < 0\}$ $D = \{x \in \mathbb{Z} \mid 3x = 0\}$
9. Geben Sie alle 8 Teilmengen von $\{0, 1, 2\}$ an.
10. Ergänzen Sie:
    a) $A \cup A =$ b) $A \cap A =$ c) $\{1\} \cup \{0\} =$ d) $\{\} \cup \{0\} =$
11. Richtig oder falsch: a) $\overline{a + b} = a + \overline{b}$ b) $\overline{a + b} = a \cdot \overline{b}$
12. Überprüfen Sie, ob $a \cdot (\overline{a} + b) = a \cdot b$ ein gültiges Gesetz der Schaltalgebra ist. Wie steht es mit $a + \overline{a} \cdot b = a + b$?
13. Geben Sie a) die DNF und b) die KNF von f_6 und von f_{14} an und vereinfachen Sie gegebenenfalls das Ergebnis.
14. Vereinfachen Sie: a) $a \cdot (\overline{a} + b)$ b) $(a \cdot \overline{b}) + b$ c) $a \cdot b + a \cdot \overline{b}$

Weiterführende Aufgaben

1. Verneinen Sie:
   a) Es gibt ein $x \in A$ mit $x < 5$.

b) Alle Pinguine schwimmen gerne.
c) Das Auto ist blau und wurde vor dem Jahr 2005 zugelassen.
d) $(x \in A)$ oder $(x \in B)$

2. Es gilt: „Wenn ich schlafe, habe ich geschlossene Augen.“ Was trifft zu?
   a) Wenn meine Augen offen sind, bin ich wach.
   b) Wenn ich nicht schlafe, sind meine Augen offen.
   c) Wenn ich geschlossene Augen habe, schlafe ich.
3. Verneinen Sie: „Alle Anwesenden sprechen Deutsch oder Englisch.“
4. Graf Hubert wurde in seinem Arbeitszimmer ermordet. Der Arzt hat festgestellt, dass der Tod zwischen 9:30 und 10:30 Uhr eingetreten ist. Die Haushälterin von Graf Hubert ist um 10:00 vom Garten in die Küche gegangen. Um an der Haushälterin vorbeizukommen, muss der Mörder vor 10:00 mit einem Schlüssel durch die Eingangstür oder nach 10:00 durchs Fenster eingestiegen sein.
   Kommissar Berghammer vermutet einen der drei Erben A, B oder C als Mörder. A hat als einziger einen Schlüssel, kann aber wegen seines Gipsfußes nicht durchs Fenster gestiegen sein. A und B haben beide kein Alibi für die Zeit nach 10 Uhr (wohl aber für die Zeit vor 10) und C hat kein Alibi für die Zeit vor 10 (wohl aber für nach 10).
   Wer von den dreien kommt als Mörder in Frage?

   (Tipp: Führen Sie z. B. folgende Aussagen ein: $S =$ „X hat einen Schlüssel“, $F =$ „X kann durchs Fenster klettern“, $V =$ „X hat kein Alibi vor 10“, $N =$ „X hat kein Alibi nach 10“. Aus der Angabe geht hervor, dass für den Mörder $S \vee F$ und $V \vee N$ und $\overline{N} \to S$ und $\overline{V} \to F$ wahr sein muss. (Finden Sie noch eine andere Möglichkeit für eine logische Formel, die den Mörder entlarvt?). Stellen Sie nun eine Wahrheitstabelle für $X = A, B, C$ auf.

	S	F	...
A	...	...	...
B	...	...	...
C	...	...	...

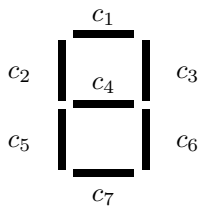
5. Eine KFZ-Versicherung hat ihre Kunden in folgende Mengen eingeteilt:
   - K ... Menge aller Kunden
   - U ... Kunden, die einen Unfall verursacht haben
   - G ... Kunden, die einen Strafzettel wegen überhöhter Geschwindigkeit bekommen haben
   - A ... Kunden, die wegen Alkohol am Steuer verurteilt worden sind

   Geben Sie folgende Mengen an (durch Bildung von Durchschnitt, Vereinigung, usw. ... von K, U, G, A):
   a) alkoholisiert oder Unfall b) weder Unfall noch alkoholisiert
   c) kein Vergehen d) kein Unfall, aber alkoholisiert
6. Gegeben seien Mengen A, B, M mit $A, B \subseteq M$. Vereinfachen Sie durch Anwendung von Rechengesetzen für Mengen: a) $A \cap (B \cup \overline{A})$ b) $(A \cap B) \cup (\overline{A} \cap B)$
7. Vereinfachen Sie: a) $(a+b) \cdot (\overline{a}+b)$ b) $a+(\overline{a \cdot b})+(b \cdot c)$ c) $(\overline{a+b})+(a \cdot \overline{b})$
8. Zeigen Sie mithilfe einer Wahrheitstabelle, dass die Formel für die DNF

$$f(a,b) = f(0,0) \cdot \overline{a} \cdot \overline{b} + f(0,1) \cdot \overline{a} \cdot b + f(1,0) \cdot a \cdot \overline{b} + f(1,1) \cdot a \cdot b$$

   gilt. Leiten Sie daraus die KNF für $f(a,b)$ her (Tipp: Verneinung beider Seiten der DNF und dann Anwendung der de Morgan'schen Regeln).

9. Eine einstellige LCD-Anzeige kann durch die sieben Variablen



dargestellt werden. Überlegen Sie zunächst, welche Balken c_j aufleuchten müssen, um die Zahlen 0, 1, 2, 3 darzustellen (Für die Anzeige der Zahl 3 leuchten zum Beispiel alle Balken außer c_2 und c_5). Dabei bedeutet $c_j = 1$, dass der zugehörige Balken leuchtet und $c_j = 0$, dass der zugehörige Balken nicht leuchtet. Geben Sie dann $c_1, \ldots, c_7$ als Verknüpfungen von a und b (Eingangsvariable) an, wenn $(ab)_2$ die zugehörige Dualdarstellung der anzuzeigenden Zahl ist.

Tipp: Stellen Sie z. B. eine Tabelle der folgenden Form auf und geben Sie die DNF oder die KNF der c_j an:

a	b	c_1	c_2	...
0	0	1	1	...
0	1			
1	0			
1	1			

10. Entwerfen Sie eine Schaltung für eine IF-Abfrage $\text{if}(t, a, b)$, die den Wert von a zurückliefert, falls $t = 1$, und den Wert von b falls $t = 0$. (Tipp: Verwenden Sie die DNF in drei Variablen. Siehe Abschnitt 1.3.1.)
11. In der **Fuzzy-Logik** (engl. *fuzzy* = unscharf, verschwommen) werden nicht nur die Wahrheitswerte 0 und 1, sondern beliebige reelle Werte im Intervall $[0, 1]$ zugelassen. Der Wahrheitswert einer Aussage kann als Wahrscheinlichkeit, mit der die Aussage wahr ist, interpretiert werden. Je kleiner der Wert ist, umso unwahrscheinlicher ist es, dass die Aussage wahr ist. Die logischen Operationen sind wie folgt definiert:

$$\overline{a} = 1 - a, \qquad a \wedge b = \min(a, b), \qquad a \vee b = \max(a, b).$$

Hier ist $\max(a, b)$ die größere der beiden Zahlen und $\min(a, b)$ die kleinere der beiden Zahlen a und b.

Diese Definition kann als Verallgemeinerung der UND- bzw. ODER-Verknüpfung in der zweiwertigen Logik angesehen werden. Auch dort hat $a \wedge b$ immer den kleineren der beiden Werte von a und b bzw. $a \vee b$ hat den größeren der beiden Werte. Auch in der Fuzzy-Logik gelten die Logikgesetze aus Satz 1.42:

Zeigen Sie, dass die de Morgan'schen Regeln

$$\overline{a \wedge b} = \overline{a} \vee \overline{b}, \qquad \overline{a \vee b} = \overline{a} \wedge \overline{b}$$

auch für die Fuzzy Logik gültig sind. (Tipp: Betrachten Sie die Fälle $a < b$, $a = b$ und $a > b$.)

Lösungen zu den Aufwärmübungen

1. keine Aussage; es ist unmöglich, einen Wahrheitswert zuzuordenen, denn in jedem Fall führt der Satz auf einen Widerspruch.
2. a) falsche Aussage b) wahre Aussage c) wahre Aussage d) wahre Aussage
3. a) „Nicht zu jedem Schloss passt ein Schlüssel“ oder „Es gibt (mindestens) ein Schloss, zu dem kein Schlüssel passt“. (Verneinung einer All-Aussage ergibt eine Existenz-Aussage.)
   b) „Für alle Mitarbeiter gilt: Er/sie kann C++ nicht“ bzw. „Es gibt keinen Mitarbeiter, der C++ kann“.
   c) „Es gibt (mindestens) ein x mit $\overline{f(x) \neq 0}$“, d.h. „Es gibt (mindestens) ein x mit $f(x) = 0$“.
   d) „Für alle $C > 0$ gilt: $\overline{f(x) \leq C \text{ für alle } x}$“, d.h. „Für alle $C > 0$ gilt: Es gibt ein x mit $\overline{f(x) \leq C}$“, also „Für alle $C > 0$ gilt: Es gibt ein x mit $f(x) > C$“. Sprachlich noch etwas schöner: „Zu jedem $C > 0$ gibt es (mindestens) ein x mit: $f(x) > C$. Alternativ kann man auch sagen: „Es gibt kein C, sodass $f(x) \leq C$ für alle x“.
4. a) ja b) nein c) ja d) nein
5. a) x durch 4 teilbar $\Rightarrow$ x durch 2 teilbar. Die Umkehrung gilt nicht. In Worten: „Wenn x durch 4 teilbar ist, dann ist x auch durch 2 teilbar (aber nicht umgekehrt)“ oder „x durch 4 teilbar ist hinreichend (aber nicht notwendig) dafür, dass x durch 2 teilbar ist“.
   b) x gerade $\Leftrightarrow$ $x + 1$ ungerade; „ x ist gerade genau dann, wenn $x + 1$ ungerade ist“.
6. Es lässt sich über mein „Feierverhalten“ nichts sagen (meine Regel sagt nur etwas für den Fall aus, dass ich die Prüfung bestehe).
7. Zum Beispiel:
   a) $A = \{x \in \mathbb{N} \mid 4 \leq x \leq 6\}$ b) $B = \{x \in \mathbb{Z} \mid -1 \leq x \leq 1\}$
   c) $C = \{x \in \mathbb{Z} \mid x \leq 1\}$ d) $D = \mathbb{N} \cup \{0\}$
8. $A = \{2, 3, 4, 5\}$, $B = \{-5, 5\}$, $C = \{\ldots, -3, -2, -1\}$, $D = \{0\}$
9. $\{\}$, $\{0\}$, $\{1\}$, $\{2\}$, $\{0, 1\}$, $\{0, 2\}$, $\{1, 2\}$, $\{0, 1, 2\}$
10. a) A b) A c) $\{0, 1\}$ d) $\{0\}$
11. a) falsch (Wertetabelle) b) richtig (Wertetabelle bzw. de Morgan’sche Regel)
12. beide richtig (Wahrheitstabelle oder Umformung mithilfe der Rechenregeln der Schaltalgebra)
13. a) DNF: $f_6(a, b) = \overline{a} \cdot b + a \cdot \overline{b}$ ($= a$ xor b) und $f_{14}(a, b) = a \cdot \overline{b} + b \cdot \overline{a} + a \cdot b$. Die Darstellung von f_{14} kann noch vereinfacht werden: $a \cdot \overline{b} + b \cdot \overline{a} + a \cdot b = a \cdot \overline{b} + b \cdot (\overline{a} + a) = a \cdot \overline{b} + b \cdot 1 = a \cdot \overline{b} + b = b + (a \cdot \overline{b}) = (b + a) \cdot (b + \overline{b}) = (b + a) \cdot 1 = a + b$.
    b) KNF: $f_6(a, b) = (a + b) \cdot (\overline{a} + \overline{b})$ (überzeugen Sie sich durch Anwendung der Rechenregeln davon, dass das gleich $\overline{a} \cdot b + a \cdot \overline{b}$ ist) und $f_{14} = a + b$.
14. a) $a \cdot (\overline{a} + b) = a \cdot \overline{a} + a \cdot b = a \cdot b$, da $a \cdot \overline{a} = 0$ ist.
    b) $(a \cdot \overline{b}) + b = b + (a \cdot \overline{b})$ (... Kommutativgesetz) $= (b + a) \cdot (b + \overline{b})$ (... Distributivgesetz) $= (b + a) \cdot 1 = b + a = a + b$.
    c) $a \cdot b + a \cdot \overline{b} = a \cdot (b + \overline{b})$ (... Distributivgesetz) $= a \cdot 1 = a$.

(Lösungen zu den weiterführenden Aufgaben finden Sie in Abschnitt B.1)

2

Zahlenmengen und Zahlensysteme

2.1 Die Zahlenmengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$

In diesem Abschnitt werden Ihnen einige vertraute Begriffe begegnen. Wir beginnen mit den natürlichen Zahlen. Sie haben sich historisch einerseits aus der Notwendigkeit zu *zählen* („Kardinalzahlen“) und andererseits aus dem Bedürfnis zu *ordnen* („Ordinalzahlen“) entwickelt:

Die natürlichen Zahlen $\mathbb{N}$

Definition 2.1 Die Menge $\mathbb{N} = \{1, 2, 3, \ldots\}$ heißt Menge der **natürlichen Zahlen**. Nehmen wir die Zahl „0“ hinzu, so schreiben wir $\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, \ldots\}$.

In manchen Büchern wird auch die Zahl „0“ als natürliche Zahl betrachtet.

Die natürlichen Zahlen sind **geordnet**. Das heißt, dass es zu jeder Zahl n einen eindeutigen **Nachfolger** $n + 1$ gibt. Man kann also die natürlichen Zahlen wie auf einer Kette auffädeln. Wir erhalten dadurch die *Ordnungsrelation* „m kleiner n“, geschrieben

$$m < n,$$

die aussagt, dass in der „Kette“ der natürlichen Zahlen m vor n kommt. Die Schreibweise $m \leq n$ bedeutet, dass m kleiner oder gleich n ist. Beispiel: $3 < 5$; eine andere Schreibweise dafür ist $5 > 3$ (die Spitze zeigt immer zur kleineren Zahl). Oder: $n \in \mathbb{N}$, $n \geq 3$ bedeutet: n ist eine natürliche Zahl größer oder gleich 3.

Die ganzen Zahlen $\mathbb{Z}$

Das „Rechnen“ mit natürlichen Zahlen ist für uns kein Problem. Wenn wir zwei natürliche Zahlen addieren oder multiplizieren, so ist das Ergebnis stets wieder eine natürliche Zahl. Die Subtraktion führt uns aber aus der Menge der natürlichen Zahlen hinaus: Es gibt zum Beispiel keine natürliche Zahl x, die $x + 5 = 3$ erfüllt. Um diese Gleichung zu lösen, müssen wir den Zahlenbereich der natürlichen Zahlen auf den der ganzen Zahlen erweitern:

Definition 2.2 Die Menge $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ heißt Menge der **ganzen Zahlen**.

Jede natürliche Zahl ist auch eine ganze Zahl: $\mathbb{N} \subseteq \mathbb{Z}$. Die ganzen Zahlen sind wie die natürlichen Zahlen geordnet, können also ebenso auf einer Kette aufgereiht werden. Beachten Sie dabei, dass $m < n \Leftrightarrow -n < -m$. Beispiel: Es ist $1 < 2$, jedoch $-2 < -1$ (und nicht $-1 < -2$)!

Die rationalen Zahlen $\mathbb{Q}$

Auch wenn uns nun bereits alle ganzen Zahlen zur Verfügung stehen, so stoßen wir doch sehr bald wieder auf Probleme: Es gibt z. B. keine ganze Zahl x, die die Gleichung $3x = 2$ erfüllt. Wieder müssen wir neue Zahlen hinzunehmen und sind damit bei den rationalen Zahlen angelangt:

Definition 2.3 Die Menge

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid q \neq 0 \text{ und } p, q \in \mathbb{Z} \right\}$$

heißt Menge der **rationalen Zahlen** oder auch Menge der Bruchzahlen. Man nennt p den **Zähler** und q den **Nenner** der rationalen Zahl $\frac{p}{q}$.

Der Nenner einer rationalen Zahl muss also laut Definition immer ungleich 0 sein. Es gibt unendlich viele rationale Zahlen. Die ganzen Zahlen begegnen uns dabei als Brüche mit Nenner 1: $\mathbb{Z} = \{\ldots, -\frac{2}{1}, -\frac{1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{2}{1}, \ldots\} \subseteq \mathbb{Q}$.

Man vereinbart, dass zwei rationale Zahlen $\frac{p_1}{q_1}$ und $\frac{p_2}{q_2}$ gleich sind genau dann, wenn $p_1 \cdot q_2 = q_1 \cdot p_2$. Das heißt nichts anderes, als dass Zähler und Nenner mit dem gleichen Faktor multipliziert bzw. durch den gleichen Faktor dividiert (*gekürzt*) werden können. Beispiel: $\frac{8}{16} = \frac{1}{2} = \frac{-4}{-8} = \ldots$

Addition und Multiplikation von rationalen Zahlen sind folgendermaßen definiert:

$$\begin{aligned} \frac{p_1}{q_1} + \frac{p_2}{q_2} &= \frac{p_1\, q_2 + p_2\, q_1}{q_1\, q_2}, \\ \frac{p_1}{q_1} \cdot \frac{p_2}{q_2} &= \frac{p_1\, p_2}{q_1\, q_2}. \end{aligned}$$

Beispiele: $\frac{3}{5} + \frac{1}{4} = \frac{3 \cdot 4 + 1 \cdot 5}{20} = \frac{17}{20}$; $\frac{3}{5} \cdot \frac{1}{4} = \frac{3}{20}$. Ich gehe aber davon aus, dass Ihnen das Rechnen mit rationalen Zahlen vertraut ist. Erinnern möchte ich Sie noch an die Abkürzung **Prozent** für „ein Hundertstel“:

$$1\% = \frac{1}{100} = 0.01.$$

Beispiele: $0.62 = 62\%$; $0.0003 = 0.03\%$.

Für das n-fache Produkt der rationalen Zahl a mit sich selbst verwendet man die abkürzende Schreibweise

$$a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ Faktoren}}.$$

Dabei heißt a die **Basis** und n der **Exponent** der **Potenz** a^n. Für $a \neq 0$ vereinbart man außerdem

$$a^{-n} = \frac{1}{a^n} \qquad \text{und} \qquad a^0 = 1.$$

Negative Potenzen sind also nichts anderes als die Kehrwerte von positiven Potenzen. Beispiele: $10^2 = 100$; $2^4 = 16$; $2^{-1} = \frac{1}{2}$; $(\frac{3}{4})^{-1} = \frac{4}{3}$; $2^0 = 1$. Mit dieser Definition gilt für $a, b \in \mathbb{Q}$ und $m, n \in \mathbb{Z}$ ($a, b \neq 0$, falls $m < 0$ oder $n < 0$)

$$a^n a^m = a^{n+m}, \qquad a^n b^n = (a\,b)^n, \qquad (a^m)^n = a^{m\,n},$$

wie man sich leicht überlegen kann. Beispiele: $x^4 \cdot x^2 = x^6$; $10^{-3} \cdot (\frac{1}{2})^{-3} = 5^{-3}$; $(x^4)^3 = x^{12}$.

Die Ordnung auf $\mathbb{Q}$ ist durch

$$\frac{p_1}{q_1} < \frac{p_2}{q_2} \quad \Leftrightarrow \quad p_1 q_2 < p_2 q_1, \qquad q_1, q_2 > 0,$$

erklärt. Die Voraussetzung $q_1, q_2 > 0$ ist keine Einschränkung, da wir das Vorzeichen des Nenners ja immer in den Zähler packen können. Beispiel: $\frac{1}{4} < \frac{3}{5}$, da $1 \cdot 5 < 3 \cdot 4$. Es ergeben sich folgende Regeln:

Satz 2.4 (Rechenregeln für Ungleichungen) Für $a, b, c \in \mathbb{Q}$ gilt:

- $a < b$ und $b < c \quad \Rightarrow \quad a < c$
- $a < b \quad \Leftrightarrow \quad a + c < b + c$
- $a < b \quad \Leftrightarrow \quad ac < bc \qquad$ falls $c > 0$
- $a < b \quad \Leftrightarrow \quad ac > bc \qquad$ falls $c < 0$

Die Regeln bleiben natürlich auch gültig, wenn man $<$ durch $\leq$ ersetzt.

Beispiele:
• $2 < 4$ und $4 < 7$, daher $2 < 7$. Oder: Wenn $x < 4$ und $y > 4$, so folgt $x < y$.
• $x < y + 1$ bedeutet $x - 1 < y$ (auf beiden Seiten wurde $c = -1$ addiert).
• Wenn $x + 10 < 5y$, so ist das gleichbedeutend mit $\frac{1}{5}x + 2 < y$.
• $-2x < 8$ ist äquivalent zu $x > -4$ (auf beiden Seiten wurde mit $c = -\frac{1}{2}$ multipliziert).

Sie können also jederzeit bei einer Ungleichung auf beiden Seiten die gleiche Zahl addieren oder beide Seiten mit der gleichen *positiven* Zahl multiplizieren. Multiplizieren Sie aber beide Seiten mit einer negativen Zahl, so muss das Ungleichzeichen umgedreht werden! Insbesondere:

Satz 2.5 Für $a, b \in \mathbb{Q}$ und $n \in \mathbb{N}$ gilt:

$$a < b \quad \Leftrightarrow \quad a^n < b^n \qquad \text{falls } a, b > 0.$$

Beispiel: $5 < 7$ ist äquivalent zu $5^9 < 7^9$. Aber Achtung: Die Äquivalenz gilt nur für $a, b > 0$! Für $x \in \mathbb{Q}$ (d.h., auch negative x eingeschlossen) gilt zum Beispiel: Aus

$x^2 < 49$ folgt $x < 7$, aber die Umkehrung ist nicht zutreffend: $x < 7 \not\Rightarrow x^2 < 49$ (warum?).

Man könnte glauben, dass nun alle Zahlen „gefunden“ sind. Die Anhänger von Pythagoras (ca. 570–480 v. Chr.) im antiken Griechenland waren jedenfalls dieser Ansicht. Insbesondere waren sie davon überzeugt, dass es eine rationale Zahl geben muss, deren Quadrat gleich 2 ist:

Zeichnen wir ein Quadrat mit der Seitenlänge 1. Dann gilt nach dem Satz des Pythagoras für die Länge d der Diagonale: $d^2 = 1^2 + 1^2 = 2$ (siehe Abbildung 2.1). Gibt es eine *rationale* Zahl d, deren Quadrat gleich 2 ist? Durch scharfes Hinsehen

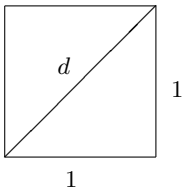


Abbildung 2.1. Quadrat mit Seitenlänge 1

lässt sich d auf jeden Fall nicht angeben. Es bleibt uns daher nichts anderes übrig, als systematisch nach Werten für p und q mit $(\frac{p}{q})^2 = 2$ zu suchen.

Beginnen wir mit $q = 2$ und probieren der Reihe nach Werte für p durch. Da $d \geq 1$ ist, kommen nur Werte $p = 2, 3, \ldots$ in Frage. Mit $p = 2$ folgt $(\frac{2}{2})^2 = 1 < 2 = d^2$ und deshalb (mit Satz 2.5) $1 < d$. Mit $p = 3$ folgt $(\frac{3}{2})^2 = \frac{9}{4} > 2 = d^2$ und deshalb $d < \frac{3}{2}$. Alle weiteren Werte $p = 4, 5, \ldots$ liefern nur noch größere Zahlen und $q = 2$ ist damit aus dem Rennen. Trotzdem können wir aber wenigstens schon den Bereich, in dem d zu suchen ist, einschränken (also eine grobe Abschätzung nach unten und oben für d geben): $1 < d < \frac{3}{2}$.

Die Wahl $q = 2$ hat zwar nicht geklappt, so leicht geben wir aber nicht auf, denn es stehen ja noch ausreichend Kandidaten zur Verfügung: $q = 3, 4, \ldots$! Da die Suche von Hand allerdings etwas mühsam ist, bietet sich ein Computerprogramm(→CAS) an, das für gegebenes q zwei rationale Zahlen $\frac{p-1}{q}$ und $\frac{p}{q}$ liefert, zwischen denen d liegen muss:

- Beginne die Suche bei $p = q$.
- Erhöhe p so lange um eins, wie $(\frac{p}{q})^2 < 2$ erfüllt ist.
- Gib $\frac{p-1}{q}$ und $\frac{p}{q}$ aus.

Damit können wir nun den Computer auf die Suche schicken. Sie können es gerne ausprobieren, aber leider kann ich Ihnen jetzt schon sagen, dass Ihre Suche erfolglos bleiben wird:

Satz 2.6 (Euklid) Es gibt keine rationale Zahl, deren Quadrat gleich 2 ist.

Den Beweis hat erstmals der griechische Mathematiker Euklid (ca. 300 v. Chr.) geführt, und sein Beweis gilt als Musterbeispiel der mathematischen Beweisführung. Es ist ein Beweis durch Wider-

spruch. Dabei wird aus der Verneinung (Negation) der Behauptung ein Widerspruch abgeleitet, weshalb die Verneinung falsch und daher die Behauptung wahr sein muss. Hier Euklids Beweis:

Angenommen $d = \frac{p}{q}$ ist eine rationale Zahl, deren Quadrat gleich 2 ist. Natürlich können wir voraussetzen, dass p und q nicht *beide* gerade sind, denn sonst könnten wir ja einfach den gemeinsamen Faktor kürzen.

Es ist also $(\frac{p}{q})^2 = 2$ oder, leicht umgeformt $p^2 = 2q^2$. Da $p^2 = 2q^2$ offensichtlich eine gerade Zahl ist (da Vielfaches von 2), muss auch p eine gerade Zahl sein (denn wenn das Produkt zweier Zahlen gerade ist (hier $p \cdot p$), dann muss mindestens eine der beiden Zahlen gerade sein). Wir können daher p in der Form $p = 2p_0$ mit einer natürlichen Zahl p_0 schreiben, und daraus ergibt sich nach Quadrieren beider Seiten: $p^2 = 4p_0^2$.

Aus $p^2 = 2q^2$ und $p^2 = 4p_0^2$ folgt nun $2q^2 = 4p_0^2$, und nachdem wir beide Seiten durch 2 dividiert haben: $q^2 = 2p_0^2$. Mit der gleichen Überlegung wie oben folgt daraus, dass q gerade ist. Also sind p und q beide gerade, was wir aber doch am Anfang ausgeschlossen haben! Unsere Annahme, d sei rational, führt also zu einem Widerspruch und muss daher falsch sein.

Etwa 200 Jahre vor Euklids Beweis hat Hippasus, ein Schüler von Pythagoras, die Vermutung geäußert, dass d keine rationale Zahl sei. Die Pythagoräer sollen darüber so erzürnt gewesen sein, dass sie Hippasus ertränken ließen. Ich hoffe, Sie wünschen mich jetzt nicht auch auf den Grund des Ozeans, weil ich Sie mit diesem Beweis gelangweilt habe.

Die reellen Zahlen $\mathbb{R}$

Die Länge der Diagonale unseres Quadrates ist also keine rationale Zahl, kann aber, wie wir gesehen haben, *beliebig genau durch rationale Zahlen approximiert (d.h. angenähert) werden*: In der Tat können wir zum Beispiel $q = 100$ wählen, und unser Programm liefert uns die Schranken $\frac{141}{100} < d < \frac{142}{100}$. Wählen wir den Wert in der Mitte $d \approx \frac{283}{200}$, so haben wir d bis auf einen Fehler von maximal $\frac{1}{200}$ approximiert, was für viele Zwecke vollkommen ausreichend ist.

Der Ausweg aus dem Dilemma ist also, die Menge der rationalen Zahlen um jene Zahlen zu erweitern, die sich durch rationale Zahlen approximieren lassen:

Definition 2.7 Die Menge $\mathbb{R}$ der **reellen Zahlen** besteht aus den rationalen Zahlen und aus Zahlen, die sich beliebig genau durch rationale Zahlen „approximieren“ lassen.

Wir wollen hier nicht näher auf die Konstruktion der reellen Zahlen eingehen und uns damit begnügen, dass die reellen Zahlen alle Rechenregeln (inklusive der Ordnung mittels $<$) von den rationalen Zahlen erben und die rationalen Zahlen als Teilmenge enthalten. Außerdem kann jede reelle Zahl beliebig genau durch rationale Zahlen angenähert werden. Das bedeutet: Ist eine Fehlerschranke gegeben, so können wir zu jeder reellen Zahl eine rationale Zahl finden, die unsere Fehlerschranke unterbietet. Beispiel: Ist die Fehlerschranke $\frac{1}{200}$, so können wir für die reelle Zahl $\sqrt{2}$ die rationale Zahl $\frac{283}{200}$ wählen.

Eine etwas konkretere Definition mithilfe von Dezimalzahlen (Kommazahlen) wird in Abschnitt 2.4 gegeben. Die Approximation ergibt sich dann dadurch, dass man je nach gewünschter Genauigkeit nach einer bestimmten Anzahl von Nachkommastellen abbricht.

Reelle Zahlen, die nicht rational sind, nennt man **irrationale Zahlen**. Ihre Existenz hat man, wie der Name zeigt, lange nicht wahrhaben wollen. Zwei der wichtigsten und zugleich bekanntesten irrationalen Zahlen sind die **Euler'sche Zahl**

$$\mathrm{e} = 2.7182818285\ldots$$

und die **Kreiszahl**

$$\pi = 3.1415926535\ldots$$

Der Schweizer Leonhard Euler (1707–1783) war einer der bedeutendsten und produktivsten Mathematiker aller Zeiten. Sein Werk umfasst über 800 Publikationen und ein großer Teil der heutigen mathematischen Symbolik geht auf ihn zurück (z. B. e, π, i, das Summenzeichen, die Schreibweise $f(x)$ für Funktionen).

In der Praxis, muss man eine irrationale Zahl immer durch eine rationale Zahl approximieren. Zum Beispiel ist $\pi \approx \frac{22}{7}$ eine gute Näherung, bei der der relative Fehler $\frac{22/7-\pi}{\pi}$ nur ca. 0.04% beträgt. Wie genau der Wert von π sein muss, hängt immer vom betrachteten Problem ab. Falls Sie mit $\pi \approx \frac{22}{7}$ die benötigte Farbmenge für einen runden Tisch ausrechnen, geht das sicher in Ordnung. Verwenden Sie es aber zur Berechnung der Flugbahn einer Mondsonde, so ergibt ein relativer Fehler von 0.04% bei der Entfernung zum Mond von 384 000 km einen Fehler von 155 km, und das könnte bedeuten, dass Ihre Sonde den Mond knapp, aber doch, verfehlt.

Es gilt also alles, was wir bis jetzt über rationale Zahlen gelernt haben, auch für reelle Zahlen. Außerdem können wir nun problemlos Wurzelziehen:

Definition 2.8 Wenn $b^n = a$ für $a, b \geq 0$, $n \in \mathbb{N}$, so heißt b die **n-te Wurzel** von a. Man schreibt

$$b = \sqrt[n]{a} \quad \text{oder auch} \quad b = a^{\frac{1}{n}},$$

und b ist für jede positive reelle Zahl a eindeutig bestimmt.

Beispiele: $2^4 = 16$, daher: $16^{\frac{1}{4}} = \sqrt[4]{16} = 2$. Oder: $10^3 = 1000$, daher: $\sqrt[3]{1000} = 10$. Außerdem gilt

$$\sqrt[n]{a\,b} = \sqrt[n]{a}\,\sqrt[n]{b}.$$

Beispiel: $\sqrt{4x} = \sqrt{4}\sqrt{x} = 2\sqrt{x}$. Wird n nicht angegeben, so ist $n = 2$, d.h. $\sqrt{a} = \sqrt[2]{a}$. Das Wurzelziehen führt oft auf ein irrationales Ergebnis. So ist ja, wie wir vorhin gesehen haben, $\sqrt{2}$ eine irrationale Zahl.

Die Definition einer Potenz lässt sich nun für *beliebige rationale* Exponenten erweitern.

Definition 2.9 Für reelles $a > 0$ und $m \in \mathbb{N}, n \in \mathbb{Z}$ ist $a^{\frac{n}{m}}$ als die n-te Potenz der m-ten Wurzel von a definiert:

$$a^{\frac{n}{m}} = (a^{\frac{1}{m}})^n = (\sqrt[m]{a})^n.$$

Beispiel: $5^{\frac{2}{3}} = (5^{\frac{1}{3}})^2 = (\sqrt[3]{5})^2$. Potenzen mit *irrationalen* Exponenten definiert man, indem man die irrationale Zahl durch rationale Zahlen annähert.

Das geschieht folgendermaßen: Sei b irgendeine irrationale Zahl und $b_1, b_2, b_3, \ldots$ eine Folge von Zahlen, die b approximieren. Dann approximiert man a^b durch $a^{b_1}, a^{b_2}, a^{b_3}, \ldots$ In diesem Sinn kann man zum Beispiel 2^π je nach gewünschter Genauigkeit durch rationale Zahlen $2^{3.14}$, $2^{3.141}$, $2^{3.1415}$, $\ldots$ annähern.

Es gelten weiterhin die bekannten Regeln

Satz 2.10 (Rechenregeln für Potenzen) Für $a, b > 0$ und $x, y \in \mathbb{R}$ gilt:

$$a^x \cdot a^y = a^{x+y}, \qquad a^x \cdot b^x = (a \cdot b)^x, \qquad (a^x)^y = a^{(x \cdot y)}, \qquad a^{-x} = \frac{1}{a^x}.$$

Beispiele: $2^3 \cdot 2^5 = 2^8$, $10^{-1} \cdot 10^3 = 10^2$, $3^4 \cdot 5^4 = 15^4$, $(a^{\frac{1}{2}})^6 = a^3$.

Die Zahlen -3 und 3 haben, wenn wir sie uns auf einer Zahlengeraden vorstellen, von 0 denselben Abstand, nämlich 3 Längeneinheiten. Diesen Abstand einer reellen Zahl von 0 nennt man den Betrag der Zahl. Er ist – als Länge – immer nichtnegativ.

Definition 2.11 Der **Absolutbetrag** oder kurz **Betrag** einer reellen Zahl a ist definiert durch

$$|a| = a \quad \text{wenn } a \geq 0 \qquad \text{und} \qquad |a| = -a \quad \text{wenn } a < 0.$$

Die Schreibweise $|a| = -a$ für $a < 0$ erscheint vielleicht etwas verwirrend, sagt aber nichts anderes als: Wenn a negativ ist, dann ist der Betrag gleich der positiven Zahl $-a$.

Beispiel: Für $a = -3$ ist $|a| = |-3| = -(-3) = 3 = -a$. Insbesondere ist $|3| = |-3| = 3$. Der Absolutbetrag $|a-b|$ wird als **Abstand** der Zahlen a und b bezeichnet. Beispiele: Der Abstand von 3 und -2 ist $|3-(-2)| = 5$; der Abstand von -3 und 0 ist $|-3-0| = 3$. Eine Abschätzung, die oft verwendet wird, sagt aus, dass der Betrag einer Summe kleiner oder gleich als die Summe der Beträge ist:

Satz 2.12 (Dreiecksungleichung) Für zwei beliebige reelle Zahlen a und b gilt

$$|a + b| \leq |a| + |b|.$$

Haben beide Zahlen gleiches Vorzeichen, so gilt Gleichheit. Haben sie aber verschiedenes Vorzeichen, so hebt sich links ein Teil weg, und $|a + b|$ ist strikt kleiner als $|a|+|b|$. Beispiele: $|2+3| = |2|+|3|$; $|-2-3| = |-2|+|-3|$; $|2-3| = |-1| < |2|+|-3|$.

Nun werden wir noch einige Begriffe und Schreibweisen für reelle Zahlen einführen, die Ihnen aber sicher schon bekannt sind. Zunächst kommen einige Abkürzungen für bestimmte Teilmengen der reellen Zahlen:

$$\begin{aligned}
[a,b] &= \{x \in \mathbb{R} \mid a \leq x \leq b\} && \text{heißt } \textbf{abgeschlossenes Intervall,} \\
[a,b) &= \{x \in \mathbb{R} \mid a \leq x < b\} && \text{und} \\
(a,b] &= \{x \in \mathbb{R} \mid a < x \leq b\} && \text{heißen } \textbf{halboffene Intervalle,} \\
(a,b) &= \{x \in \mathbb{R} \mid a < x < b\} && \text{heißt } \textbf{offenes Intervall}.
\end{aligned}$$

Man nennt sie **endliche Intervalle**, im Gegensatz zu **unendlichen Intervallen**, die „unendlich lang“ sind. Diese unendliche Länge drückt man mit dem Unendlich-Zeichen ∞ aus:

$$\begin{aligned}
[a,\infty) &= \{x \in \mathbb{R} \mid a \leq x\} \\
(a,\infty) &= \{x \in \mathbb{R} \mid a < x\} \\
(-\infty,b] &= \{x \in \mathbb{R} \mid x \leq b\} \\
(-\infty,b) &= \{x \in \mathbb{R} \mid x < b\}.
\end{aligned}$$

Beispiele: $[0,1]$ enthält alle reellen Zahlen zwischen 0 und 1 inklusive 0 und 1. Hingegen ist in $(0,1]$ die 0 nicht enthalten. Das Intervall $(-\infty,0)$ enthält alle negativen reellen Zahlen.

Anstelle einer runden Klammer wird auch oft eine umgedrehte eckige Klammer verwendet: $(a,b] =]a,b]$, $[a,b) = [a,b[$, $(a,b) =]a,b[$.

Definition 2.13 Eine Menge $M \subseteq \mathbb{R}$ von reellen Zahlen heißt **nach oben beschränkt**, falls es eine Zahl $K \in \mathbb{R}$ gibt mit

$$x \leq K \text{ für alle } x \in M.$$

Eine solche Zahl K wird als eine **obere Schranke** von M bezeichnet.

Eine Menge muss nicht nach oben beschränkt sein. Falls sie es ist, so nennt man die *kleinste* obere Schranke das **Supremum** von M. Man schreibt für das Supremum kurz $\sup M$. Ist M nach oben beschränkt, so ist das Supremum eine eindeutig bestimmte Zahl:

Satz 2.14 (Vollständigkeit der reellen Zahlen) Jede nach oben beschränkte Menge $M \subseteq \mathbb{R}$ besitzt ein Supremum.

Dieser Satz gilt nicht in $\mathbb{Q}$, denn zum Beispiel die Menge $\{x \in \mathbb{Q} \mid x^2 < 2\}$ hat eben kein Supremum *in* $\mathbb{Q}$. Das Supremum $\sqrt{2}$ ist eine reelle Zahl. Die reellen Zahlen sind in diesem Sinn vollständig im Vergleich zu $\mathbb{Q}$.

Ist M nicht beschränkt, so schreibt man dafür $\sup M = \infty$. Analog:

Definition 2.15 $M \subseteq \mathbb{R}$ heißt **nach unten beschränkt**, falls es eine Zahl $k \in \mathbb{R}$ mit

$$x \geq k \text{ für alle } x \in M$$

gibt. Eine solche Zahl k wird dann als eine **untere Schranke** von M bezeichnet.

Die *größte* untere Schranke heißt das **Infimum** von M, kurz $\inf M$. Es ist ebenfalls eindeutig bestimmt (wir können $\inf M = -\sup(-M)$ mit $-M = \{-x | x \in M\}$ setzen). Ist M nicht nach unten beschränkt, so schreibt man symbolisch $\inf M = -\infty$. Wenn M sowohl nach unten als auch nach oben beschränkt ist, so nennt man M kurz **beschränkt**.

Nicht beschränkt heißt also (Regel von de Morgan), dass M nicht nach oben oder nicht nach unten beschränkt ist (einschließendes oder).

Beispiel 2.16 Beschränkte und unbeschränkte Mengen
Finden Sie (falls vorhanden) Beispiele für obere und untere Schranken, sowie das Supremum bzw. Infimum folgender Mengen: a) $(3,4)$ b) $\mathbb{N}$ c) $\mathbb{Z}$

Lösung zu 2.16

a) Für alle Zahlen aus dem offenen Intervall $(3,4)$ gilt: $x \geq 3$ (es gilt sogar $x > 3$, aber das ist für die Bestimmung des Infimum unwichtig). Daher ist 3 eine untere Schranke von $(3,4)$. Jede reelle Zahl, die kleiner als 3 ist, ist ebenfalls eine untere Schranke von $(3,4)$, z. B. -17. Von allen unteren Schranken ist 3 aber die *größte*, also $\inf(3,4) = 3$. Analog ist 4 die kleinste obere Schranke: $\sup(3,4) = 4$. Weitere obere Schranken sind alle reelle Zahlen, die größer als 4 sind, z. B. 291.

b) Für alle natürlichen Zahlen x gilt: $x \geq 1$. Daher ist 1 eine untere Schranke von $\mathbb{N}$. Jede reelle Zahl, die kleiner als 1 ist, z. B. $-\frac{1}{2}$, ist ebenfalls eine untere Schranke. Es gibt aber keine Zahl, die größer als 1 ist, und die gleichzeitig auch untere Schranke von $\mathbb{N}$ ist. Also ist 1 die *größte* untere Schranke von $\mathbb{N}$, d.h., $1 = \inf \mathbb{N}$. Nach oben sind die natürlichen Zahlen aber nicht beschränkt (denn es gibt keine größte natürliche Zahl). Das schreibt man in der Form: $\sup \mathbb{N} = \infty$.

c) Die ganzen Zahlen sind weder nach unten noch nach oben beschränkt: $\inf \mathbb{Z} = -\infty$, $\sup \mathbb{Z} = \infty$. ■

Beachten Sie, dass das Supremum von M nicht unbedingt auch Element von M sein muss (z. B. $\sup(3,4) = 4 \notin (3,4)$). Wenn jedoch das Supremum auch in M liegt, dann ist es gleichzeitig auch das **größte Element** von M. Man nennt das größte Element von M das **Maximum** von M, geschrieben $\max M$. Analog muss auch das Infimum von M nicht in M liegen. Falls aber das Infimum in M liegt, so ist es das **kleinste Element** von M, genannt **Minimum** von M, kurz geschrieben $\min M$.

Beispiel 2.17 Maximum und Minimum

a) Das offene Intervall $(3,4)$ ist beschränkt, besitzt aber kein Minimum, denn 3 liegt nicht im Intervall. Ebenso besitzt es kein Maximum.

b) Das abgeschlossene Intervall $[3,4]$ besitzt das kleinste Element 3, also $\inf[3,4] = \min[3,4] = 3$ und das größte Element 4, d.h. $\sup[3,4] = \max[3,4] = 4$.

c) Das Minimum von $\mathbb{N}$ ist 1, also $\min \mathbb{N} = 1$.

Definition 2.18 Die **Abrundungsfunktion** $\lfloor x \rfloor$ ordnet jeder reellen Zahl x die größte ganze Zahl, die kleiner oder gleich x ist, zu:

$$\lfloor x \rfloor = \max\{k \in \mathbb{Z} \mid k \leq x\}.$$

Analog ordnet die **Aufrundungsfunktion** $\lceil x \rceil$ jeder reellen Zahl x die kleinste ganze Zahl, die größer oder gleich x ist zu:

$$\lceil x \rceil = \min\{k \in \mathbb{Z} \mid k \geq x\}.$$

Die Abrundungsfunktion wird auch **Gaußklammer** genannt, nach dem deutschen Mathematiker Carl Friedrich Gauß (1777–1855). Die englischen Bezeichnungen für $\lfloor x \rfloor$ und $\lceil x \rceil$ sind **floor** („Boden“) bzw. **ceiling** („Zimmerdecke“). Es gilt übrigens $\lceil x \rceil = -\lfloor -x \rfloor$.

Beispiel 2.19 Es gilt $\lfloor 1.7 \rfloor = 1$, $\lceil 1.7 \rceil = 2$ und $\lfloor -1.7 \rfloor = -2$, $\lceil -1.7 \rceil = -1$.

Die komplexen Zahlen $\mathbb{C}$

Für unsere Zahlenmengen gilt bisher $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ und man könnte wirklich glauben, dass wir nun in der Lage sind, *jede* Gleichung zu lösen. Betrachten wir aber zum Beispiel die Gleichung $x^2 + 1 = 0$, so müssen wir wohl oder übel einsehen, dass es keine reelle Zahl gibt, deren Quadrat gleich -1 ist. Um diese Gleichung lösen zu können, müssen wir weitere Zahlen einführen:

Definition 2.20 Die Menge $\mathbb{C} = \{x + \mathrm{i} \cdot y \mid x, y \in \mathbb{R}\}$ heißt Menge der **komplexen Zahlen**. Die Zahl $\mathrm{i} \in \mathbb{C}$ wird **imaginäre Einheit** genannt. Sie ist definiert durch: $\mathrm{i}^2 = -1$. Man nennt x den **Realteil** beziehungsweise y den **Imaginärteil** der komplexen Zahl $x + \mathrm{i}\, y$ und schreibt

$$\mathrm{Re}(z) = x, \qquad \mathrm{Im}(z) = y.$$

Beispiel: $3 - 5\mathrm{i}$ ist die komplexe Zahl mit Realteil 3 und Imaginärteil -5. Achtung: Der Imaginärteil ist die reelle Zahl -5, und nicht $-5\mathrm{i}$!

In der Elektrotechnik wird die imaginäre Einheit mit j anstelle von i bezeichnet, denn das Symbol i ist dort bereits für den Strom vergeben.

Die reellen Zahlen erscheinen Ihnen vielleicht als technisches Ärgernis, mit dem man leben muss, weil die Wurzel aus 2 sich eben nicht als Bruch schreiben lässt. Wozu aber soll es gut sein, dass man für die Gleichung $x^2 + 1 = 0$ *formal* eine Lösung angeben kann?

Auch die Mathematik ist lange ohne komplexe Zahlen ausgekommen. Sie wurden zuerst nur in Zwischenrechnungen, bei denen sich am Ende alles Nicht-Reelle weggehoben hat, verwendet (z. B. zur Lösung von Gleichungen). Im Laufe der Zeit hat man aber erkannt, dass viele Berechnungen einfach und effizient werden, wenn man komplexe Zahlen verwendet (z. B. in der Elektrotechnik oder der Signalverarbeitung sind sie heute nicht mehr wegzudenken). Der französische Mathematiker Jacques Salomon Hadamard (1865–1963) hat sogar einmal gemeint: „Der kürzeste Weg zwischen zwei reellen Wahrheiten führt durch die komplexe Ebene.“

Ein Vergleich: In einer zweidimensionalen Welt lebend würden Sie wahrscheinlich jeden Mathematiker belächeln, der erzählt, dass Kreis und Rechteck eigentlich ein-und dasselbe Objekt darstellen; nur einmal von der Seite, und einmal von oben betrachtet. Wenn ich Sie dann aber in die dreidimensionale Welt hole und Ihnen einen Zylinder zeige, werden Sie wohl Ihre Meinung über die Mathematiker revidieren müssen. Ähnlich, wie ein Zylinder einen Kreis und ein Rechteck verknüpft, sind in der komplexen Welt die Exponentialfunktion und die trigonometrischen Funktionen verknüpft; eine Erkenntnis, die mit einem Schlag eine Vielzahl von praktischen Resultaten liefert!

Die reellen Zahlen sind gerade die komplexen Zahlen mit Imaginärteil 0. Somit gilt: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Die komplexen Zahlen können in einer Ebene veranschaulicht werden (Abbildung 2.2), der so genannten **Gauß'schen Zahlenebene**.

Eine komplexe Zahl $x + \mathrm{i}y$ kann also als Punkt in der Gauß'schen Zahlenebene betrachtet werden. In diesem Sinn kann $x + \mathrm{i}y$ auch als geordnetes Paar von reellen Zahlen (x, y) angegeben werden.

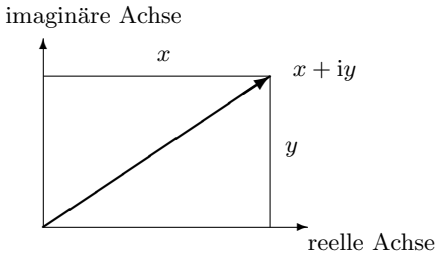


Abbildung 2.2. Gauß'sche Zahlenebene

Addition und Multiplikation von komplexen Zahlen folgen aus den entsprechenden Operationen für reelle Zahlen:

$$\begin{aligned}(x_1 + \mathrm{i}y_1) + (x_2 + \mathrm{i}y_2) &= (x_1 + x_2) + \mathrm{i}(y_1 + y_2)\\ (x_1 + \mathrm{i}y_1) \cdot (x_2 + \mathrm{i}y_2) &= (x_1x_2 - y_1y_2) + \mathrm{i}(x_1y_2 + y_1x_2)\\ \frac{1}{x + \mathrm{i}y} &= \frac{x}{x^2 + y^2} + \mathrm{i}\frac{-y}{x^2 + y^2}.\end{aligned}$$

Man kann mit komplexen Zahlen also wie mit reellen Zahlen rechnen. Die Zahl i wird dabei wie eine Variable behandelt, man muss nur berücksichtigen, dass $\mathrm{i}^2 = -1$ ist.

Aber Achtung: Im Gegensatz zu den reellen Zahlen können zwei komplexe Zahlen nicht ihrer Größe nach verglichen werden (d.h., nicht geordnet werden). Der Ausdruck $z_1 \leq z_2$ macht also für komplexe Zahlen z_1, z_2 keinen Sinn!

Für eine komplexe Zahl $z = x + \mathrm{i}y$ benötigt man oft ihre **konjugiert komplexe Zahl**

$$\overline{z} = x - \mathrm{i}y$$

(sie wird oft auch mit z^* bezeichnet). Real- und Imaginärteil lassen sich damit als

$$\mathrm{Re}(z) = \frac{z + \overline{z}}{2}, \qquad \mathrm{Im}(z) = \frac{z - \overline{z}}{2\mathrm{i}}$$

schreiben und es gelten folgende Rechenregeln:

$$\overline{(z_1 + z_2)} = \overline{z_1} + \overline{z_2}, \qquad \overline{(z_1 \cdot z_2)} = \overline{z_1} \cdot \overline{z_2} \qquad \overline{\left(\frac{1}{z}\right)} = \frac{1}{\overline{z}}.$$

Der **Absolutbetrag** einer komplexen Zahl ist

$$|z| = \sqrt{z\overline{z}} = \sqrt{x^2 + y^2}.$$

Für den Spezialfall, dass z reell ist, ergibt sich daraus der vorhin definierte Absolutbetrag für reelle Zahlen. Die **Dreiecksungleichung** gilt auch für komplexe Zahlen:

$$|z_1 + z_2| \leq |z_1| + |z_2|.$$

Nach dem Satz von Pythagoras entspricht $|z|$ der Länge des Pfeils, der z in der Gauß'schen Zahlenebene darstellt. Die komplexe Konjugation entspricht der Spiegelung des Pfeils an der reellen Achse.

Beispiel 2.21 (→CAS) Rechnen mit komplexen Zahlen
Berechnen Sie für die komplexen Zahlen $z_1 = 1 + 2\mathrm{i}$, $z_2 = 3 - \mathrm{i}$:
a) $z_1 + z_2$ b) $z_1 z_2$ c) $\overline{z_2}$ d) $|z_2|$ e) $\frac{z_1}{z_2}$

Lösung zu 2.21 Wir rechnen wie gewohnt und betrachten dabei i zunächst als Variable. Wann immer wir möchten, spätestens jedoch im Endergebnis, verwenden wir $\mathrm{i}^2 = -1$:
a) $z_1 + z_2 = 1 + 2\mathrm{i} + 3 - \mathrm{i} = 4 + \mathrm{i}$.
b) $z_1 z_2 = 3 - \mathrm{i} + 6\mathrm{i} - 2\mathrm{i}^2 = 3 + 5\mathrm{i} - 2 \cdot (-1) = 5 + 5\mathrm{i}$.
c) $\overline{z_2} = 3 + i$, es dreht sich also das Vorzeichen des Imaginärteils um.
d) $|z_2| = \sqrt{(3 - i)(3 + i)} = \sqrt{3^2 + 1^2} = \sqrt{10}$.
e) Wir multiplizieren Zähler und Nenner mit der konjugiert komplexen Zahl von $3 - \mathrm{i}$. Durch diesen „Trick“ wird der Nenner eine reelle Zahl:

$$\frac{1 + 2\mathrm{i}}{3 - \mathrm{i}} = \frac{(1 + 2\mathrm{i})(3 + \mathrm{i})}{(3 - \mathrm{i})(3 + \mathrm{i})} = \frac{1 + 7\mathrm{i}}{10} = \frac{1}{10} + \frac{7}{10}\mathrm{i}.$$

■

Ganzzahlige Potenzen sind analog wie für reelle Zahlen definiert und erfüllen auch die gleichen Rechenregeln. Bei gebrochenen Potenzen (z. B. Wurzelziehen) muss man aber vorsichtig sein: Wurzeln lassen sich zwar analog definieren, aber die gewohnten Rechenregeln stimmen nicht mehr! Mit $\sqrt{-1} = \mathrm{i}$ folgt zum Beispiel

$$1 = \sqrt{1} = \sqrt{(-1)(-1)} \neq \sqrt{-1}\sqrt{-1} = \mathrm{i} \cdot \mathrm{i} = -1.$$

Mehr dazu, und insbesondere wie man komplexe Wurzeln berechnet, werden Sie im Abschnitt „Polardarstellung komplexer Zahlen“ in Band 2 erfahren.

2.2 Summen und Produkte

Definition 2.22 Für die Summe von reellen (oder komplexen) Zahlen $a_0, \ldots, a_n$ schreibt man abkürzend

$$\sum_{k=0}^{n} a_k = a_0 + \ldots + a_n, \quad \text{gelesen „Summe über alle } a_k \text{ für } k \text{ gleich 0 bis } n\text{“}.$$

Das Summenzeichen $\sum$ ist das griechische Symbol für „S“ (großes Sigma).

Die einzelnen Summanden ergeben sich dadurch, dass der „Laufindex“ k alle ganzen Zahlen von 0 bis zu einer bestimmten Zahl n durchläuft. Anstelle von k kann jeder beliebige Buchstabe für den Laufindex verwendet werden. Der Laufindex muss auch nicht bei 0, sondern kann bei jeder beliebigen ganzen Zahl beginnen.

Beispiel 2.23 Summenzeichen
Berechnen Sie:
a) $\sum_{k=1}^{4} k^2$ b) $\sum_{k=0}^{4}(-1)^k 2^k$ c) $\sum_{m=1}^{5}(-1)^{m+1}(2m)$

Schreiben Sie mithilfe des Summenzeichens:
d) $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots+\frac{1}{20}$ e) $1-3+5-7+9-11$ f) $1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}$

Lösung zu 2.23
a) Wir erhalten alle Summanden, indem wir für k nacheinander $1, 2, 3$ und 4 einsetzen: $\sum_{k=1}^{4} k^2 = 1^2+2^2+3^2+4^2 = 30$.
b) Der Faktor $(-1)^k$ bewirkt hier, dass das Vorzeichen der Summanden abwechselt: $\sum_{k=0}^{4}(-1)^k 2^k = (-1)^0\cdot 2^0+(-1)^1\cdot 2^1+(-1)^2\cdot 2^2+(-1)^3\cdot 2^3+(-1)^4\cdot 2^4 = 2^0-2^1+2^2-2^3+2^4 = 11$.
c) Hier haben wir den Laufindex zur Abwechslung mit m bezeichnet: $\sum_{m=1}^{5}(-1)^{m+1}(2m) = (-1)^2\cdot(2\cdot 1)+(-1)^3\cdot(2\cdot 2)+\ldots+(-1)^6\cdot(2\cdot 5) = 2-4+6-8+10 = 6$. Der Term $2m$ hat uns lauter gerade Zahlen erzeugt.
d) Der k-te Summand kann als $\frac{1}{k}$ geschrieben werden. Für den ersten Summanden muss $k=1$ sein, für den letzten muss $k=20$ sein. Daher läuft k von 1 bis 20: $\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots+\frac{1}{20} = \sum_{k=1}^{20}\frac{1}{k}$.
e) Hier ist der k-te Summand immer eine ungerade Zahl, die wir mit $2k+1$ erzeugen können. Der Index k muss von 0 bis 5 laufen, damit der erste Summand 1 und der letzte Summand 11 ist: $1-3+5-7+9-11 = (-1)^0\cdot(2\cdot 0+1)+(-1)^1\cdot(2\cdot 1+1)+\ldots+(-1)^5\cdot(2\cdot 5+1) = \sum_{k=0}^{5}(-1)^k(2k+1)$.
f) Der k-te Summand ist $\frac{1}{2^k}$ und k muss von 0 bis 4 laufen: $1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16} = \frac{1}{2^0}+\frac{1}{2^1}+\frac{1}{2^2}+\frac{1}{2^3}+\frac{1}{2^4} = \sum_{k=0}^{4}\frac{1}{2^k}$. ■

Aus den Rechenregeln für reelle Zahlen folgt, dass man Summen gliedweise addieren und konstante Faktoren herausheben kann:

Satz 2.24 (Rechenregeln für Summen) Für $n\in\mathbb{N}$, reelle oder komplexe Zahlen $a_0,\ldots,a_n,b_0,\ldots,b_n$ und c gilt:

$$\begin{aligned}\sum_{k=0}^{n}(a_k+b_k) &= \sum_{k=0}^{n}a_k+\sum_{k=0}^{n}b_k,\\ \sum_{k=0}^{n}c\,a_k &= c\sum_{k=0}^{n}a_k.\end{aligned}$$

Beispiel 2.25 Rechenregeln für Summen
a) Hier kann die Summe „auseinander gezogen“ und leichter berechnet werden, weil wir auf das Ergebnis von Beispiel 2.23 a) zurückgreifen können:

$$\sum_{k=1}^{4}(k^2+k) = \sum_{k=1}^{4}k^2+\sum_{k=1}^{4}k = 30+(1+2+3+4) = 40.$$

b) Hier kann 3 vor die Summe gezogen werden und damit wieder mithilfe unserer Vorarbeit in Beispiel 2.23 a)

$$\sum_{k=0}^{4} 3k^2 = 3\sum_{k=0}^{4} k^2 = 3 \cdot 30 = 90$$

berechnet werden.

Summenzeichen können auch verschachtelt werden:

$$\begin{aligned}\sum_{j=1}^{3}\sum_{k=1}^{j}(-1)^j 2^k &= \sum_{k=1}^{1}(-1)^1 2^k + \sum_{k=1}^{2}(-1)^2 2^k + \sum_{k=1}^{3}(-1)^3 2^k = \\ &= (-2) + (2+4) + (-2-4-8) = -10.\end{aligned}$$

Hier wurde einfach schrittweise aufgelöst. Zuerst wurde die äußere Summe ausgeschrieben, wodurch drei Summanden (für $j = 1, 2, 3$) entstanden. Dann wurde noch das Summenzeichen jedes Summanden aufgelöst, indem für k eingesetzt wurde. Sind die Grenzen der Indizes konstant, so ist sogar die Reihenfolge, in der die Summen ausgewertet werden, egal:

Satz 2.26 (Vertauschung von Summen) Für $m, n \in \mathbb{N}$, und reelle oder komplexe Zahlen $a_{00}, \ldots, a_{mn}$ gilt:

$$\sum_{j=0}^{m}\sum_{k=0}^{n} a_{jk} = \sum_{k=0}^{n}\sum_{j=0}^{m} a_{jk}$$

Auch für Produkte von reellen (oder komplexen) Zahlen $a_0, \ldots, a_n$ gibt es eine abkürzende Schreibweise:

$$\prod_{k=0}^{n} a_k = a_0 \cdot a_1 \cdots a_n, \quad \text{gelesen „Produkt über alle } a_k \text{ für } k \text{ gleich 0 bis } n\text{“}$$

Das Produktzeichen $\prod$ ist das griechische Symbol für „P“ (großes Pi).

Das Produkt der ersten n natürlichen Zahlen wird als **Fakultät** bezeichnet

$$n! = \prod_{k=1}^{n} k = 1 \cdot 2 \cdots n.$$

Beispiel: $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$. Man vereinbart $0! = 1$. Im Gegensatz zur Summe über die ersten n natürlichen Zahlen, kann für dieses Produkt keine einfachere Formel mehr angegeben werden.

2.3 Vollständige Induktion

Es ist oft schwer, eine Summe mit variablen Grenzen zu berechnen. Zum Beispiel: Was ist die Summe der ersten n natürlichen Zahlen,

$$1 + 2 + 3 + \ldots + n = ?$$

Gibt es dafür eine einfache Formel? Manchmal ist es möglich, eine solche Formel zu *erraten*. Ich behaupte jetzt einfach, dass $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$. Wie überzeuge ich Sie (und mich) davon? Wir könnten als Erstes einmal überprüfen, ob die Formel für kleine Zahlen, z. B. $n = 1$ oder $n = 2$ stimmt. Für $n = 1$ erhalten wir $1 = \frac{1 \cdot 2}{2}$, da stimmt die Formel also. Für $n = 2$ erhalten wir $1 + 2 = \frac{2 \cdot 3}{2}$, stimmt also auch. Auf diese Weise können wir die Formel für weitere Werte von n überprüfen, nie werden wir aber so die *Gewissheit* haben, dass sie für *jedes* n stimmt. Der Ausweg aus unserem Dilemma ist das **Induktionsprinzip**, mit dem man eine solche Formel für *alle* n nachweisen kann.

Satz 2.27 (Induktionsprinzip oder Vollständige Induktion) Sei $A(n)$ eine Aussage für beliebiges $n \in \mathbb{N}$, sodass gilt:

- Induktionsanfang: $A(1)$ ist richtig (Induktionsanfang)
  und
- Induktionsschluss: Aus der Richtigkeit von $A(n)$ für ein beliebiges, festes $n \in \mathbb{N}$ („Induktionsvoraussetzung“) folgt die Richtigkeit von $A(n + 1)$. (Anstelle der Richtigkeit von $A(n)$ kann sogar die Richtigkeit von $A(k)$ für alle $k \leq n$ vorausgesetzt werden.)

Dann ist $A(n)$ für alle $n \in \mathbb{N}$ richtig.

Das Induktionsprinzip ist wie der Dominoeffekt. Sie möchten, dass alle Steine umfallen (dass die Aussage für alle n bewiesen wird). Dazu müssen Sie den ersten Stein anstoßen (Induktionsanfang) und es muss sichergestellt sein, dass ein beliebiger Stein den darauf folgenden umwirft (Schluss von n auf $n + 1$).

Die Induktion muss nicht bei 1 beginnen, sondern kann auch angewendet werden, wenn eine Aussage für alle ganzen Zahlen ab einer bestimmten Zahl $n_0 \in \mathbb{Z}$ (z. B. $n_0 = 0$ oder $n_0 = 2$) formuliert wird.

Beispiel 2.28 (→CAS) Induktionsprinzip
Zeigen Sie, dass die Formel

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$$

für alle $n \in \mathbb{N}$ gültig ist.

Lösung zu 2.28

- Induktionsanfang: Die kleinste Zahl, für die die Formel gelten soll, ist 1. Betrachten wir daher die Formel für $n = 1$: $1 = \frac{1 \cdot 2}{2}$ ist richtig.
- Induktionsschluss: Wir setzen voraus, dass wir ein $n \in \mathbb{N}$ gefunden haben, für das die Formel gilt:

  $$1 + 2 + \ldots + n = \frac{n(n+1)}{2} \qquad \text{Induktionsvoraussetzung (IV).}$$

  Nun müssen wir zeigen, dass sie unter dieser Voraussetzung auch für die nächste natürliche Zahl $n + 1$ gilt, dass also auch

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

Dazu verwenden wir unsere Induktionsvoraussetzung und formen dann noch etwas um:

$$\underbrace{1+2+3+\ldots+n}_{=\frac{n(n+1)}{2}\text{ nach IV}}+(n+1)=\frac{n(n+1)}{2}+(n+1)=\frac{(n+2)(n+1)}{2}.$$

Wir haben also gezeigt, dass aus der Richtigkeit von $1+2+\ldots+n=\frac{n(n+1)}{2}$ für ein beliebiges, festes n auch die Richtigkeit von $1+2+\ldots+n+(n+1)=\frac{(n+1)(n+2)}{2}$ folgt. Nach dem Induktionsprinzip ist damit die Formel für *alle* natürlichen Zahlen richtig. ■

Der Mathematiker Carl Friedrich Gauß bekam in der Volksschule die Aufgabe, die ersten hundert natürlichen Zahlen zu addieren. Sein Lehrer hoffte, er könnte die Klasse damit eine Zeit beschäftigen. Leider hat das nicht funktioniert, denn der kleine Gauß war nach kürzester Zeit fertig. Er hatte erkannt, dass die größte und die kleinste Zahl addiert $1+100=101$ ergibt, genauso wie die zweite und die zweitletzte Zahl $2+99=101$, und so weiter. Die Summe kann also aus 50 Summanden der Größe 101 gebildet werden und das Ergebnis ist somit 5050.

Zuletzt noch ein Beispiel zur Anwendung von Satz 2.24:

Beispiel 2.29 Rechenregeln für Summen
Berechnen Sie die Summe der ersten n ungeraden natürlichen Zahlen.

Lösung zu 2.29 Wir suchen eine Formel für $1+3+\cdots+2n-1$, oder kompakt angeschrieben:

$$\sum_{j=1}^{n}(2j-1)=?$$

Wir könnten diese Formel leicht direkt mithilfe von Induktion beweisen, aber mit den Rechenregeln für Summen aus Satz 2.24 und unter Verwendung der Formel, die wir im Beispiel 2.28 bereits bewiesen haben, erhalten wir das Ergebnis schneller:

$$\sum_{j=1}^{n}(2j-1)=2\sum_{j=1}^{n}j-\sum_{j=1}^{n}1=2\frac{n(n+1)}{2}-n=n^2.$$

■

2.4 Stellenwertsysteme

Gewöhnlich schreiben wir Zahlen mithilfe der zehn Ziffern $0,...,9$. Mit der Schreibweise 26.73 meinen wir zum Beispiel die folgende Summe:

$$26.73=2\cdot 10^1+6\cdot 10^0+7\cdot 10^{-1}+3\cdot 10^{-2}.$$

Die Schreibweise 26.73 ist also nichts anderes als eine abgekürzte Schreibweise für eine Summe von Potenzen von 10.

Definition 2.30 Wir nennen eine Zahl in der Darstellung

$$a_n \cdots a_0.a_{-1} \cdots a_{-m} = \sum_{j=-m}^{n} a_j 10^j, \qquad a_j \in \{0, 1, 2, \ldots, 9\}$$

eine **Dezimalzahl**.

(Achtung: Zwischen a_0 und a_{-1} steht der Dezimalpunkt!) Die Stelle einer Ziffer innerhalb der Zahl gibt an, mit welcher Potenz von 10 sie zu multiplizieren ist („Einerstelle“, „Zehnerstelle“, „Nachkommastellen“, ...). Man nennt ein derartiges System allgemein auch **Stellenwertsystem**.

Im Gegensatz dazu haben die Römer für bestimmte natürliche Zahlen Symbole (I, V, X, L, C, ...) benutzt, die – unabhängig von ihrer Lage innerhalb einer Zahlendarstellung – immer denselben Wert haben. Wie man sich vorstellen kann, war das Rechnen in diesem System aber ziemlich schwierig. (Böse Zungen behaupten sogar, das sei der Grund für den Untergang des römischen Weltreichs gewesen.)

Rationale Zahlen sind genau jene Zahlen, die entweder **endlich viele** oder **unendlich viele periodische** Nachkommastellen haben.

Das können wir uns leicht veranschaulichen:
• $\frac{7}{4} = 7 : 4 = 1.75$. Die Division bricht ab, weil der Rest 0 wird. Umgekehrt können wir leicht 1.75 als Bruch darstellen: $1.75 = \frac{175}{100} = \frac{7}{4}$.
• $\frac{5}{27} = 5 : 27 = 0.185185185\ldots = 0.\overline{185}$. Die Division bricht nie ab. Die Reste müssen sich aber irgendwann wiederholen, weil ein Rest immer kleiner als der Nenner ist und es somit nur endlich viele Möglichkeiten dafür gibt. Es entsteht eine **periodische** Zahl. Hier lässt sich umgekehrt die Bruchdarstellung von $0.\overline{185}$ nicht so ohne weiteres durch Hinsehen finden.

Beispiel 2.31 Rationale Zahlen als Kommazahlen geschrieben
a) $\frac{7}{4} = 1.75$ b) $\frac{4}{30} = 0.133333\ldots = 0.1\overline{3}$ c) $\frac{2}{11} = 0.18181\ldots = 0.\overline{18}$
d) $\frac{3}{9} = \frac{1}{3} = 0.\overline{3}$ e) $\frac{4}{9} = 0.\overline{4}$ f) $1 = \frac{9}{9} = 0.\overline{9}$

Irrationale Zahlen, also Zahlen, die nicht als Bruch geschrieben werden können, haben immer **unendlich viele nicht-periodische** Nachkommastellen.

Beispiel 2.32 Irrationale Zahlen als Kommazahlen geschrieben
a) $\pi = 3.141592653\ldots$ b) $\sqrt{2} = 1.4142135623\ldots$

Wir hätten also die reellen Zahlen auch als die Menge aller Dezimalzahlen mit endlich vielen oder unendlich vielen Nachkommastellen einführen können.

Dabei ist zu beachten, dass eine Zahl verschiedene Darstellungen haben kann, z. B. $1 = 0.\overline{9}$.

Die Approximation einer irrationalen Zahl durch eine rationale Zahl erhält man, indem man die unendlich vielen Nachkommastellen der irrationalen Zahl – je nach gewünschter Genauigkeit – an irgendeiner Stelle abbricht. So genügt es etwa für viele Anwendungen, für π die rationale Zahl 3.14 zu verwenden.

Kommen wir nun zurück zum Begriff des Stellenwertsystems. Die Basis „10“ hat sich vor allem für das alltägliche Rechnen als sehr praktisch erwiesen (nicht zuletzt deshalb, weil der Mensch zehn Finger hat). Es ist aber natürlich möglich, eine beliebige andere natürliche Zahl b als Basis zu wählen und Zahlen in der Form

$$\sum_{j=-m}^{n} a_j b^j, \qquad a_j \in \{0, 1, 2, \ldots, b-1\}$$

darzustellen. Insbesondere ist für Computer, die nur *zwei* Finger besitzen („Spannung“ und „keine Spannung“), das System mit Basis 2 vorteilhafter. Dieses System wird **Dualsystem** (auch **Binärsystem**) genannt und Zahlen, die im Dualsystem dargestellt werden, heißen **Dualzahlen** (oder **Binärzahlen**). Sie enthalten nur zwei Ziffern 0 und 1, die den beiden Zuständen entsprechen.

Wussten Sie übrigens, dass man die Menschen in 10 Gruppen einteilen kann: in jene, die Dualzahlen kennen und jene, die sie nicht kennen;-)

Beispiel 2.33 Dualzahlen
a) Stellen Sie die Dualzahl 1101 im Dezimalsystem dar.
b) Stellen Sie die Dezimalzahl 36.75 im Dualsystem dar.

Lösung zu 2.33
a) $(1101)_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = (13)_{10}$.
Wenn nicht klar ist, in welchem Zahlensystem eine Ziffernfolge zu verstehen ist, dann kann man, so wie hier, einen tiefergestellten Index verwenden.
b) $(36.75)_{10} = 32 + 4 + 0.5 + 0.25 = 2^5 + 2^2 + 2^{-1} + 2^{-2} = (100100.11)_2$.
Das Komma kennzeichnet in jedem Stellenwertsystem den Beginn der negativen Potenzen. ■

In der Datenverarbeitung sind neben dem Dualsystem auch das **Oktalsystem** und das **Hexadezimalsystem** gebräuchlich. Im Oktalsystem wird 8 als Basis verwendet, im Hexadezimalsystem wird 16 verwendet. Da das Hexadezimalsystem auf einem Vorrat von 16 Ziffern aufbaut, muss man zu den zehn Ziffern $0, \ldots, 9$ noch sechs weitere Ziffern hinzufügen. Üblicherweise werden dazu die Buchstaben A, B, C, D, E, F verwendet, die den Dezimalzahlen $10, \ldots, 15$ entsprechen. Die Bedeutung dieser beiden Systeme in der Datenverarbeitung liegt vor allem darin, dass man mit ihrer Hilfe Dualzahlen übersichtlicher schreiben kann. Denn eine Ziffer im Hexadezimalsystem bzw. Oktalsystem entspricht genau einem Block aus vier bzw. drei Ziffern im Dualsystem.

Beispiel 2.34 (→CAS) Oktalzahlen, Hexadezimalzahlen
a) Stellen Sie die Hexadezimalzahl $(FAD)_{16}$ im Dezimalsystem dar.
b) Stellen Sie die Hexadezimalzahl $(FAD)_{16}$ im Dualsystem dar.
c) Stellen Sie die Oktalzahl $(67)_8$ im Dezimalsystem dar.

Lösung zu 2.34
a) $(FAD)_{16} = 15 \cdot 16^2 + 10 \cdot 16^1 + 13 \cdot 16^0 = (4013)_{10}$.
b) Hier können wir verwenden, dass jede Ziffer im Hexadezimalsystem einem Block aus vier Ziffern im Dualsystem entspricht: $(F)_{16} = (1111)_2$, $(A)_{16} = (1010)_2$, $(D)_{16} = (1101)_2$. Die gesuchte Dualdarstellung erhalten wir nun durch Aneinanderreihung dieser Blöcke: $(FAD)_{16} = (111110101101)_2$.
c) $(67)_8 = 6 \cdot 8^1 + 7 \cdot 8^0 = (55)_{10}$. ■

Die Umwandlung vom Dezimalsystem in ein anderes Zahlensystem von Hand funktioniert am schnellsten, wenn man beachtet, dass Division durch die Basis das Komma um eine Stelle nach links und Multiplikation mit der Basis das Komma um eine Stelle nach rechts verschiebt.

Im Zehnersystem überlegt: Wird die Dezimalzahl 234.0 durch 10 dividiert, so verschiebt sich die Einerstelle 4 hinter das Komma: 23.4. Der Rest bei Division durch 10 ist also gerade die Einerstelle (im Dezimalsystem) der Zahl 234. Wenn wir die Kommastelle von 23.4 weglassen, und 23.0 nochmals durch 10 dividieren, so erhalten wir als Rest die Zehnerstelle von 234 usw.

Analog funktioniert es, wenn wir die Nachkommastellen von 0.51 erhalten möchten: Wir multiplizieren mit 10 und erhalten 5.1. Der Überlauf 5 links vom Komma ist gerade der Koeffizient von 10^{-1}, usw.

Am besten gleich ein Beispiel dazu:

Beispiel 2.35 Umwandlung einer Dezimalzahl ins Dualsystem

a) Stellen Sie die Dezimalzahl 237 im Dualsystem dar.
b) Stellen Sie die Dezimalzahl 0.1 im Dualsystem dar.
c) Stellen Sie die Dezimalzahl 237.1 im Dualsystem dar.

Lösung zu 2.35

a) Wir dividieren sukzessive durch 2 und notieren die Reste: $237 : 2 = 118$, Rest 1 (das ist der Koeffizient a_0 von 2^0); $118 : 2 = 59$, Rest 0 (das ist a_1); $59 : 2 = 29$, Rest 1; $29 : 2 = 14$, Rest 1; $14 : 2 = 7$, Rest 0; $7 : 2 = 3$, Rest 1; $3 : 2 = 1$, Rest 1; $1 : 2 = 0$, Rest 1. Damit lautet die gesuchte Dualdarstellung (alle Reste angeschrieben):
$$(237)_{10} = (11101101)_2.$$
b) Wir multiplizieren sukzessive mit 2 und notieren die Überläufe: $0.1 \cdot 2 = 0.2$, Überlauf 0 (das ist der Koeffizient a_{-1} von 2^{-1}); $0.2 \cdot 2 = 0.4$, Überlauf 0 (das ist der Koeffizient a_{-2} von 2^{-2}); $0.4 \cdot 2 = 0.8$, Überlauf 0; $0.8 \cdot 2 = 1.6$, Überlauf 1; $0.6 \cdot 2 = 1.2$, Überlauf 1; $0.2 \cdot 2 = 0.4$, Überlauf 0. Da 0.4 bereits aufgetreten ist, wiederholen sich ab nun die Überläufe periodisch. Die gesuchte Dualdarstellung ist daher (alle Überläufe angeschrieben):
$$(0.1)_{10} = (0.0\overline{0011})_2,$$
und $(0.1)_{10}$ ist somit im Dualsystem eine Zahl mit unendlich vielen periodischen Nachkommastellen!
c) Mithilfe von a) und b) kein Problem: $(237.1)_{10} = (11101101.0\overline{0011})_2$. ■

Es kann also – wie wir in Beispiel 2.35 b) sehen – vorkommen, dass eine rationale Zahl in einem Zahlensystem nur *endlich* viele, in einem anderen System aber *unendlich viele periodische* Nachkommastellen hat. Niemals aber wird eine rationale Zahl in einem System unendlich viele *nicht-periodische* Nachkommastellen haben.

2.5 Maschinenzahlen

Ein Computer hat nur eine endliche Speicherkapazität und kann daher nur endlich viele Stellen einer Zahl abspeichern. Jene Zahlen, die ein Rechner noch exakt darstellen kann, heißen **Maschinenzahlen**. Maschinenzahlen bilden also eine endliche

Teilmenge der Menge der rationalen Zahlen. Alle anderen reellen Zahlen werden vom Computer immer auf die nächstgelegene Maschinenzahl gerundet.

Im einfachsten Fall verwendet man eine feste Anzahl von Stellen vor und nach dem Komma (**Festkommadarstellung** oder **Festpunktdarstellung**). Dabei kann aber nur ein relativ enger Zahlenbereich abgedeckt werden. Um einen möglichst weiten Zahlenbereich abzudecken, werden Zahlen im Computer daher in der so genannten *Gleitkommadarstellung* gespeichert:

Definition 2.36 Die **Gleitkommadarstellung** (**Gleitpunktdarstellung**) hat die Form

$$M \cdot b^E, \qquad \text{mit } |M| < 1, E \in \mathbb{Z}.$$

Dabei ist b die Basis des Stellenwertsystems, die Kommazahl M heißt **Mantisse** und die ganze Zahl E wird **Exponent** genannt.

Im Computer wird die Basis $b = 2$ verwendet. M und E werden im zugrunde liegenden Stellenwertsystem mit Basis b dargestellt. Dabei ist für sie eine feste Anzahl von t bzw. s Stellen festgelegt:

$$M = \pm 0.m_1 m_2 \dots m_t = \pm \sum_{j=1}^{t} m_j b^{-j}, \qquad E = \pm e_{s-1} \dots e_1 e_0 = \pm \sum_{j=0}^{s-1} e_j b^j.$$

Die Gleitkommadarstellung einer Zahl ist aber so weit noch nicht eindeutig, da zum Beispiel (im Dezimalsystem) 0.1 als $0.1 \cdot 10^0$, $0.01 \cdot 10^1$, ... dargestellt werden kann. Um eine *eindeutige* Darstellung zu erhalten wird bei der **normalisierten Gleitkommadarstellung** der Exponent so gewählt, dass die erste Stelle der Mantisse ungleich 0 ist. Der kleinste Wert für die Mantisse ist daher b^{-1}:

$$b^{-1} \leq |M| < 1.$$

Insbesondere kann die Zahl Null nicht in normalisierter Gleitkommadarstellung dargestellt werden und erhält eine Sonderstellung.
Beispiel: 346.17 wird in der Form $0.34617 \cdot 10^3$ abgespeichert. Die Mantisse ist dabei 0.34617 (Länge 5) und der Exponent ist 3.

Versuchen wir uns den Unterschied zwischen Gleit- und Festkommadarstellung anhand eines kleinen Beispiels zu veranschaulichen. Damit es für uns leichter wird, stellen wir uns vor, dass der Computer Zahlen im Dezimalsystem darstellt. Unsere Überlegung gilt aber gleichermaßen für das Dualsystem bzw. für jedes beliebige Stellenwertsystem. Nehmen wir weiters an, dass es sich um einen sehr einfachen Computer mit Mantissenlänge 1 und Exponentenlänge 1 handelt. Dann sind die positiven darstellbaren Zahlen gegeben durch

$$0.1 \cdot 10^{-9},\ 0.2 \cdot 10^{-9}, \dots, 0.9 \cdot 10^{-9},\ 0.1 \cdot 10^{-8},\ 0.2 \cdot 10^{-8}, \dots, 0.9 \cdot 10^{9}.$$

Die Maschinenzahlen dieses Computers können also in Gleitkommadarstellung den positiven Zahlenbereich von 0.0000000001 bis 900000000 abdecken. Dazu kommen noch ebenso viele negative Zahlen und die 0. Bei einer Festkommadarstellung mit je einer Zahl vor und nach dem Komma könnte nur der positive Zahlenbereich von 0.1 bis 9.9 abgedeckt werden (d.h. gleich viele Zahlen wie in Gleitkommadarstellung, aber auf einem engeren Zahlenbereich konzentriert). Der Preis, den man für den weiteren Zahlenbereich in Gleitkommadarstellung zahlt, ist, dass die Maschinenzahlen in Gleitkommadarstellung nicht gleichmäßig verteilt sind: Zwischen 1 und 10 liegen z. B. genauso

viele Maschinenzahlen (1, 2, 3, ..., 10) wie zwischen 10 und 100 (10, 20, 30, ..., 100), nämlich genau zehn.

Bei der Verarbeitung von Kommazahlen durch den Computer müssen immer wieder Zahlen auf die nächstgelegene Maschinenzahl gerundet werden. Und zwar passiert das nicht nur nach der Eingabe (aufgrund der Umwandlung vom Dezimal- ins Dualsystem), sondern auch nach jeder Rechenoperation, da die Summe bzw. das Produkt von zwei Maschinenzahlen im Allgemeinen nicht wieder eine Maschinenzahl ist.

Wie groß ist dieser **Rundungsfehler** maximal? Ist $x = M\,b^E$ der exakte und $\tilde{x} = \tilde{M}\,b^E$ der zugehörige gerundete Wert, so ist der **absolute Fehler** gleich

$$|\text{gerundeter Wert} - \text{exakter Wert}| = |\tilde{x} - x| = |\tilde{M} - M| b^E.$$

Definition 2.37 Der **relative Fehler** ist gegeben durch

$$\left|\frac{\text{absoluter Fehler}}{\text{exakter Wert}}\right| = \left|\frac{\tilde{x} - x}{x}\right| = \left|\frac{\tilde{M}\,b^E - M\,b^E}{M\,b^E}\right| = \left|\frac{\tilde{M} - M}{M}\right|.$$

Den relativen Fehler möchten wir nun abschätzen: Wenn die Mantisse t Stellen hat, so wird beim Runden die t-te Stelle um höchstens $\frac{1}{2}b^{-t}$ auf- oder abgerundet.

Beispiel aus dem Dezimalsystem mit 3-stelliger Mantisse: Die exakten Werte 0.4275, 0.4276, 0.4277, 0.4278 und 0.4279 werden auf 0.428 aufgerundet; die exakten Werte 0.4271, 0.4272, 0.4273 und 0.4274 werden auf 0.427 abgerundet; die Mantisse wird also um höchstens $0.0005 = \frac{1}{2}10^{-3}$ gerundet.

Das Ergebnis beim Runden hängt vom verwendeten Zahlensystem und der Konvention beim Runden ab. Beim **kaufmännischen Runden** wird z. B. eine letzte Ziffer 5 immer aufgerundet (*round to larger*). Das bedeutet aber, dass ein systematischer Fehler entsteht, der sich im statistischen Mittel nicht weghebt. Deshalb wird in Computern im Grenzfall so gerundet, dass die letzte Stelle gerade ist (*round to even*). Im Dualsystem ist das noch wichtiger, denn während das Rundungsproblem im Dezimalsystem nur in 10% aller Fälle eintritt (der Grenzfall 5 ist eine von zehn möglichen Ziffern), muss im Dualsystem in 50% der Fälle (der Grenzfall 1 ist eine von zwei möglichen Ziffern) gerundet werden.

Das heißt, $\tilde{M}$ und M unterscheiden sich um höchstens $\frac{1}{2}b^{-t}$: $|\tilde{M} - M| \leq \frac{1}{2}b^{-t}$. Da in der normalisierten Gleitkommadarstellung weiters $b^{-1} \leq |M| < 1$ gilt, folgt $\frac{1}{|M|} \leq b$. Also erhalten wir insgesamt

$$\left|\frac{\tilde{M} - M}{M}\right| \leq \frac{1}{2}b^{-t} \cdot b = \frac{1}{2}b^{1-t}.$$

Damit folgt:

Satz 2.38 Beim Rechnen in Gleitkommadarstellung gilt für den relativen Rundungsfehler:

$$\left|\frac{\tilde{x} - x}{x}\right| \leq \frac{1}{2}b^{1-t} \qquad (|x| \geq b^{-b^s}).$$

Der maximale Wert $\varepsilon = \frac{1}{2}b^{1-t}$ für den relativen Fehler wird als **Maschinengenauigkeit** bezeichnet.

Damit kann also der relative Fehler beim Runden abgeschätzt werden. Was passiert aber, wenn das Ergebnis einer Rechnung zu groß wird, oder zu nahe bei 0 liegt? Wenn also $E \geq b^s$ oder $E \leq -b^s$ wird? Ein Exponentenüberlauf (zu großes Ergebnis) wird in der Regel als Fehler gemeldet. Bei einem *Exponentenunterlauf* wird das Ergebnis gleich null gesetzt, $\tilde{x} = 0$. Im letzteren Fall ist der relative Fehler 1 und somit größer als die Maschinengenauigkeit.

In den meisten Fällen sind Rundungsfehler klein und können vernachlässigt werden. Auch wenn eine Zahl viele Rechenoperationen durchläuft und das Ergebnis immer wieder gerundet wird, haben Rundungsfehler die Tendenz sich nicht aufzusummieren, sondern sich wegzumitteln (es ist eben unwahrscheinlich, dass bei zehn Operationen jedes Mal auf- und nie abgerundet wird).

Beispiel 2.39 Rundungsfehler
Gehen wir einfachheitshalber von einem Computer aus, der Zahlen im Dezimalsystem darstellt und der eine 4-stellige Mantisse hat. Wie groß ist die Maschinengenauigkeit? Welches Ergebnis gibt der Computer für $1.492 \cdot 1.066$ aus? Wie groß ist der relative Fehler?

Lösung zu 2.39 Wegen $t = 4$ ist die Maschinengenauigkeit gleich $\varepsilon = \frac{1}{2}10^{1-4} = 0.0005 = 0.05\%$. D.h., die Abweichung (der absolute Fehler) vom exakten Wert beträgt maximal 0.05% vom exakten Wert. Konkret wäre für unsere Rechenoperation das exakte Ergebnis gleich $1.492 \cdot 1.066 = 1.590472$. Aufgrund der 4-stelligen Mantisse muss der Computer runden und gibt daher den Wert $0.1590 \cdot 10^1 = 1.590$ aus. Der relative Fehler beträgt hier

$$\left|\frac{\text{absoluter Fehler}}{\text{exakter Wert}}\right| = \left|\frac{1.590 - 1.590472}{1.590472}\right| \approx 0.0003,$$

also 0.03%. ■

Allein durch die im Computer nötige Umwandlung vom Dezimal- ins Dualsystem können bereits Rundungsfehler auftreten. Beispiel 2.35 hat uns ja gezeigt, dass bei Umwandlung von $(0.1)_{10}$ ins Dualsystem eine Zahl mit unendlich vielen Nachkommastellen entsteht. Diese Nachkommastellen müssen vom Computer abgebrochen und gerundet werden.

Der relative Fehler des Computers aus Beispiel 2.39 wird in den meisten Anwendungen vernachlässigbar sein. Im folgenden Beispiel ergibt sich aber ein großer relativer Fehler:

Beispiel 2.40 Großer Rundungsfehler
Welches Ergebnis gibt unser Computer aus Beispiel 2.39 für die Berechnung von $(0.01 + 100) - 100 = 0.01$ aus? Wie groß ist der relative Fehler?

Lösung zu 2.40 Die Zahlen 0.01 und 100 werden intern im Gleitkommaformat dargestellt als $0.1 \cdot 10^{-1}$ bzw. $0.1 \cdot 10^3$. Für die Addition müssen die beiden Zahlen in eine Form mit gleicher Hochzahl umgewandelt werden. Es ist (exakt) $0.1 \cdot 10^{-1} = 0.00001 \cdot 10^3$, unser Computer kann aber nur 4 Stellen der Mantisse abspeichern und muss daher auf $0.0000 \cdot 10^3$ runden. Sein Ergebnis ist daher $(0.0 \cdot 10^3 + 0.1 \cdot 10^3) - 0.1 \cdot 10^3 = 0.0$! Der relative Fehler ist damit $\frac{0.01-0}{0.01} = 1$, also 100%. ■

Dieses Beispiel mag Ihnen vielleicht unrealistisch erscheinen. Der gleiche Effekt kann aber auch bei einer Genauigkeit von 16 Stellen bewirken, dass die Lösung eines einfachen Gleichungssystems vollkommen falsch berechnet wird (Übungsaufgabe 9).

In der Praxis tendiert man oft dazu, Rundungsfehler zu vernachlässigen und meistens geht das auch gut. In bestimmten Situationen können sich Rundungsfehler aber aufsummieren und dadurch von kleinen Problemen zu schweren Unfällen führen. So ist das im Golfkrieg beim Steuerprogramm der amerikanischen Abwehrraketen passiert: Während der kurzen Testphasen haben sich die Rundungsfehler nie ausgewirkt und wurden daher im Steuerprogramm nicht bemerkt. Beim längeren Betrieb während des Einsatzes haben sich die Fehler aber so weit aufsummiert, dass die Abwehrraketen ihr Ziel verfehlt haben.

Eine Möglichkeit ist, die Rechengenauigkeit zu erhöhen. Aber auch dann ist nicht immer klar, ob die erhöhte Genauigkeit ausreicht. Besser ist es, anstelle eines gerundeten Näherungswertes zwei Werte zu berechnen, die einmal nach oben und einmal nach unten gerundet wurden. Dadurch erhält man ein Intervall, begrenzt durch den nach oben und nach unten gerundeten Wert, in dem der exakte Wert liegen muss. Man spricht in diesem Fall von **Intervallarithmetik**. Intervallarithmetik ist zwar nicht genauer als Gleitkommaarithmetik, man kann aber sofort ablesen, wie genau das Ergebnis *mindestens* ist. Der Hauptnachteil besteht darin, dass Prozessoren derzeit nur Gleitkommaarithmetik beherrschen, während Intervallarithmetik mittels Software implementiert werden muss.

2.6 Teilbarkeit und Primzahlen

Es gilt $15 : 5 = 3$, oder anders geschrieben, $15 = 3 \cdot 5$. Man sagt, dass 3 und 5 Teiler von 15 sind. Es gibt Zahlen, die besonders viele Teiler haben und daher in der Praxis sehr beliebt sind. Zum Beispiel sind die Zahlen 24 und 60 besonders vielfältig teilbar, und nicht umsonst hat ein Tag 24 Stunden, eine Stunde 60 Minuten. Auf der anderen Seite gibt es die so genannten unteilbaren Zahlen, die Primzahlen. Sie haben große praktische Bedeutung für die Kryptographie und Codierungstheorie.

Definition 2.41 Eine ganze Zahl a heißt durch eine natürliche Zahl b **teilbar**, wenn es eine ganze Zahl n gibt, sodass $a = n \cdot b$ ist. Die Zahl b heißt in diesem Fall **Teiler** von a. Man schreibt dafür $b|a$, gelesen: „b teilt a“.

Beispiel 2.42 Teilbarkeit
a) $15 = 1 \cdot 15 = 3 \cdot 5$, hat also die Teiler 1, 3, 5 und 15. Insbesondere ist jede Zahl durch sich selbst und 1 teilbar. Also: $1|15$, $3|15$, $5|15$ und $15|15$.
b) -15 hat die Teiler 1, 3, 5 und 15. (Ein Teiler ist per Definition immer positiv.)
c) 13 hat nur die Teiler 1 und 13.

Definition 2.43 Eine natürliche Zahl $p > 1$, die nur durch sich selbst und durch 1 teilbar ist, heißt **Primzahl.**

Beispiel 2.44 (→CAS) Primzahlen
a) 2 ist eine Primzahl, weil 2 nur durch sich selbst und durch 1 teilbar ist.
b) Auch 3 ist eine Primzahl.
c) 4 ist keine Primzahl, weil 4 neben 1 und 4 auch den Teiler 2 hat.

d) 1 ist nur durch sich selbst teilbar, wird aber laut Definition nicht als Primzahl bezeichnet.

Die ersten Primzahlen sind 2, 3, 5, 7, 11, 13, 17, ... Primzahlen bilden im folgenden Sinn die „Bausteine“ der natürlichen Zahlen:

Satz 2.45 (Primfaktorzerlegung) Jede natürliche Zahl größer als 1 ist entweder selbst eine Primzahl, oder sie lässt sich als Produkt von Primzahlen schreiben. Die Faktoren einer solchen Zerlegung sind (bis auf ihre Reihenfolge) eindeutig und heißen **Primfaktoren**.

Warum haben Klavierbauer ein Problem mit der Primzahlzerlegung? Pythagoras hat vermutlich als erster erkannt, dass „wohlklingende Intervalle“ durch Schwingungsverhältnisse niedriger ganzer Zahlen beschrieben werden können. So wird eine Oktave durch das Schwingungsverhältnis $\frac{2}{1}$ beschrieben, eine Quint durch $\frac{3}{2}$, eine Quart durch $\frac{4}{3}$, usw. Das Schwingungsverhältnis zweier Quinten ist $(\frac{3}{2})^2 = \frac{9}{4}$.

Will man ein Klavier bauen, so stellt sich die Frage, wieviele Tasten pro Oktave benötigt werden, damit von jedem Ton weg eine reine Oktave und eine reine Quint gespielt werden kann. Ist c das Schwingungsverhältnis zweier benachbarter Tasten, so muss $c^n = \frac{2}{1}$ gelten, um nach n Tasten eine Oktave zu haben. Also $c = \sqrt[n]{2}$. Um zusätzlich nach m Tasten eine Quint zu haben, muss $\frac{3}{2} = c^m = 2^{m/n}$ gelten, oder umgeformt

$$3^n = 2^{n+m}.$$

Nach der Primfaktorzerlegung kann es für diese Gleichung aber keine ganzzahligen Lösungen geben. Kann man also kein Klavier bauen?

In der heutigen Praxis wird als Ausweg die *gleichstufige Stimmung* verwendet. Es wird dabei bei allen Intervallen ein wenig geschummelt. Die Schwingungsverhältnisse sind allesamt irrational, aber in der Nähe einfacher ganzzahliger Verhältnisse. Die Anzahl von 12 Tasten (7 weiße und 5 schwarze) bietet sich an, weil man dabei nur wenig schummeln muss ($\frac{3}{2} \approx 2^{7/12} = 1.4983$). Die nächstgrößere Zahl, bei der man weniger schummeln müßte, ist 41.

Beispiel 2.46 (→CAS) Primfaktorzerlegung
Zerlegen Sie in Primfaktoren: a) 60 b) 180

Lösung zu 2.46

a) $60 = 2 \cdot 30 = 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$. Nun wird auch klar, warum man 1 nicht als Primzahl bezeichnen möchte: Dann wären die Primfaktoren nicht mehr eindeutig, denn $60 = 2^2 \cdot 3 \cdot 5$ oder zum Beispiel auch $60 = 1 \cdot 2^2 \cdot 3 \cdot 5$ oder $60 = 1^2 \cdot 2^2 \cdot 3 \cdot 5$.

b) $180 = 3 \cdot 60 = 2^2 \cdot 3^2 \cdot 5$. ■

Man kann zeigen, dass es **unendlich viele Primzahlen** gibt. Bis heute wurde aber kein *Bildungsgesetz* gefunden, nach dem sich alle Primzahlen leicht berechnen lassen.

Der erste Beweis dafür, dass es unendlich viele Primzahlen gibt, stammt vom griechischen Mathematiker Euklid. Er leitet aus der Verneinung der Behauptung einen Widerspruch ab (Beweis durch Widerspruch).

Die Behauptung ist: „Es gibt unendlich viele Primzahlen.“ Nehmen wir nun deren Verneinung an, dass es also nur endlich viele Primzahlen gibt. Schreiben wir sie der Größe nach geordnet auf: $2, 3, 5, \ldots, p$, wobei also p die größte Primzahl ist. Bilden wir nun das Produkt dieser Primzahlen und zählen 1 dazu: $(2 \cdot 3 \cdot 5 \cdot 7 \cdots p) + 1$. Diese Zahl lässt sich nicht durch die Primzahlen $2, 3, 5, \ldots, p$ teilen, denn wir erhalten stets den Rest 1. Sind (wie angenommen) $2, 3, 5, \ldots, p$ die *einzigen* Primzahlen,

so ist diese Zahl also nur durch sich selbst und durch 1 teilbar – das bedeutet aber, dass sie eine weitere Primzahl ist! Damit haben wir einen Widerspruch zu unserer Annahme, dass $1, 2, 3, 5, \ldots, p$ bereits alle Primzahlen sind. Es muss also unendlich viele Primzahlen geben.

Definition 2.47 Wenn zwei natürliche Zahlen a und b keinen gemeinsamen Teiler außer 1 besitzen, dann nennt man sie **teilerfremd**. Das ist genau dann der Fall, wenn a und b keine gemeinsamen Primfaktoren haben.

Beispiel: $14 = 2 \cdot 7$ und $15 = 3 \cdot 5$ sind teilerfremd.

Ob zwei Zahlen a und b teilerfremd sind, kann man auch überprüfen, indem man ihren **größten gemeinsamen Teiler** $\mathrm{ggT}(a, b)$ berechnet. Ist dieser gleich 1, dann sind die Zahlen teilerfremd.

Beispiel 2.48 (→CAS) Teilerfremd, größter gemeinsamer Teiler
Bestimmen Sie: a) $\mathrm{ggT}(8, 12)$ b) $\mathrm{ggT}(137, 139)$

Lösung zu 2.48

a) $\mathrm{ggT}(8, 12) = 4$; denn 8 und 12 haben die *gemeinsamen* Teiler $1, 2, 4$, der größte gemeinsame Teiler ist daher 4.

b) $\mathrm{ggT}(137, 139) = 1$, die beiden Zahlen sind also teilerfremd. Warum sieht man das ohne zu rechnen? Nun, wenn q ein Teiler von 137 ist, dann gilt $q > 2$ und $139 \bmod q = (137 + 2) \bmod q = 2$. Es bleibt also immer ein Rest und die beiden Zahlen sind teilerfremd (was wir hier verwendet haben, ist bereits die Grundidee des Euklid'schen Algorithmus zur Berechnung des ggT – wir kommen in Abschnitt 3.3 darauf zurück). ■

Im Allgemeinen wird bei der Division einer ganzen Zahl durch eine natürliche Zahl ein Rest auftreten. Wenn wir etwa 17 durch 5 dividieren, so erhalten wir $17 = 3 \cdot 5 + 2$, also den Rest 2.

Satz 2.49 (Division mit Rest) Ist allgemein $a \in \mathbb{Z}$ und $m \in \mathbb{N}$, so ist

$$a = q \cdot m + r,$$

mit ganzen Zahlen q und r. Diese sind eindeutig bestimmt, indem man festlegt, dass $0 \leq r < m$ sein soll (das heißt, r soll die *kleinstmögliche nichtnegative* Zahl sein). Man nennt dabei m den **Modul**, r den **Rest modulo** m und schreibt abkürzend

$$r = a \bmod m \qquad \text{und} \qquad q = a \operatorname{div} m.$$

Beispiel 2.50 (→CAS) Rest modulo m
Berechnen Sie den Rest von a modulo 5:
a) $a = 17$ b) $a = -17$ c) $a = 35$ d) $a = 3$ e) $a = 22$

Lösung zu 2.50

a) Es ist $17 = 3 \cdot 5 + 2$, der Rest von 17 modulo 5 ist also $r = 2$. Es wäre z. B. auch $17 = 4 \cdot 5 - 3$, oder auch $17 = -1 \cdot 5 + 22$, oben wurde aber vereinbart, dass wir als Rest die kleinstmögliche nichtnegative Zahl bezeichnen. Daher muss r in diesem Beispiel $0 \leq r < 5$ erfüllen.
b) $-17 = -4 \cdot 5 + 3$, der Rest der Division ist also $r = 3$.
c) $35 = 7 \cdot 5 + 0$ der Rest ist hier also $r = 0$. Mit anderen Worten: 35 ist durch 5 teilbar.
d) $3 = 0 \cdot 5 + 3$, auch hier ist also der Rest $r = 3$.
e) $22 = 4 \cdot 5 + 2$, daher ist der Rest $r = 2$. ■

Auch im Alltag rechnen wir „modulo m“: Ist es zum Beispiel 16 Uhr am Nachmittag, so sagen wir auch, es sei 4 Uhr nachmittags. Wir haben den Rest von 16 modulo 12 angegeben.

Das Rechnen modulo einer natürlichen Zahl hat eine Vielzahl von Anwendungen in der Praxis, z. B. bei der Verwendung von Prüfziffern (siehe Kapitel 3).

2.7 Mit dem digitalen Rechenmeister

Approximation von $\sqrt{2}$

Das auf Seite 38 beschriebene Programm zur Annäherung der Wurzel aus 2 kann mit `Mathematica` wie folgt implementiert werden:

```
In[1]:= d[q_] := Module[{p = q},
                  While[(p/q)^2 < 2, p = p + 1];
                  {(p - 1)/q, p/q}]

In[2]:= d[100]
Out[2]= {141/100, 70/50}
```

Der Befehl `Module` fasst mehrere Befehle zusammen. Das erste Argument ist dabei eine Liste von lokalen Variablen.

Ungleichungen

`Mathematica` kann auch mit Ungleichungen umgehen. Der `Simplify`-Befehl kann zum Überprüfen von Ungleichungen verwendet werden:

```
In[3]:= Simplify[x/(x^2 + y^2) < 1/y, x > 0&&y > 0]
Out[3]= True
```

Mit `Reduce` können Ungleichungen sogar aufgelöst werden:

```
In[4]:= Reduce[1 - x^2 > 0, x]
```

```
Out[4]= -1 < x < 1
```

Komplexe Zahlen

Mit komplexen Zahlen rechnet man folgendermaßen:

```
In[5]:= z1 = 1 + 2I; z2 = 3 - I; z1/z2
Out[5]= 1/10 + 7i/10
```

Die imaginäre Einheit kann entweder über die Tastatur (als großes `I`) oder über die Palette (als $\mathbf{i}$) eingegeben werden. Real- bzw. Imaginärteil, komplexe Konjugation und Absolutbetrag erhält man mit

```
In[6]:= {Re[z1], Im[z1], Conjugate[z1], Abs[z1]}
Out[6]= {1, 2, 1 - 2i, Sqrt[5]}
```

Manchmal muss man mit dem Befehl `ComplexExpand` noch nachhelfen, damit das Ergebnis in Real- und Imaginärteil aufgespalten wird:

```
In[7]:= Sqrt[1 + I Sqrt[3]]
Out[7]= Sqrt[1 + I Sqrt[3]]

In[8]:= ComplexExpand[%]
Out[8]= Sqrt[3/2] + i/Sqrt[2]
```

Mehr noch, `Mathematica` geht bei allen Variablen standardmäßig davon aus, dass sie komplexwertig sind. Deshalb wird zum Beispiel der Ausdruck

```
In[9]:= Simplify[Sqrt[a b]/Sqrt[a]]
Out[9]= Sqrt[a b]/Sqrt[a]
```

nicht zu $\sqrt{b}$ vereinfacht, denn das stimmt im Allgemeinen nur für $a > 0$! Abhilfe schafft in so einem Fall die Möglichkeit, im `Simplify`-Befehl die Zusatzinformation $a > 0$ zu geben:

```
In[10]:= Simplify[Sqrt[a b]/Sqrt[a], a > 0]
Out[10]= Sqrt[b]
```

Summen- und Produktzeichen

Das Summenzeichen kann entweder direkt über die Palette eingegeben werden,

```
In[11]:= Sum[k, {k, 1, n}]
```

$$\texttt{Out[11]=}\ \frac{1}{2}\texttt{n}(1+\texttt{n})$$

oder auch als `Sum[k,{k,1,n}]`. Wie Sie sehen, wertet `Mathematica` (falls möglich) Summen sofort aus. Analog für Produkte: `Product[k,{k,1,n}]`.

Umwandlung zwischen Zahlensystemen

Der `Mathematica`-Befehl `BaseForm[x,b]` wandelt die Dezimalzahl `x` in eine Zahlendarstellung mit Basis `b` um. Zum Beispiel wird die Zahl $(0.1)_{10}$ mit

```
In[12]:= BaseForm[0.1, 2]
Out[12]//BaseForm=
         0.0001100110011001100110012
```

vom Dezimalsystem ins Dualsystem umgewandelt. Die Umwandlung einer Zahl x von einem System mit Basis b ins Dezimalsystem erhält man mit `b^^x`:

```
In[13]:= 16^^FAD
Out[13]//BaseForm=
         4013
```

wandelt die Hexadezimalzahl $(FAD)_{16}$ ins Dezimalsystem um oder

```
In[14]:= 8^^67
Out[14]//BaseForm=
         55
```

wandelt die Oktalzahl $(67)_8$ ins Dezimalsystem um.

Teilbarkeit und Primzahlen

Mit dem `Mathematica`-Befehl `PrimeQ` kann man feststellen, ob eine Zahl eine Primzahl ist:

```
In[15]:= PrimeQ[4]
Out[15]= False
```

Das „Q“ steht dabei für „question“. Mit einer `Do`-Schleife können wir zum Beispiel die Liste aller Primzahlen bis 5 ausgeben lassen:

```
In[16]:= Do[
           If[PrimeQ[n], Print[n]],
         {n, 1, 5}];

           2
           3
           5
```

Der Befehl zur Primfaktorzerlegung heißt `FactorInteger` und liefert die Liste aller Primfaktoren, zusammen mit der zugehörigen Vielfachheit:

```
In[17]:= FactorInteger[180]
Out[17]= {{2, 2}, {3, 2}, {5, 1}}
```

also $180 = 2^2 \cdot 3^2 \cdot 5^1$. Der größte gemeinsame Teiler kann mit dem Befehl `GCD` („greatest common divisor“) berechnet werden:

```
In[18]:= GCD[75, 38]
Out[18]= 1
```

Die Zahlen 75 und 38 sind also teilerfremd. Der Rest der Division einer ganzen Zahl x durch die natürliche Zahl m wird mit `Mod[x,m]` erhalten:

```
In[19]:= Mod[22, 5]
Out[19]= 2
```

Der Quotient der Division wird mit

```
In[20]:= Quotient[22, 5]
Out[20]= 4
```

berechnet. Also ist $22 = 4 \cdot 5 + 2$.

2.8 Kontrollfragen

Fragen zu Abschnitt 2.1: Die Zahlenmengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$

Erklären Sie folgende Begriffe: natürliche, ganze, rationale, irrationale, reelle, komplexe Zahlen, Potenz, Wurzel, Betrag einer reellen Zahl, Intervall, beschränkte Menge, Supremum, Infimum, Maximum, Minimum, Abrundungsfunktion, Realteil, Imaginärteil, Gauß'sche Zahlenebene, Betrag einer komplexen Zahl, konjugiert-komplexe Zahl.

1. Richtig oder falsch?
   a) $10^{-1} = \frac{1}{10}$ b) $10^0 = 0$ c) $100^{\frac{1}{2}} = 50$ d) $3 \cdot 2^2 = 6^2$
   e) $\frac{3x-2y}{3a-2b} = \frac{x-y}{a-b}$ f) $(5a^3)^2 = 25 \cdot a^6$ g) $9^{-2} = 3$ h) $(2x^3)^3 = 8x^6$
2. Bringen Sie den vor dem Wurzelzeichen stehenden Faktor unter die Wurzel:
   a) $3\sqrt{3}$ b) $3x\sqrt{x}$ c) $5\sqrt[3]{2}$ d) $x^2\sqrt[3]{4x}$
3. Ziehen Sie möglichst viele Faktoren vor die Wurzel:
   a) $\sqrt{18}$ b) $\sqrt[3]{81}$ c) $\sqrt{4a}$ d) $\sqrt[3]{2x^3}$ e) $\sqrt{\frac{8}{x^3}}$
4. Für welche reellen x sind die folgenden Ausdrücke definiert?
   a) $\frac{2x-1}{x^2-9}$ b) $\frac{x^2-1}{x^2}$ c) $\frac{4}{(x-1)(x+2)}$ d) $\frac{1}{x(x-1)}$
5. Richtig oder falsch? Sind a, b beliebige reelle Zahlen mit $a < b$, dann gilt:
   a) $-b < -a$ b) $2a < 3b$ c) $a^2 < b^3$
6. Richtig oder falsch?
   a) $|-5| > 0$ b) $|-1| - |1| = -2$ c) $|-a| = |a|$
   d) $|a| = a$ e) $4 - |-3| = 7$
7. Welche Zahlen haben den Abstand 2?
   a) -2 und 2 b) -2 und 0 c) 1 und -1

8. Welche reellen Zahlen x sind hier gemeint? Alle x mit:
   a) $|x| = 1$ b) $|x| < 1$ c) $|x - 3| = 1$ d) $|x| \leq 1$ e) $|x + 2| = 3$
9. Geben Sie die folgenden Mengen in Intervallschreibweise an:
   a) $\{x \in \mathbb{R} \mid 0 \leq x \leq 4\}$ b) $\{x \in \mathbb{R} \mid -1 < x \leq 1\}$ c) $\{x \in \mathbb{R} \mid x < -1\}$
   d) $\{x \in \mathbb{R} \mid 0 < x\}$ e) $\{x \in \mathbb{R} \mid x \leq 0\}$ f) $\mathbb{R}$
10. Berechnen Sie folgende Intervalle:
    a) $[0, 5] \cap (1, 6] = ?$ b) $[0, 7) \cup [7, 9] = ?$
11. Richtig oder falsch?
    a) $2 + 4\mathrm{i}$ und $-2 - 4\mathrm{i}$ sind zueinander konjugiert komplex.
    b) Der Imaginärteil von $3 - 5\mathrm{i}$ ist $-5\mathrm{i}$.
    c) $|2 + 4\mathrm{i}|$ hat Imaginärteil 0.

Fragen zu Abschnitt 2.2: Summen und Produkte

Erklären Sie folgende Begriffe: Summenzeichen, Produktzeichen, Fakultät.

1. Schreiben Sie die Summe aus und berechnen Sie sie gegebenenfalls:
   a) $\sum_{n=0}^{3}(-1)^n n^2$ b) $\sum_{n=1}^{3} n^n$ c) $\sum_{k=0}^{3} k\,(k+1)$
   d) $\sum_{k=0}^{3} x^k$ e) $\sum_{k=0}^{3} 4a_k$ f) $\sum_{k=0}^{3} b_{2k+1}$
2. Schreiben Sie mithilfe des Summenzeichens:
   a) $1 + 3 + 5 + 7 + \ldots + 23$ b) $x - \frac{x^2}{2} + \frac{x^3}{3} \mp \ldots - \frac{x^8}{8}$
   c) $1 - 2 + 3 - 4 + 5 - \ldots + 9 - 10$ d) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + 8 \cdot 9$
   e) $a_2 + a_4 + a_6 + a_8 + a_{10}$ f) $2 \cdot 4^1 + 2 \cdot 4^2 + 2 \cdot 4^3 + 2 \cdot 4^4 + 2 \cdot 4^5$

Fragen zu Abschnitt 2.3: Vollständige Induktion

Erklären Sie folgende Begriffe: vollständige Induktion, Induktionsanfang, Induktionsvoraussetzung, Induktionsschluss.

1. Richtig oder falsch:
   a) Die Induktion ist eine Möglichkeit um eine Aussage, die für endlich oder unendlich viele natürliche Zahlen behauptet wird, zu beweisen.
   b) Der Induktionsanfang besteht immer darin, dass die Aussage für $n = 1$ nachgeprüft wird.
   c) Beim Induktionsschluss wird vorausgesetzt, dass die behauptete Aussage stimmt. Dadurch beißt sich die Katze in den Schwanz.
   d) Die Induktion kann auch verwendet werden um Aussagen zu beweisen, die für alle reellen Zahlen gelten sollen.

Fragen zu Abschnitt 2.4: Stellenwertsysteme

Erklären Sie folgende Begriffe: Stellenwertsystem, Dezimalsystem, Dualsystem, Hexadezimalsystem.

1. Welche Zahlen sind durch einen Bruch darstellbar?
   a) 1.367 b) $0.00\overline{145}$ c) $0.3672879\ldots$ (nicht periodisch)
2. $0.\overline{145} = \frac{145}{999}$. Geben Sie eine Bruchdarstellung von $0.00\overline{145}$ an.
3. Geben Sie 302.015 als Summe von Zehnerpotenzen an.

4. a) Stellen Sie $(10101.1)_2$ im Dezimalsystem dar.
   b) Stellen Sie $(23.25)_{10}$ im Dualsystem dar.
   c) Stellen Sie $(75.25)_{10}$ im Oktalsystem dar.
   d) Stellen Sie $(2D)_{16}$ im Dezimalsystem dar.

Fragen zu Abschnitt 2.5: Maschinenzahlen

Erklären Sie folgende Begriffe: Maschinenzahl, Festkommadarstellung, (normalisierte) Gleitkommadarstellung, Mantisse, Exponent, Rundungsfehler, Maschinengenauigkeit.

1. Richtig oder falsch?
   a) Ein Computer kann aus Speichergründen nur endlich viele Zahlen darstellen.
   b) Die Zahl $\frac{1}{3}$ kann im Computer wie jede andere rationale Zahl ohne Rundungsfehler im Gleitkommaformat dargestellt werden.
   c) Bei der elektronischen Zahlenverarbeitung liegen (relative) Rundungsfehler immer unter 1%.
2. Einfachheitshalber gehen wir von einem Computer aus, der Zahlen im Dezimalsystem darstellt und eine 2-stelliger Mantisse hat. Welches gerundete Ergebnis gibt der Computer für $0.70 \cdot 10^1 \cdot 0.42 \cdot 10^1$ aus? Wie groß ist der relative Fehler?

Fragen zu Abschnitt 2.6: Teilbarkeit und Primzahlen

Erklären Sie folgende Begriffe: teilbar, Primzahl, Primfaktorzerlegung, teilerfremd, größter gemeinsamer Teiler, Division mit Rest, Modul, Rest modulo m.

1. Geben Sie alle Teiler an von: a) 24 b) 10 c) 7
2. Welche der Zahlen 1, 2, 3, 4, 5 sind Primzahlen?
3. Wie viele Primzahlen gibt es?
4. Kann man ein Bildungsgesetz angeben, nach dem sich alle Primzahlen berechnen lassen?
5. Finden Sie die Primfaktorzerlegung von: a) 24 b) 20 c) 28
6. Sind die folgenden Zahlen teilerfremd? Bestimmen Sie ihren größten gemeinsamen Teiler: a) 8 und 12 b) 8 und 9 c) 5 und 7
7. Richtig oder falsch:
   a) Zwei Primzahlen sind immer teilerfremd.
   b) Zwei teilerfremde Zahlen sind immer Primzahlen.

Lösungen zu den Kontrollfragen

Lösungen zu Abschnitt 2.1

1. a) richtig
   b) falsch; es ist $a^0 = 1$ für jede beliebige Basis $a \neq 0$, also $10^0 = 1$
   c) falsch; $100^{\frac{1}{2}} = \sqrt{100} = 10$
   d) falsch; Potenzieren hat Vorrang vor Multiplikation, daher $3 \cdot 2^2 = 3 \cdot 4 = 12$
   e) falsch; nur gemeinsame Faktoren von Zähler und Nenner können gekürzt werden
   f) richtig g) falsch; $9^{-2} = \frac{1}{9^2}$ h) falsch; $(2x^3)^3 = 8x^9$

2. a) $\sqrt{27}$ b) $\sqrt{9x^3}$ c) $\sqrt[3]{250}$ d) $\sqrt[3]{4x^7}$
3. a) $3\sqrt{2}$ b) $3\sqrt[3]{3}$ c) $2\sqrt{a}$ d) $x\sqrt[3]{2}$ e) $\frac{2}{x}\sqrt{\frac{2}{x}}$
4. Die Brüche sind nur für jene x definiert, für die der Nenner ungleich 0 ist, also:
   a) $x \in \mathbb{R}\backslash\{-3, 3\}$ b) $x \in \mathbb{R}\backslash\{0\}$ c) $x \in \mathbb{R}\backslash\{-2, 1\}$ d) $x \in \mathbb{R}\backslash\{0, 1\}$
5. a) richtig b) falsch; (z. B. $a = -4$, $b = -3$)
   c) falsch; (z. B. $a = -2$, $b = -1$)
6. a) richtig b) falsch; $|-1| - |1| = 0$ c) richtig
   d) falsch; $|a| = a$ stimmt nicht, wenn a negativ ist, z. B. $|-3| \neq -3$
   e) falsch; $4 - |-3| = 1$
7. a) falsch; $|-2-2| = 4$ b) richtig c) richtig
8. a) $x \in \{-1, 1\}$ b) $x \in (-1, 1)$
   c) alle x, deren Abstand von 3 gleich 1 ist: $x = 4$ oder $x = 2$
   d) $x \in [-1, 1]$ e) $x = 1$ oder $x = -5$
9. a) $[0, 4]$ b) $(-1, 1]$ c) $(-\infty, -1)$ d) $(0, \infty)$ e) $(-\infty, 0]$ f) $(-\infty, \infty)$
10. a) $(1, 5]$ b) $[0, 9]$
11. a) falsch; komplexe Konjugation ändert nur das Vorzeichen des Imaginärteils
    b) falsch; der Imaginärteil ist -5 (eine reelle Zahl!)
    c) richtig; der Betrag ist immer eine reelle (nichtnegative) Zahl

Lösungen zu Abschnitt 2.2

1. a) -6 b) 32 c) 20 d) $1 + x^1 + x^2 + x^3$ e) $4\,a_0 + 4\,a_1 + 4\,a_2 + 4\,a_3$
   f) $b_1 + b_3 + b_5 + b_7$
2. a) $\sum_{k=0}^{11}(2k+1)$ b) $\sum_{n=1}^{8}(-1)^{n+1}\,\frac{x^n}{n}$
   c) $\sum_{k=0}^{9}(-1)^k\,(k+1)$ oder $\sum_{k=1}^{10}(-1)^{k+1}\,k$ d) $\sum_{k=1}^{8} k\,(k+1)$
   e) $\sum_{n=1}^{5} a_{2n}$ f) $\sum_{k=1}^{5} 2 \cdot 4^k$

Lösungen zu Abschnitt 2.3

1. a) falsch; die Induktion wird nur verwendet, wenn eine Aussage für **unendlich** viele ganze Zahlen ab einer bestimmten Zahl $n_0 \in \mathbb{Z}$ (z. B. alle natürlichen Zahlen) behauptet wird
   b) falsch; beim Induktionsanfang wird die Aussage für die kleinste Zahl, für die die Behauptung aufgestellt wurde, geprüft. Das ist meist $n = 1$, kann aber auch z. B. $n = 0$ oder $n = 2$ oder sogar eine negative ganze Zahl sein. (Das ist sozusagen der erste Dominostein, alle nachfolgenden werden dann umgeworfen.)
   c) falsch; beim Induktionsschluss setzt man voraus, dass man *ein (beliebiges) festes* n gefunden hat, für das die Behauptung gilt. Dann schließt man daraus, dass die Formel auch für $n + 1$ gilt.
   d) falsch, denn je zwei reelle Zahlen liegen nicht im Abstand 1 voneinander entfernt

Lösungen zu Abschnitt 2.4

1. a) $1.367 = \frac{1367}{1000}$
   b) durch Bruch darstellbar, weil periodisch
   c) nicht als Bruch darstellbar, weil nicht-periodisch

2. $0.00\overline{145} = \frac{145}{99900}$
3. $302.015 = 3 \cdot 10^2 + 2 \cdot 10^0 + 1 \cdot 10^{-2} + 5 \cdot 10^{-3}$
4. a) $(10101.1)_2 = 2^4 + 2^2 + 2^0 + 2^{-1} = (21.5)_{10}$
   b) $(23.25)_{10} = 16 + 4 + 2 + 1 + 0.25 = (10111.01)_2$
   c) $(75.25)_{10} = 64 + 11 + 0.25 = 8^2 + 8^1 + 3 \cdot 8^0 + 2 \cdot 8^{-1} = (113.2)_8$
   d) $(2D)_{16} = 2 \cdot 16^1 + 13 \cdot 16^0 = (45)_{10}$

Lösungen zu Abschnitt 2.5

1. a) richtig
   b) falsch; rationale Zahlen, die unendlich viele Nachkommastellen haben, müssen vom Computer gerundet werden
   c) falsch; siehe Beispiel 2.40 auf Seite 56
2. $0.70 \cdot 10^1 \cdot 0.42 \cdot 10^1 = 0.294 \cdot 10^2$ (exakt). Wegen der nur 2-stelligen Mantisse gibt der Computer das Ergebnis $0.29 \cdot 10^2$ aus. Relativer Fehler: $\frac{0.4}{29.4} = 0.0136 = 1.4\%$.

Lösungen zu Abschnitt 2.6

1. a) $1, 2, 3, 4, 6, 8, 12, 24$ b) $1, 2, 5, 10$ c) $1, 7$
2. 2, 3 und 5 sind Primzahlen. 1 ist per Definition keine Primzahl, und 4 hat neben 1 und 4 noch den Teiler 2.
3. unendlich viele
4. nein, ein solches Bildungsgesetz wurde bis heute nicht gefunden
5. Man spaltet so oft wie möglich die kleinste Primzahl 2 ab, dann so oft wie möglich 3, dann 5, usw.:
   a) $24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$ b) $20 = 2^2 \cdot 5$ c) $28 = 2^2 \cdot 7$
6. a) nein; $\mathrm{ggT}(8, 12) = 4$
   b) $8 = 2 \cdot 2 \cdot 2$ und $9 = 3 \cdot 3$ sind teilerfremd, weil sie keine gemeinsamen Primfaktoren besitzen. Anders argumentiert: teilerfremd, weil $\mathrm{ggT}(8, 9) = 1$.
   c) ja, da $\mathrm{ggT}(5, 7) = 1$
7. a) richtig
   b) falsch; zum Beispiel sind 9 und 4 teilerfremd, aber keine Primzahlen

2.9 Übungen

Aufwärmübungen

1. Vereinfachen Sie $|a| + a$ für a) positives a b) negatives a.
   Machen Sie am Ende die Probe, indem Sie eine konkrete positive bzw. negative Zahl für a einsetzen.
2. (Wiederholung Rechnen mit Brüchen) Schreiben Sie den Ausdruck als einen einzigen Bruch und vereinfachen Sie:
   a) $\dfrac{1}{x-y} - \dfrac{1}{y-x}$ b) $\dfrac{5}{b-1} - \dfrac{6b}{b^2-1} - \dfrac{1-2b}{b+b^2}$

3. Lösen Sie nach der angegebenen Variablen auf:
   a) $w = \frac{1}{2}v\left(1 - \frac{1+k}{1+\frac{a}{b}}\right)$; b =? b) $\frac{A}{2} = \frac{b}{a\left(\frac{1}{x} - \frac{1}{y}\right)}$; x =?
4. (Wiederholung Rechnen mit Potenzen) Vereinfachen Sie:
   a) $\frac{(3 \cdot 10^{-2})^2 \cdot 4 \cdot 10^3}{10^{-1}}$ b) $\left(2a^2\right)^2 \frac{1}{(2a)^3}\frac{1}{a^{-1}}$ c) $\frac{b^{\frac{1}{2}}(b^{\frac{1}{2}} - b^{\frac{5}{2}})}{b}$
   d) $\left(x^{-1} + \frac{1}{3x}\right)\left(\frac{x}{3} + 1\right)^{-1}$
5. (Wiederholung Rechnen mit Potenzen) Vereinfachen Sie:
   a) $\frac{\sqrt[3]{16}}{\sqrt[3]{2}}$ b) $\frac{\sqrt{xy}}{\sqrt{\frac{x}{y}}}$ c) $\frac{\sqrt[3]{u^4 v}}{\sqrt[3]{uv}}$ d) $\frac{\sqrt{x^{2m+1}}}{\sqrt{x}}$
6. Es gilt $0 = 1$, wie die folgende Kette von Äquivalenzumformungen zeigt:

$$\begin{aligned} 6^2 - 6 \cdot 11 &= 5^2 - 5 \cdot 11 \\ 6^2 - 6 \cdot 11 + (\frac{11}{2})^2 &= 5^2 - 5 \cdot 11 + (\frac{11}{2})^2 \\ (6 - \frac{11}{2})^2 &= (5 - \frac{11}{2})^2 \\ 6 - \frac{11}{2} &= 5 - \frac{11}{2} \\ 1 &= 0 \end{aligned}$$

   Wo steckt der Fehler?
7. (Wiederholung Rechnen mit Ungleichungen) Finden Sie alle $x \in \mathbb{R}$, die folgende Ungleichung erfüllen:
   a) $|x - 2| < 1$ b) $\frac{1+x}{1-x} < 3$
8. Berechnen Sie für $z_1 = 1 - \mathrm{i}$ und $z_2 = 6 + 2\mathrm{i}$ und geben Sie jeweils den Real- und den Imaginärteil an.
   a) $z_1 + z_2$ b) $z_1 z_2$ c) $\overline{z_2}$ d) $|z_2|$ e) $\frac{z_1}{z_2}$
9. Schreiben Sie mithilfe des Summenzeichens:
   a) $1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \frac{x^6}{6!} + \frac{x^8}{8!}$ b) $a_0a_1 + a_1a_2 + a_2a_3 + a_3a_4$ c) $x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4}$
10. Zeigen Sie mithilfe des Induktionsprinzips, dass

$$2^0 + 2^1 + \ldots + 2^{n-1} = 2^n - 1$$

    für alle natürlichen Zahlen n gilt.
11. Zeigen Sie mithilfe vollständiger Induktion, dass $2^n > n$ für alle $n \in \mathbb{N}$ gilt.
12. Zeigen Sie mithilfe vollständiger Induktion, dass
    a) $\sum_{k=1}^{n}(2k-1) = n^2$ b) $\sum_{k=1}^{n} k^2 = \frac{(2n+1)(n+1)n}{6}$
    für alle $n \in \mathbb{N}$ gilt.
13. Zeigen Sie mithilfe vollständiger Induktion, dass $n! \leq n^n$ für alle $n \in \mathbb{N}$ gilt.
14. Unter UNIX werden die Zugriffsrechte für eine Datei durch neun Bit (d.h. eine 9-stellige Dualzahl) dargestellt. Die ersten drei Bit legen fest, ob der Besitzer Lese-, Schreib- oder Ausführbarkeitsrechte besitzt. Die nächsten drei Bit legen dasselbe für Benutzer der gleichen Gruppe

fest, und die letzten drei Bit definieren die Rechte für alle anderen Benutzer.
Beispiel: $(111\,110\,100)_2$ würde bedeuten, dass der Besitzer alle Rechte hat, die Gruppe Lese- und Schreibrechte, und alle übrigen Benutzer nur Leserechte. Die Rechte werden übersichtlichkeitshalber in der Regel nicht dual, sondern oktal angegeben. So würde man anstelle von $(111\,110\,100)_2$ schreiben: $(764)_8$.

Geben Sie die UNIX-Zugriffsrechte dual und oktal an:
a) Besitzer kann lesen und schreiben, alle anderen nur lesen.
b) Besitzer kann alles, alle anderen lesen und ausführen.
c) Besitzer und Gruppe können lesen und schreiben, alle anderen nur lesen.

15. Welche UNIX-Zugriffsrechte wurden definiert?
a) $(640)_8$ b) $(744)_8$ c) $(600)_8$
16. Welches gerundete Ergebnis gibt ein Computer für $0.738 \cdot 0.345$ aus, der
a) eine 3-stellige Mantisse hat b) eine 4-stellige Mantisse hat.
Wie groß ist jeweils der relative Fehler? (Nehmen Sie einfachheitshalber an, dass der Computer Zahlen im Dezimalsystem darstellt.)
17. Ist die Zahl 97 eine Primzahl? Überprüfen Sie das, indem Sie *der Reihe nach* für die Primzahlen $2, 3, 5, 7, \cdots$ feststellen, ob sie ein Teiler von 97 sind (d.h., ermitteln Sie die Primfaktorzerlegung von 97). Müssen Sie alle Primzahlen von 2 bis 97 durchprobieren, oder können Sie schon früher aufhören?

Weiterführende Aufgaben

1. a) Gilt für beliebige $x, y \in \mathbb{R}$ mit $0 < x < y$ und für beliebiges $b \in \mathbb{R}$ mit $b > 0$ immer
$$\frac{x}{b+x} < \frac{y}{b+y}?$$
b) Gilt für beliebige Zahlen $a, b, n \in \mathbb{N}$ immer
$$\frac{a \cdot 2^{-n}}{a \cdot 2^{-n} + b} \leq \frac{a}{b} \cdot 2^{-n}.$$
Diese Abschätzungen werden z. B. gebraucht um die Wahrscheinlichkeit zu berechnen, dass ein Primzahltest – der z. B. Primzahlen für den RSA-Algorithmus finden soll – eine Zahl fälschlicherweise als Primzahl identifiziert.
2. Zeigen Sie, dass $\sqrt{3}$ irrational ist.
3. Zeigen Sie mithilfe vollständiger Induktion, dass
$$\sum_{k=1}^{n} (-1)^k k^2 = (-1)^n \frac{n(n+1)}{2} \qquad \text{für alle } n \in \mathbb{N}$$
gilt.
4. Zeigen Sie mithilfe vollständiger Induktion, dass
$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4} \qquad \text{für alle } n \in \mathbb{N}$$
gilt.

5. Zeigen Sie mithilfe vollständiger Induktion, dass

$$\prod_{k=1}^{n}\left(1+\frac{2}{k}\right)=\frac{(n+1)(n+2)}{2} \qquad \text{für alle } n\in\mathbb{N}$$

gilt.

6. Zeigen Sie mithilfe vollständiger Induktion, dass

$$(1+x)^n > 1+n\cdot x \qquad \text{für alle } n\in\mathbb{N}, \text{mit } n>1$$

gilt (dabei ist $x\in\mathbb{R}$, $x>-1$, $x\neq 0$).

7. Zeigen Sie mithilfe vollständiger Induktion, dass

$$n^3-n \text{ durch 6 teilbar} \qquad \text{für alle } n\in\mathbb{N}$$

ist.

8. a) Stellen Sie $(110\,011.01)_2$ im Dezimalsystem dar.
   b) Stellen Sie $(359.2)_{10}$ im Dualsystem dar.
   c) Stellen Sie $(8978)_{10}$ im Oktalsystem dar.
   d) Stellen Sie $(ABCD)_{16}$ im Dezimalsystem dar.
9. Die Lösung des Gleichungssystems $ax-by=1$, $cx-dy=0$ ist gegeben durch $x=\frac{d}{ad-bc}$ und $y=\frac{c}{ad-bc}$. Berechnen Sie die Lösung für den Fall $a=64919121$, $b=159018721$, $c=41869520.5$, $d=102558961$ mit Gleitkommaarithmetik (Mantisse mit 16 Dezimalstellen) und exakt. Nehmen Sie an, dass eine zu lange Mantisse einmal auf- und einmal abgerundet wird (in der Praxis hängt das Ergebnis vom verwendeten Zahlensystem und der genauen Rundungsvorschrift ab).

   Dieses Problem kann auch geometrisch verstanden werden: Die beiden Gleichungen können als zwei Geraden interpretiert werden. Die Lösung ist der Schnittpunkt der beiden Geraden. Im Allgemeinen wird eine kleine Verschiebung einer Geraden (aufgrund von Rundungsfehlern) auch den Schnittpunkt nur wenig verschieben. Sind die beiden Geraden aber fast parallel, so bewirkt eine kleine Verschiebung eine starke Verschiebung des Schnittpunkts. Letzterer Fall liegt hier vor.

Lösungen zu den Aufwärmübungen

1. a) positives a: $|a|+a=a+a=2a$; Probe z. B. mit $a=3$: $|3|+3=3+3=6=2\cdot 3$
   b) negatives a: $|a|+a=(-a)+a=0$; Probe z. B. mit $a=-3$: $|-3|+(-3)=3-3=0$
2. a) $\frac{1}{x-y}-\frac{1}{y-x}=\frac{1}{x-y}+\frac{1}{-(y-x)}=\frac{2}{x-y}$
   b) Wir bringen alle Brüche auf gemeinsamen Nenner und vereinfachen:
   $\frac{5}{b-1}-\frac{6b}{(b+1)(b-1)}-\frac{1-2b}{b(b+1)}=\frac{5b(b+1)-6b^2-(1-2b)(b-1)}{b(b+1)(b-1)}=\frac{b+1}{b(b-1)}$
3. a) $b=\frac{a(v-2w)}{kv+2w}$ b) $x=\frac{Aay}{2by+Aa}$
4. a) 36 b) $\frac{a^2}{2}$ c) $1-b^2$ d) $\frac{4}{x(x+3)}$
5. a) 2 b) y c) u d) x^m
6. Aus $a^2=b^2$ folgt nur $|a|=|b|$: $6-\frac{11}{2}=+\frac{1}{2}$ und $5-\frac{11}{2}=-\frac{1}{2}$.

7. a) Die Unbekannte x steht zwischen Betragstrichen. Um die Betragsstriche loszuwerden, müssen wir laut Definition 2.11 unterscheiden, ob der Ausdruck zwischen den Betragstrichen ≥ 0 oder < 0 ist:
(i) $x-2 \geq 0$, also $x \geq 2$. Für diese x lautet die Angabe: $|x-2| = x-2 < 1$, also $x < 3$. Alle x mit $x \geq 2$ und $x < 3$ sind also Lösungen. In Intervallschreibweise notiert: $x \in [2,3)$.
(ii) $x-2 < 0$, d.h. $x < 2$, wir durchsuchen nun also diese x auf Lösungen. Die Angabe lautet nun: $|x-2| = -x+2 < 1$, also $x > 1$. Unter den x mit $x < 2$ sind demnach alle x mit $x > 1$ Lösungen: $x \in (1,2)$.
Insgesamt wird die gegebene Ungleichung von jenen x erfüllt, die $x \in (1,2)$ oder $x \in [2,3)$ erfüllen, also von $x \in (1,3)$.
b) Um die Ungleichung aufzulösen, möchten wir als Erstes beide Seiten mit dem Nenner multiplizieren. Nun kann dieser, je nach dem Wert von x, positiv oder negativ sein, und dementsprechend bleibt die Richtung des Ungleichungszeichens bestehen oder ändert sich. Daher sind wieder zwei Fälle zu unterscheiden:
(i) Nenner $1-x > 0$ bzw. umgeformt, $x < 1$. Für diese x lautet die Angabe (nach Multiplikation beider Seiten mit dem Nenner): $1+x < 3(1-x)$ und daraus folgt $x < \frac{1}{2}$. Es muss also für eine Lösung $x < 1$ und $x < \frac{1}{2}$ gelten. Die Bedingung $x < 1$ ist insbesondere für alle x mit $x < \frac{1}{2}$ erfüllt, also $x \in (-\infty, \frac{1}{2})$.
(ii) Nenner $1-x < 0$, also suchen wir unter den x mit $x > 1$ nach Lösungen. Nach Multiplikation beider Seiten mit dem Nenner (und Umdrehung der Richtung des Ungleichungszeichens), lautet die Angabe $1+x > 3(1-x)$ und daraus folgt $x > \frac{1}{2}$. Lösungen müssen demnach $x > 1$ und $x > \frac{1}{2}$ erfüllen; also $x \in (1,\infty)$.
Insgesamt wird die gegebene Ungleichung von $x \in (-\infty, \frac{1}{2})$ oder $x \in (1,\infty)$ erfüllt: $x \in (-\infty, \frac{1}{2}) \cup (1,\infty)$.
8. a) $7+\mathrm{i}$; Realteil: 7, Imaginärteil: 1
b) $8-4\mathrm{i}$; Realteil: 8, Imaginärteil: -4
c) $6-2\mathrm{i}$; Realteil: 6, Imaginärteil: -2
d) $\sqrt{40} = 2\sqrt{10}$; Realteil: $\sqrt{40}$, Imaginärteil: 0 (Absolutbetrag ist reelle Zahl!)
e) $\frac{1}{10}(1-2\mathrm{i})$; Realteil: $\frac{1}{10}$, Imaginärteil: $-\frac{1}{5}$
9. a) $\displaystyle\sum_{k=0}^{4} \frac{x^{2k}}{(2k)!}$ b) $\displaystyle\sum_{i=0}^{3} a_i \cdot a_{i+1}$ c) $\displaystyle\sum_{k=1}^{4} \frac{(-1)^{k+1}x^k}{k}$
10. Induktionsanfang: Wir überprüfen, ob die Beziehung für $n = 1$ gilt: $2^0 = 2^1 - 1$ ist richtig.
Induktionsschluss: Wir setzen voraus, dass wir ein $n \in \mathbb{N}$ mit

$$2^0 + 2^1 + \ldots + 2^{n-1} = 2^n - 1$$

gefunden haben(Induktionsvoraussetzung). Nun ist zu zeigen, dass die Formel auch für die nächstgrößere natürliche Zahl, also für $n+1$ gilt, also dass

$$2^0 + 2^1 + \ldots + 2^{n-1} + 2^n = 2^{n+1} - 1.$$

Wir betrachten davon die linke Seite, verwenden die Induktionsvoraussetzung, und formen um:

$$\underbrace{2^0 + 2^1 + \ldots + 2^{n-1}}_{= 2^n - 1 \text{ nach IV}} + 2^n = 2^n - 1 + 2^n = 2 \cdot 2^n - 1 = 2^{n+1} - 1.$$

Damit ist der Induktionsschluss gelungen und wir haben somit gezeigt, dass die Beziehung $\sum_{k=0}^{n-1} 2^k = 2^n - 1$ für alle n gilt.

11. Induktionsanfang: Wir überprüfen, ob die Beziehung für $n = 1$ gilt. Dazu setzen wir in $2^n > n$ für n den Wert 1 ein: $2^1 > 1$ ist richtig. Überprüfen wir auch (wir werden das später brauchen), ob die Beziehung für $n = 2$ gilt: $2^2 > 2$ stimmt auch.
Induktionsschluss: Wir setzen voraus, dass wir ein $n > 1$ mit $2^n > n$ gefunden haben (Induktionsvoraussetzung). (Das trifft zu, denn wir haben für $n = 2$ herausgefunden, dass die Beziehung gilt.) Nun ist zu überprüfen, ob unter dieser Voraussetzung die Beziehung für $n + 1$ gilt, ob also $2^{n+1} > n + 1$ gilt. Gehen wir wieder von der linken Seite aus, formen diese ein wenig um, und verwenden dann die Induktionsvoraussetzung:

$$2^{n+1} = \underbrace{2^n}_{> n \text{ nach IV}} \cdot 2 > n \cdot 2.$$

Da $n \cdot 2 = n + n$ und $n > 1$ ist, folgt $n + n > n + 1$, also erhalten wir zusammenfassend

$$2^{n+1} = 2^n \cdot 2 > n \cdot 2 = n + n > n + 1.$$

Damit steht die Ungleichung für $n + 1$ da und somit ist der Induktionsschluss gelungen. Wir haben gezeigt, dass die Beziehung $2^n > n$ für alle n gilt.

12. (Wenn Sie sich leichter tun, dann schreiben Sie alle Summen aus. Die kompakte Schreibweise mit dem Summenzeichen ist zwar einerseits übersichtlicher, aber andererseits auch eine Fehlerquelle.)
a) Induktionsanfang: $\sum_{k=1}^{1}(2k-1) = 1 = 1^2$ ist richtig.
Induktionsschluss: Wir setzen voraus, dass wir ein n gefunden haben, für das $\sum_{k=1}^{n}(2k-1) = n^2$ gilt (Induktionsvoraussetzung). Nun ist zu zeigen, dass die Formel auch für $n + 1$ gilt, also dass

$$\sum_{k=1}^{n+1}(2k-1) = (n+1)^2.$$

Betrachten wir davon die linke Seite, verwenden die Induktionsvoraussetzung und formen noch etwas um:

$$\sum_{k=1}^{n+1}(2k-1) = \underbrace{\sum_{k=1}^{n}(2k-1)}_{= n^2 \text{ nach IV}} + (2(n+1)-1) = n^2 + 2n + 1 = (n+1)^2$$

wie gewünscht.
b) Induktionsanfang: $\sum_{k=1}^{1} k^2 = 1 = \frac{6}{6}$ ist richtig.
Induktionsschluss: Wir nehmen an, dass wir ein $n \in \mathbb{N}$ gefunden haben, für das $\sum_{k=1}^{n} k^2 = \frac{(2n+1)(n+1)n}{6}$ gilt (Induktionsvoraussetzung). Zu zeigen ist, dass unter dieser Voraussetzung auch $\sum_{k=1}^{n+1} k^2 = \frac{(2n+3)(n+2)(n+1)}{6}$ gilt. Wieder gehen wir von der linken Seite aus, verwenden die Induktionsvoraussetzung und formen um: $\sum_{k=1}^{n+1} k^2 = \sum_{j=1}^{n} k^2 + (n+1)^2 = \frac{(2n+1)(n+1)n}{6} + (n+1)^2 = \frac{(2n+1)(n+1)n+6(n+1)^2}{6}$

$= \frac{(2n+3)(n+2)(n+1)}{6}$. Damit ist der Induktionsschluss gelungen und die Formel für alle $n \in \mathbb{N}$ bewiesen.

13. Induktionsanfang: $1! = 1 = 1^1$ und somit ist $1! \leq 1^1$ richtig.
Induktionsschluss: Wir setzen voraus, dass wir ein $n \in \mathbb{N}$ gefunden haben, für das $n! \leq n^n$ gilt (Induktionsvoraussetzung). Zu zeigen: $(n+1)! \leq (n+1)^{n+1}$. Also:

$$(n+1)! = (n+1) \cdot \underbrace{n!}_{\leq n^n} \leq (n+1)n^n \leq (n+1)(n+1)^n = (n+1)^{n+1},$$

wie gewünscht.

14. a) $(110\,100\,100)_2 = (644)_8$ b) $(111\,101\,101)_2 = (755)_8$ c) $(110\,110\,100)_2 = (664)_8$
15. a) Besitzer kann lesen und schreiben, Gruppe kann lesen.
b) Besitzer kann alles, alle anderen nur lesen.
c) Nur der Besitzer kann lesen und schreiben.
16. Exakte Lösung wäre 0.25461; Ergebnis des Computers:
a) 0.255; relativer Fehler = 0.15% b) 0.2546; relativer Fehler = 0.004%
17. Ja. Es reicht, 2, 3, 5, 7 zu probieren (alle Primzahlen $\leq \sqrt{121} = 11$), da $11^2 = 121$ bereits größer als 97 ist (diese Idee geht auf den griechischen Mathematiker Eratosthenes (ca. 284–202 v. Chr.) zurück: „Sieb des Eratosthenes“).

(Lösungen zu den weiterführenden Aufgaben finden Sie in Abschnitt B.2)

3

Elementare Begriffe der Zahlentheorie

3.1 Modulare Arithmetik oder das kleine Einmaleins auf endlichen Mengen

Erinnern Sie sich an die Division mit Rest aus Satz 2.49: Wenn $a \in \mathbb{Z}$ und $m \in \mathbb{N}$, so kann man a in der Form

$$a = q \cdot m + r$$

schreiben, wobei q und r aus $\mathbb{Z}$ eindeutig bestimmt sind durch die Festlegung $0 \leq r < m$. Diese Zahl r heißt Rest der Division und man verwendet dafür auch die Schreibweise $r = a \bmod m$. Beispiel: $17 \bmod 5 = 2$, in Worten: „Der Rest der Division von 17 durch 5 ist 2“ oder kurz „17 modulo 5 ist 2“.

In diesem Kapitel werden wir uns näher mit dem Rechnen mit Resten, der so genannten modularen Arithmetik beschäftigen. Insbesondere werden wir es dabei nur mit ganzen Zahlen, also Elementen aus $\mathbb{Z}$, zu tun haben.

Modulare Arithmetik ist für viele Anwendungen in der Informatik wichtig, vor allem in der Kryptographie (z. B. IDEA oder RSA-Algorithmus) und Codierungstheorie. Denn immer, wenn man es mit einem endlichen Alphabet (durch Zahlen codiert) zu tun hat, stößt man unweigerlich auf Reste. Ein einfaches Beispiel, das die Idee verdeutlichen soll: Das Alphabet {A, ..., Z} kann durch die Zahlen $\{0, 1, \ldots, 25\}$ dargestellt werden. Angenommen, eine Verschlüsselungsvorschrift lautet $y = x + 3$. Dann wird $x = 2$ (= Buchstabe C) zu $y = 2 + 3 = 5$ (Buchstabe F) verschlüsselt; $x = 25$ (Buchstabe Z) wird aber zu $y = 28$ verschlüsselt. Wir fallen also aus dem Alphabet heraus, es sei denn, wir beginnen bei 26 wieder mit A. Mathematisch formuliert nehmen wir den Rest modulo 26: $y = (x + 3) \bmod 26$. Damit ist $y = 28 \bmod 26 = 2$ (Buchstabe C).

Definition 3.1 Wenn zwei ganze Zahlen a und b bei Division durch $m \in \mathbb{N}$ denselben Rest haben, so sagt man, a und b sind **kongruent modulo** m. Man schreibt dafür $a \equiv b \,(\mathrm{mod}\, m)$ oder auch einfach $a = b \,(\mathrm{mod}\, m)$. Die Zahl m heißt **Modul**.

Zum Beispiel ist $17 = 22 \,(\mathrm{mod}\, 5)$, da sowohl 17 als auch 22 bei Division durch 5 den Rest 2 haben. Man kann auch überprüfen, ob zwei Zahlen kongruent modulo m sind, indem man ihre Differenz betrachtet:

Satz 3.2 Zwei Zahlen a und b sind kongruent modulo m genau dann, wenn sie sich um ein Vielfaches von m unterscheiden, d.h., wenn $a - b = km$ mit $k \in \mathbb{Z}$ ist.

Das ist leicht zu verstehen: $a = b \,(\mathrm{mod}\, m)$ genau dann, wenn beide denselben Rest r bei Division durch m haben; das heißt, es gibt ganze Zahlen q_1 und q_2 mit $a = q_1 m + r$ und $b = q_2 m + r$. Das bedeutet aber, dass $a - b = (q_1 - q_2)m$, dass also $a - b$ ein Vielfaches von m ist.

Beispiel 3.3 (→CAS) Kongruente Zahlen
Richtig oder falsch?
a) $17 = 2 \,(\mathrm{mod}\, 5)$ b) $17 = -3 \,(\mathrm{mod}\, 5)$ c) $18 = 25 \,(\mathrm{mod}\, 6)$

Lösung zu 3.3
a) Richtig, denn die Differenz $17 - 2 = 15$ ist ein Vielfaches von 5 (oder anders ausgedrückt: 17 und 2 haben bei Division durch 5 denselben Rest).
b) Richtig, denn $17 - (-3) = 17 + 3 = 20$ ist ein Vielfaches von 5.
c) Falsch, denn $18 - 25 = -7$ ist kein Vielfaches von 6. ■

Wir haben in Beispiel 3.3 gesehen, dass 17 kongruent modulo 5 sowohl zu 2, als auch zu -3 ist. Mehr noch: 17 ist kongruent modulo 5 zu allen Zahlen, die sich von 17 um ein Vielfaches von 5 unterscheiden: zu 17, 22, 27, 32, usw. und auch zu 12, 7, 2, -3, -8, -13, usw. Denn alle diese Zahlen haben bei Division durch 5 den Rest 2. Man sagt, alle diese Zahlen liegen in derselben **Restklasse**. Da bei der Division durch 5 die Reste 0, 1, 2, 3, 4 auftreten können, gibt es fünf Restklassen modulo 5:

$$\begin{aligned}
\{\ldots, -15, -10, -5, 0, 5, 10, \ldots\} &\quad \ldots \quad \text{alle Zahlen mit Rest 0 modulo 5} \\
\{\ldots, -14, -9, -4, 1, 6, 11, \ldots\} &\quad \ldots \quad \text{alle Zahlen mit Rest 1 modulo 5} \\
\{\ldots, -13, -8, -3, 2, 7, 12, \ldots\} &\quad \ldots \quad \text{alle Zahlen mit Rest 2 modulo 5} \\
\{\ldots, -12, -7, -2, 3, 8, 13, \ldots\} &\quad \ldots \quad \text{alle Zahlen mit Rest 3 modulo 5} \\
\{\ldots, -11, -6, -1, 4, 9, 14, \ldots\} &\quad \ldots \quad \text{alle Zahlen mit Rest 4 modulo 5}
\end{aligned}$$

Allgemein gibt es m Restklassen modulo m, nämlich für jeden der Reste 0, 1, ..., $m - 1$ genau eine Restklasse.

Alle Zahlen innerhalb einer Restklasse verhalten sich bei Addition bzw. Multiplikation gleich. Das sagen die folgenden Rechenregeln:

Satz 3.4 Wenn $a = b \,(\mathrm{mod}\, m)$ und $c = d \,(\mathrm{mod}\, m)$ gilt, dann folgt

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

Man darf also in Summen und Produkten ohne weiteres eine Zahl durch irgendeinen anderen Vertreter aus ihrer Restklasse ersetzen, sofern man nur am Ergebnis modulo m interessiert ist. Insbesondere folgt daraus, dass man auf beiden Seiten der Kongruenzgleichung eine *ganze* Zahl c addieren oder mit c multiplizieren darf. Achtung: Wir können aber im Allgemeinen *nicht kürzen*: $8 = 2 \,(\mathrm{mod}\, 6)$, aber nicht

$4 = 1 \pmod 6$! Das Kürzen durch 2 würde hier einer Multiplikation mit der *Bruchzahl* $\frac{1}{2}$ auf beiden Seiten der Kongruenzgleichung entsprechen, und von Bruchzahlen ist in obiger Regel aber keine Rede.

Warum gelten die Rechenregeln aus Satz 3.4? Nun, $a = b \pmod m$ bedeutet gleicher Rest, also eine Darstellung der Form $a = qm + r_1$ und $b = pm + r_1$. Analog bedeutet $c = d \pmod m$ gleicher Rest, also $c = km + r_2$ und $d = hm + r_2$. Setzen wir das nun für a, b, c, d ein: $a + c = qm+r_1+km+r_2 = (q+k)m+(r_1+r_2)$, analog ist $b+d = pm+r_1+hm+r_2 = (p+h)m+(r_1+r_2)$. Wir sehen also, dass $a+c$ und $b+d$ denselben Rest bei Division durch m haben, kurz: $a+c = b+d \pmod m$. Analog geht die Überlegung für die Multiplikation.

Beispiel 3.5 Rechnen mit kongruenten Zahlen
Berechnen Sie den angegebenen Rest:
a) $(38 + 22) \bmod 9$ b) $(101 + 234) \bmod 5$ c) $(38 \cdot 22) \bmod 9$
d) $(101 \cdot 234) \bmod 5$ e) $(38 + 22 \cdot 17) \bmod 4$

Lösung zu 3.5
a) Natürlich können wir $38 + 22 = 60$ und dann den Rest von 60 bei Division durch 9 berechnen: $60 \bmod 9 = 6$. Alternative: Wir suchen den kleinsten Vertreter aus der Restklasse von 38, ebenso aus der Restklasse von 22 (das sind gerade die Reste 2 bzw. 4 höchstpersönlich). Aus Satz 3.4 folgt dann: $38 + 22 = 2 + 4 = 6 \pmod 9$.
b) Wieder ersetzen wir die vorkommenden Zahlen durch ihre Reste modulo 5: $101 + 234 = 1 + 4 = 5 = 0 \pmod 5$. Die Zahl $101 + 234 = 335$ hat bei Division durch 5 also den Rest 0.
c) Wegen $38 = 2 \pmod 9$ und $22 = 4 \pmod 9$ ist $38 \cdot 22 = 2 \cdot 4 = 8 \pmod 9$. Wir konnten also recht mühelos berechnen, dass die Zahl $38 \cdot 22$ bei Division durch 9 den Rest 8 hat!
d) Wegen $101 = 1 \pmod 5$ und $234 = 4 \pmod 5$ ist $101 \cdot 234 = 1 \cdot 4 = 4 \pmod 5$.
e) $38 + 22 \cdot 17 = 2 + 2 \cdot 1 = 4 = 0 \pmod 4$. ■

Beispiel 3.6 Wochentagsformel
Welcher Wochentag war der 15.5.1955?
(Hinweise: (i) Der 1.1.1900 war ein Montag. (ii) Alle durch 4 teilbaren Jahre sind Schaltjahre, mit Ausnahme der durch 100 teilbaren, die nicht auch gleichzeitig durch 400 teilbar sind. Zum Beispiel war 1900 kein Schaltjahr, da es durch 100, nicht jedoch durch 400 teilbar ist; aber 2000 war ein Schaltjahr, weil es durch 400 teilbar ist.)

Lösung zu 3.6 Wir müssen die Anzahl der Tage, die zwischen dem 1.1.1900 und dem 15.5.1955 vergangen sind, berechnen und modulo 7 nehmen. Dann wissen wir den Wochentag (0 = Montag, 1 = Dienstag, usw.).

Beginnen wir mit den Tagen zwischen dem 1.1.1900 und dem 1.1.1955. Da ein Jahr 365 Tage hat, waren es $365 \cdot 55$ Tage (Schaltjahre noch nicht berücksichtigt). Da wir nur das Ergebnis modulo 7 brauchen, können wir $365 = 1 \pmod 7$ und $55 = 6 \pmod 7$ verwenden und erhalten $365 \cdot 55 = 1 \cdot 6 = 6 \pmod 7$. Wegen $55 = 4 \cdot 13 + 3$ gab es dazwischen 13 Schaltjahre (1900 war kein Schaltjahr). Für jedes Schaltjahr müssen wir einen Tag dazurechnen, also kommen wir auf $6 + 13 = 19 = 5 \pmod 7$. Der 1.1.1955 war also ein Samstag.

Nun zu den Tagen zwischen 1.1.1955 und 1.5.1955. Wir brauchen nur die Tage der Monate (Achtung beim Februar, falls es sich um ein Schaltjahr handelt)

Monat	1	2	3	4	5	6	7	8	9	10	11	12
Tage	31	28/29	31	30	31	30	31	31	30	31	30	31
Tage (mod 7)	3	0/1	3	2	3	2	3	3	2	3	2	3

zusammenzuzählen: $3 + 0 + 3 + 2 = 1 \pmod 7$. Die Bilanz bisher (vom 1.1.1900 bis 1.5.1955) lautet dann: $5 + 1 = 6$. Der 1.5.1955 war somit ein Sonntag. Nehmen wir nun noch die 14 Tage seit Monatsbeginn (1.5.1955 bis 15.5.1955) dazu und zählen alles zusammen, so erhalten wir $5 + 1 + 14 = 20 = 6 \pmod 7$. Der gesuchte Tag war also ein Sonntag! ■

Wenn man zuerst die Anzahl der Tage berechnet und erst am Ende modulo 7 rechnet, dann muss man schon ganz gut im Kopfrechnen sein. So ist es aber auch für ungeübte Kopfrechner zu schaffen! Analoges gilt für Computerprogramme; da kann es nämlich schnell passieren (z. B. in der Kryptographie, wo mit großen Zahlen „modulo“ gerechnet wird), dass man einen Überlauf produziert, wenn man es ungeschickt angeht.

Modulorechnen wird auch bei Prüfziffern verwendet.

Vielleicht haben Sie schon einmal im Internet mit Ihrer Kreditkarte bezahlt und der Computer hat beim Absenden der Daten Ihre Kartennummer als ungültig zurückgewiesen. Bei Kontrolle der Nummer ist Ihnen dann aufgefallen, dass Sie bei der Eingabe zwei Ziffern vertauscht haben. Hätte der Computer diesen Fehler nicht sofort erkannt, so wären vermutlich einige Umstände auf Sie, den Verkäufer und die Kreditkartenfirma zugekommen. Wie aber hat der Computer erkannt, dass Sie zwei Ziffern vertauscht haben? Die Lösung ist einfach: Die letzte Ziffer einer Kreditkartennummer ist eine Prüfziffer, die mit modularer Arithmetik aus den übrigen Ziffern berechnet wird. Stimmt sie nicht, so wurde bei der Eingabe ein Fehler gemacht.

Beispiel 3.7 Prüfziffer
Auf Büchern findet sich eine zehnstellige *Internationale Standard-Buchnummer* (ISBN) der Form *a-bcd-efghi-p*. Dabei ist a das Herkunftsland (so steht etwa $a = 3$ für Deutschland, Österreich, Schweiz), bcd bezeichnet den Verlag und p ist die Prüfziffer, die

$$10a + 9b + 8c + 7d + 6e + 5f + 4g + 3h + 2i + p = 0 \pmod{11}$$

erfüllen muss. (Anstelle von 10 wird das Symbol X geschrieben.) Das Buch „Geheime Botschaften“ von S. Singh hat die ISBN 3-446-19873-p. Wie lautet die Prüfziffer p $(0 \le p \le 10)$?

Lösung zu 3.7 Die Prüfziffer p muss Lösung der Gleichung

$$10 \cdot 3 + 9 \cdot 4 + 8 \cdot 4 + 7 \cdot 6 + 6 \cdot 1 + 5 \cdot 9 + 4 \cdot 8 + 3 \cdot 7 + 2 \cdot 3 + p = 0 \pmod{11}$$

sein. Es muss also $250 + p = 8 + p = 0 \pmod{11}$ gelten. Somit ist p die Lösung der Gleichung $8 + p = 0 \pmod{11}$. Wegen Satz 3.4 können wir hier auf beiden Seiten -8 addieren um nach p aufzulösen: $p = -8 = 3 \pmod{11}$. ■

3.1.1 Anwendung: Hashfunktionen

Modulare Arithmetik wird auch bei **Hashverfahren** verwendet. Eine **Hashfunktion** ist eine Funktion, die Datensätzen beliebiger Länge (beliebig viele Bit) Datensätze fester Länge (z. B. 128 Bit) zuordnet. Diese Datensätze fester Länge (also z. B. alle Dualzahlen der Länge 128) heißen **Hashwerte**. Hashverfahren werden in der Informatik zum Beispiel zum effizienten Speichern und Suchen von Datensätzen verwendet.

Betrachten wir folgendes Beispiel: Wir möchten Orte und zugehörige Vorwahlen so speichern, dass man zu einem gegebenen Ort möglichst schnell die zugehörige Vorwahl bekommt. Jeder Datensatz besteht aus zwei Teilen: Ort (das ist der Suchbegriff, der eingegeben wird) und Vorwahl. Der Teil, nach dem gesucht wird, in unserem Fall der Ort, wird **Schlüssel** genannt. Der andere Teil des Datensatzes, in unserem Fall die Vorwahl, wird als **Wert** bezeichnet.

Die Idee ist, dass die Speicheradresse aus dem Schlüssel (Suchbegriff) selbst berechnet wird, sodass aufwändige Suchverfahren nicht notwendig sind. Dies geschieht durch eine Hashfunktion. Das ist in diesem Beispiel eine Abbildung H von der Menge K aller möglichen Schlüssel k (Orte) in die Menge A der verfügbaren Speicheradressen:

$$\begin{array}{rcl} H:\ K & \to & A = \{0, 1, \ldots, N-1\} \\ k & \mapsto & H(k) \end{array}$$

Wir haben hier angenommen, dass es N Adressen gibt, die mit $0, \ldots, N-1$ durchnummeriert werden. Der Schlüssel k wird also unter der Adresse $H(k)$ (Hashwert des Schlüssels) abgelegt bzw. wieder gefunden.

Beispiel 3.8 Hashfunktion
Die möglichen Schlüssel k sind Zeichenketten, die Orte bedeuten. Die Hashfunktion sei

$$H(k) = \sum_i a_i \bmod N,$$

wobei a_i die Stelle des i-ten Buchstaben im Alphabet bezeichnet (Beispiel: Für $k = XYZ$ ist $a_1 = 24$, $a_2 = 25$ und $a_3 = 26$). Angenommen, es gibt $N = 7$ Speicheradressen. Berechnen Sie dann den Wert der Hashfunktion für folgende Schlüssel: WIEN, GRAZ, SALZBURG, DORNBIRN.

Lösung zu 3.8 Dem Ort WIEN entsprechen die Zahlen $23, 9, 5, 14$ (da W der 23. Buchstabe im Alphabet ist, I der 9. Buchstabe, usw.). Die Speicheradresse von WIEN ist daher $H(\text{WIEN}) = 23+9+5+14 = 51 = 2 \pmod 7$. Analog folgt $H(\text{GRAZ}) = 3$, $H(\text{SALZBURG}) = 1$, $H(\text{DORNBIRN}) = 3$. (Da hier immer modulo 7 gerechnet wird, lassen wir den Zusatz $(\text{mod}\,7)$ weg, um Schreibarbeit zu sparen.) ■

Dieses Beispiel zeigt das typische Problem bei Hashverfahren: Den Schlüsseln GRAZ und DORNBIRN wird derselbe Speicherplatz zugeordnet. Man spricht von einer **Kollision**. In der Tat ist die Anzahl aller möglichen Schlüssel (hier alle möglichen Buchstabenkombinationen) in der Regel um ein Vielfaches größer als die Anzahl der verfügbaren Hashwerte (hier Speicheradressen). Daher legt man im Fall einer

Kollision den Schlüssel auf einem um eine bestimmte Schrittweite m verschobenen Speicherplatz ab.

Zusammenfassend geht man daher wie folgt vor: Soll der Datensatz (k, v) bestehend aus Schlüssel k (für engl. *key* = Schlüssel) und Wert v (engl. *value* = Wert) abgelegt werden, so

- berechne den Hashwert $n = H(k)$.
- Ist der Speicherplatz n frei, so lege den Datensatz dort ab, sonst (Kollision) versuche den um m Plätze verschobenen Speicherplatz $n + m \pmod N$.

Soll zu einem gegebenen Schlüssel k der zugehörige Wert v gefunden werden, so

- berechne $n = H(k)$.
- Ist der dort liegende Schlüssel k_n gleich k, so ist das zugehörige v_n der gesuchte Wert. Andernfalls gehe auf den um m verschobenen Speicherplatz $n+m \pmod N$ und vergleiche erneut den Suchbegriff mit dem dort abgelegten Schlüssel.

Für die Fälle, dass beim Abspeichern kein freier Platz mehr gefunden wird, oder der Suchbegriff keinem Datensatz entspricht, müssen noch Abbruchbedingungen eingebaut werden, um Endlosschleifen zu vermeiden.

Beispiel 3.9 Hashtabelle
Gegeben seien folgende Paare aus Schlüsseln und Werten: (WIEN, 01), (GRAZ, 0316), (SALZBURG, 0662), (DORNBIRN, 05572). Die Hashfunktion sei wie im vorigen Beispiel definiert. Bei Auftreten einer Kollision soll um $m = 1$ Speicherplätze weitergegangen werden. Stellen Sie die Hashtabelle auf und suchen Sie den Wert von DORNBIRN.

Lösung zu 3.9 Aus dem letzten Beispiel wissen wir bereits, dass $H(\text{WIEN}) = 2$, $H(\text{GRAZ}) = 3$, $H(\text{SALZBURG}) = 1$ und $H(\text{DORNBIRN}) = 3$. Wir legen also die Datensätze für WIEN, GRAZ und SALZBURG auf die Speicherplätze 2, 3 bzw. 1. Da der Speicherplatz 3 bereits belegt ist, legen wir DORNBIRN auf dem Platz $3 + 1 = 4$ ab:

Speicherplatz (n)	Schlüssel (k_n)	Wert (v_n)
0		
1	SALZBURG	0662
2	WIEN	01
3	GRAZ	0316
4	DORNBIRN	05572
5		
6		

Um nach DORNBIRN zu suchen, berechnen wir zunächst $H(\text{DORNBIRN}) = 3$. Da $k_3 = \text{GRAZ} \neq \text{DORNBIRN}$, müssen wir 3 um 1 erhöhen. Nun ist $k_4 = \text{DORNBIRN}$ und $v_4 = 05572$ der gesuchte Wert. ■

In der Praxis sollten natürlich nicht zu viele Kollisionen auftreten, deshalb muss eine gute Hashfunktion die möglichen Schlüssel möglichst gleichmäßig auf die möglichen Speicherplätze verteilen. Als Faustregel gilt weiters, dass maximal 80% der verfügbaren Speicherplätze aufgefüllt werden sollten.

Die Wahrscheinlichkeit, dass *irgendeine* Kollision auftritt, ist übrigens recht hoch, wie das folgende **Geburtstagsparadoxon** zeigt: Nehmen wir an, Sie ordnen jeder Person in einem Raum ihren Geburtstag zu. Die Personen werden also gleichmäßig auf 365 Plätze verteilt (wir nehmen an, dass jeder Geburtstag gleich wahrscheinlich ist). Eine Kollision tritt auf, wenn *irgendwelche* zwei Personen darunter am gleichen Tag Geburtstag haben. Die Wahrscheinlichkeit dafür ist bei 23 Personen bereits über 50%! Wenn Sie also bei einer Party mit mehr als 23 Personen wetten, dass *irgendwelche* zwei Gäste am gleichen Tag Geburtstag haben, so sind Ihre Chancen zu gewinnen größer als 50%! Verteilt man n Schlüssel (Personen) auf N Plätze (Tage im Jahr), so ist die Wahrscheinlichkeit für mindestens eine Kollision (gemeinsamer Geburtstag) $P = 1 - \frac{N!}{(N-n)!N^n}$.

Hashfunktionen werden auch oft als Prüfziffern verwendet. Ein häufig verwendetes Verfahren ist der MD5-Algorithmus (Message Digest Version 5), der aus Daten beliebiger Länge eine 128-Bit Prüfziffer (=Hashwert) berechnet. Wenn Sie sich zum Beispiel Software aus dem Internet laden, dann wird oft zusätzlich zur Datei die MD5-Prüfziffer angegeben. Nach dem Download können Sie diese Prüfziffer berechnen und durch Vergleich sicherstellen, dass die Datei ohne Fehler heruntergeladen wurde. Zum Beispiel unter GNU UNIX (unter BSD UNIX lautet der Befehl `md5`):

```
[susanne@soliton susanne]$ md5sum kdebase-3.0.3.tar.bz2
a1c6cb06468608318c5e59e362773360 kdebase-3.0.3.tar.bz2
```

Die MD5-Prüfziffer wird dabei als Hexadezimalzahl ausgegeben. Der MD5-Algorithmus hat noch eine weitere Eigenschaft: Während es bei klassischen Prüfziffern (z. B. ISBN) leicht möglich ist, Daten (gezielt) zu verändern, ohne die Prüfziffer zu ändern, ist dies hier praktisch unmöglich. Solche Hashfunktionen sind schwer zu finden und werden als **Einweg-Hashfunktionen** oder **digitaler Fingerabdruck** bezeichnet. Die Einweg-Eigenschaft ist entscheidend für Anwendungen in der Kryptographie (z. B. für die digitale Signatur). Hier verwendet man heutzutage den Secure-Hash-Algorithmus (SHA-1, SHA-256, SHA-512), der die Einweg-Anforderung noch besser erfüllt.

3.2 Gruppen, Ringe und Körper

Fassen wir alle möglichen Reste, die bei der Division modulo m entstehen können, zu einer neuen Menge zusammen:

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

Äquivalent kann man $\mathbb{Z}_m$ auch als die Menge aller Restklassen modulo m definieren, da jede Restklasse $\{r + m \cdot n \mid n \in \mathbb{Z}\}$ ja eindeutig durch den zugehörigen Rest r bestimmt ist. Manchmal wird die Schreibweise $\mathbb{Z}/m\mathbb{Z}$ für $\mathbb{Z}_m$ verwendet.

Diese Menge von Resten hat, wie eingangs erwähnt, zum Beispiel die Bedeutung eines Alphabets: etwa $\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$ oder, für die Informatik besonders wichtig, $\mathbb{Z}_2 = \{0, 1\}$.

In $\mathbb{Z}_m$ (also für die „Buchstaben des Alphabets“) kann man nun auf einfache Weise eine Addition und eine Multiplikation definieren, indem man als Ergebnis immer den Rest modulo m nimmt (und somit niemals aus dem Alphabet herausfällt). Zum Beispiel erhalten wir für $\mathbb{Z}_5$ folgende Additions- und Multiplikationstabelle:

+	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

·	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

Zur linken Tabelle: Zum Beispiel ist $4 + 2 = 1 \pmod 5$, da $4 + 2 = 6$ und der Rest von 6 bei Division durch 5 gleich 1 ist. Rechte Tabelle: $2 \cdot 3 = 6 = 1 \pmod 5$. Das Ergebnis liegt also immer wieder in $\mathbb{Z}_5$.

Dieses Einmaleins ist also recht einfach, denn es gibt nur endlich viele Möglichkeiten, Summen bzw. Produkte zu bilden. Eine derartige Additions- bzw. Multiplikationstabelle für $\mathbb{Z}$ ist gar nicht möglich, da $\mathbb{Z}$ ja aus unendlich vielen Zahlen besteht.

Beispiel 3.10 Addition und Multiplikation in $\mathbb{Z}_m$
Berechnen Sie:
a) $3 + 5 \pmod 7$ b) $8 + 3 \pmod{11}$ c) $3 \cdot 5 \pmod 7$ d) $8 \cdot 3 \pmod{11}$

Lösung zu 3.10

a) $3+5 = 8 = 1 \pmod 7$. Für den Zwischenschritt haben wir das Ergebnis $3+5 = 8$ in $\mathbb{Z}$ berechnet (also $\mathbb{Z}_7$ verlassen) und dann die zu 8 kongruente Zahl aus $\mathbb{Z}_7$ als Ergebnis erhalten. Alle Gleichheitszeichen bedeuten hier „ist kongruent modulo 7“ (was auch den Fall „ist gleich“ mit einschließt).
b) $8 + 3 = 11 = 0 \pmod{11}$, da der Rest von 11 bei Division durch 11 gleich 0 ist.
c) $3 \cdot 5 = 15 = 1 \pmod 7$
d) $8 \cdot 3 = 24 = 2 \pmod{11}$

■

Genau genommen rechnet auch jeder Computer mit Resten. Nehmen wir einfachheitshalber an, dass zur Speicherung nur zwei (Dezimal-)Stellen zur Verfügung stehen. Dann tritt z. B. bei der Addition $86 + 22$ ein Überlauf auf und das Ergebnis ist nicht 108, sondern 8. Der Computer rechnet hier also modulo 100. Es ist die Aufgabe des Programms, diesen Fehler zu erkennen und abzubrechen.

Andererseits ist es aber auch möglich, diesen Überlauf bewusst auszunutzen, um mit *negativen* Zahlen zu rechnen: Da $86 = -14 \pmod{100}$, verhält sich 86 bei Rechnungen modulo 100 gleich wie -14. So ist zum Beispiel $22+86 = 8 \pmod{100}$, ebenso wie $22-14 = 8 \pmod{100}$. In der Informatik verwendet man das, um negative ganze Zahlen abzuspeichern:

Stehen $n + 1$ Bit zur Verfügung, so werden die ganzen Zahlen von -2^n bis $2^n - 1$ dadurch abgespeichert, dass man jede negative Zahl x zwischen -2^n und -1 mit der zugehörigen positiven Zahl y zwischen 2^n und $2^{n+1} - 1$ identifiziert, die $x = y \pmod{2^{n+1}}$ erfüllt. Beispiel: Bei $n + 1 = 4$ Bit werden die Zahlen $-2^3, \ldots, -1$ durch die Zahlen $2^3, \ldots, 2^4 - 1$ dargestellt. Zum Beispiel wird -4 durch 12 dargestellt, denn $-4 = 12 \pmod{16}$.

In Dualdarstellung lässt sich das leicht durchführen, indem man mit dem Betrag beginnt, $|-4| = 4 = (0100)_2$, alle Nullen und Einsen vertauscht, $(1011)_2 = (11)_{10}$ (**Einskomplement**), und dann eins hinzuaddiert, $(1100)_2 = (12)_{10}$ (**Zweikomplement**).

Wir sehen aus obiger Tabelle, dass $4 + 1 = 0 \pmod 5$. Man kann also 1 als Negatives zu 4 in $\mathbb{Z}_5$ betrachten.

Definition 3.11 Zu $e \in \mathbb{Z}_m$ ist das **Negative** oder **additive Inverse** jene Zahl $d \in \mathbb{Z}_m$, für die

$$e + d = 0 \pmod m$$

ist. Man schreibt (in Anlehnung an die gewohnte Schreibweise für die reellen Zahlen) kurz $-e$ für das additive Inverse zu $e \in \mathbb{Z}_m$.

Ein additives Inverses gibt es zu jeder Zahl aus $\mathbb{Z}_m$ und es lässt sich auch leicht berechnen:

Satz 3.12 Zu jeder Zahl e aus $\mathbb{Z}_m$ gibt es genau ein additives Inverses d:

$$d = m - e \text{ für } e \neq 0 \qquad \text{und} \qquad d = 0 \text{ für } e = 0.$$

Beispiel 3.13 Additives Inverses in $\mathbb{Z}_m$
Finden Sie das additive Inverse von $0, 1, 2, 3, 4$ in $\mathbb{Z}_5$.

Lösung zu 3.13 Das additive Inverse von 0 ist 0, denn $0 + 0 = 0 \pmod 5$. Das additive Inverse zu $e = 1$ ist $d = m - e = 5 - 1 = 4$. (Das ist jene Zahl aus $\mathbb{Z}_5$, die in derselben Restklasse wie -1 liegt.) Analog ist das additive Inverse von 2 in $\mathbb{Z}_5$ gleich $5 - 2 = 3$, das additive Inverse von 3 ist $5 - 3 = 2$, und von 4 ist das additive Inverse $5 - 4 = 1$. Probe: $0 + 0 = 0 \pmod 5$, $1 + 4 = 0 \pmod 5$, $2 + 3 = 0 \pmod 5$, $3 + 2 = 0 \pmod 5$, $4 + 1 = 0 \pmod 5$. ■

Eine kleine Anwendung des additiven Inversen ist die so genannte Caesar-Verschlüsselung. Julius Caesar (100–44 v. Chr.) soll damit geheime Botschaften verschlüsselt haben:

Beispiel 3.14 Caesar-Verschlüsselung
Codieren Sie die Buchstaben des Alphabets zunächst gemäß A = 0, B = 1, ..., Z = 25 durch Zahlen und verschlüsseln Sie dann die Nachricht „KLEOPATRA“ nach der Vorschrift

$$y = x + e \pmod{26} \quad \text{mit dem Schlüssel } e = 3.$$

Wie wird wieder entschlüsselt?

Lösung zu 3.14 In Zahlen lautet KLEOPATRA: $10, 11, 4, 14, 15, 0, 19, 17, 0$. Verschlüsseln wir jede dieser Zahlen x gemäß $y = x + 3 \pmod{26}$:

x	10	11	4	14	15	0	19	17	0
$y = x + 3 \pmod{26}$	13	14	7	17	18	3	22	20	3

Wir erhalten die verschlüsselte Nachricht (in Zahlen) $13, 14, 7, 17, 18, 3, 22, 20, 3$, oder, wieder in Buchstaben: NOHRSDWUD.

Zum Entschlüsseln müssen wir $y = x + 3 \pmod{26}$ nach x auflösen, indem wir auf beiden Seiten -3 addieren, also $x = y - 3 = y + 23 \pmod{26}$. Zum Beispiel erhalten wir für $y = 13$ den Klartextbuchstaben $x = 13 + 23 = 36 = 10 \pmod{26}$ usw. Alternativ wäre hier der Rechengang $x = 13 - 3 = 10 \pmod{26}$ zulässig gewesen.

y	13	14	7	...	20	3
$x = y + 23 \pmod{26}$	10	11	4	...	17	0

■

Warnung: Dieses Verfahren bietet keinerlei Sicherheit, da es nur 25 Möglichkeiten für die Verschiebung gibt, es also leicht ist, alle Möglichkeiten durchzuprobieren. Das Knacken des Codes geht sogar noch schneller, wenn der Text lang genug ist: Da der häufigste Buchstabe im Deutschen das „E“ ist, liegt die Vermutung nahe, dass er auf den häufigsten Buchstaben im Geheimtext abgebildet wird. Und wenn wir die Verschlüsselung eines einzigen Buchstaben kennen, dann kennen wir bei der Caesar-Verschlüsselung bereits die gesamte Verschlüsselungsvorschrift.

Sie kennen die Caesar-Verschlüsselung vielleicht auch aus dem Internet als ROT13. Hier wird um genau 13 Stellen verschoben. Dadurch ergibt sich die spezielle Eigenschaft von ROT13, dass die gleiche Funktion zum Ver- und Entschlüsseln verwendet wird, denn: $13 = -13 \pmod{26}$, also $d = e$.

Nehmen wir uns nun die Multiplikation in $\mathbb{Z}_m$ vor: Wir sehen aus obiger Multiplikationstabelle, dass $2 \cdot 3 = 1 \pmod{5}$. Man kann also 3 als den *Kehrwert* von 2 in $\mathbb{Z}_5$ betrachten.

Definition 3.15 Wenn es zu $e \in \mathbb{Z}_m$ eine Zahl $d \in \mathbb{Z}_m$ gibt mit

$$e \cdot d = 1 \pmod{m},$$

so nennt man d den **Kehrwert** oder das **multiplikative Inverse** zu e modulo m. In Anlehnung an die gewohnte Schreibweise in $\mathbb{R}$ schreibt man das multiplikative Inverse zu e in $\mathbb{Z}_m$ kurz als e^{-1} oder als $\frac{1}{e}$.

Also ist in $\mathbb{Z}_5$ mit der Schreibweise $\frac{1}{2}$ die Zahl 3 gemeint. Achtung: Im Unterschied zum additiven Inversen gibt es nicht zu allen Zahlen aus $\mathbb{Z}_m$ ein multiplikatives Inverses! Zu 0 gibt es zum Beispiel kein multiplikatives Inverses in $\mathbb{Z}_m$.

Das ist klar: Denn für jedes d gilt ja, dass $0 \cdot d = 0$ ist, also kann das Ergebnis niemals 1 werden. Aus demselben Grund gibt es auch in $\mathbb{R}$ für die 0 keinen Kehrwert („Division durch 0 gibt es nicht“). Abgesehen von der 0 gibt es in $\mathbb{R}$ aber für jede Zahl einen Kehrwert.

Auch wenn man die 0 ausnimmt, gibt es in $\mathbb{Z}_m$ nicht unbedingt zu jeder Zahl einen Kehrwert. Um einen Kehrwert zu besitzen, muss eine Zahl eine bestimmte Eigenschaft haben:

Satz 3.16 Für $e \neq 0$ in $\mathbb{Z}_m$ gilt: Es gibt (genau) ein multiplikatives Inverses genau dann, wenn e und m teilerfremd sind.

Das kann man folgendermaßen sehen: Suchen wir zum Beispiel ein Inverses zu 2 modulo 6, also d mit $2d = 1 \pmod{6}$. Das bedeutet, dass sich $2d$ und 1 um ein Vielfaches von 6 unterscheiden müssen, dass also $2d = 1 + n6$ für ein $n \in \mathbb{Z}$ gelten muss; oder, umgeformt, $2d - 6n = 1$. Weil 6 und 2 nun den gemeinsamen Teiler 2 haben, können wir diesen Teiler herausheben: $2d - 6n = 2(d - 3n) = 1$. Es gibt aber kein ganzzahliges d, sodass diese Gleichung, die ja die Form 2·ganze Zahl = 1 hat, erfüllt ist! Da 2 und 6 also einen gemeinsamen Teiler haben, gibt es kein multiplikatives Inverses für 2 modulo 6.

Wenn es einen Kehrwert gibt, dann kann er (zumindest für kleines m) einfach mit der Hand berechnet werden:

Beispiel 3.17 (→CAS) Multiplikatives Inverses in $\mathbb{Z}_m$

a) Gibt es ein multiplikatives Inverses zu 4 in $\mathbb{Z}_9$? Geben Sie es gegebenenfalls an.
b) Für welche Zahlen aus $\mathbb{Z}_5$ gibt es ein multiplikatives Inverses? Geben Sie es gegebenenfalls an.
c) Für welche Zahlen aus $\mathbb{Z}_6$ gibt es ein multiplikatives Inverses?

Lösung zu 3.17

a) Da 4 und 9 teilerfremd sind, gibt es zu 4 ein multiplikatives Inverses. Schreiben wir es einfach wie gewohnt mit $\frac{1}{4}$ an, nun ist jedoch eine ganze Zahl aus $\mathbb{Z}_9$ damit gemeint. Wir finden sie ganz einfach mit folgendem „Trick“: Wir ersetzen die 1 im Zähler durch eine beliebige andere Zahl aus derselben Restklasse, und probieren solange verschiedene kongruente Zahlen für den Zähler, bis der Bruch eine ganze Zahl darstellt:

$$\frac{1}{4}, \frac{1+9}{4}, \frac{1+2\cdot 9}{4} \text{ sind keine ganzen Zahlen, aber } \frac{1+3\cdot 9}{4} = 7.$$

Also ist $\frac{1}{4} = 7$ in $\mathbb{Z}_9$. Probe: Wenn man 4 mit 7 multipliziert, bleibt modulo 9 der Rest 1.

b) Für 0 gibt es niemals ein multiplikatives Inverses. Da $1, 2, 3, 4$ zum Modul 5 teilerfremd sind, gibt es für sie ein multiplikatives Inverses. Wir können uns also auf die Suche nach $\frac{1}{1}$, $\frac{1}{2}$, $\frac{1}{3}$, und $\frac{1}{4}$ in $\mathbb{Z}_5$ machen. Entweder wir lesen es aus der Multiplikationstabelle auf Seite 82 ab, oder wir berechnen es:

$$\frac{1}{1} = 1,\ \frac{1}{2} = \frac{1+5}{2} = 3,\ \frac{1}{3} = \frac{1+5}{3} = 2,\ \frac{1}{4} = \frac{1+3\cdot 5}{4} = 4.$$

Analog zu a) wird die Zahl 1 im Zähler so lange durch einen Vertreter aus ihrer Restklasse modulo 5 ersetzt (indem man hier sukzessive $5, 2\cdot 5, 3\cdot 5, \ldots$ addiert), bis sich der Bruch ohne Rest kürzen lässt. Es ist also 1 das multiplikative Inverse von sich selbst, ebenso ist 4 multiplikativ invers zu sich selbst. Und 3 und 2 sind multiplikativ invers zueinander.

c) Für 0 gibt es nie eines, und hier auch nicht für 2, 3 und 4, da jede dieser Zahlen einen gemeinsamen Teiler mit dem Modul 6 hat. Also gibt es nur multiplikative Inverse zu 1 und 5 (da sie zum Modul teilerfremd sind). Wir finden:

$$\frac{1}{1} = 1,\ \frac{1}{5} = \frac{1+4\cdot 6}{5} = 5.$$

Das multiplikative Inverse zu 1 ist also 1 selbst, ebenso ist das multiplikative Inverse zu 5 wieder 5 selbst. ■

Für die Berechnung des multiplikativen Inversen von $e \in \mathbb{Z}_m$ (wenn es existiert) ist es leider nicht so leicht möglich, eine allgemeine Formel anzugeben (wie für das additive Inverse in Satz 3.12). Die Umformung durch Veränderung des Zählers wie im letzten Beispiel kann auch sehr aufwändig werden, wenn m groß ist. Wir werden aber im nächsten Abschnitt einen effektiven Algorithmus, den erweiterten Euklid'schen Algorithmus, für die Berechnung des multiplikativen Inversen in $\mathbb{Z}_m$ kennen lernen.

Sie fragen sich nun bestimmt schon die ganze Zeit: Wozu brauche ich das? Nehmen wir uns wieder ein einfaches Beispiel aus der Kryptographie her: Die Verschlüsselungsvorschrift sei $y = 3x \pmod{26}$. Wie wird wieder entschlüsselt? Es wird nach x aufgelöst: $x = \frac{1}{3}y = 9y \pmod{26}$. Damit entschlüsselt werden kann ist es also unbedingt notwendig, dass der Kehrwert $\frac{1}{3} = 9$ in $\mathbb{Z}_{26}$ existiert.

Zur Berechnung von Prüfziffern oder Entschlüsselungsvorschriften müssen Gleichungen gelöst werden:

Satz 3.18 Seien a, b ganze Zahlen, m eine natürliche Zahl. Dann gilt:

a) $a + x = b \pmod{m}$ besitzt immer eine eindeutige Lösung x in $\mathbb{Z}_m$ (und unendlich viele dazu kongruente Lösungen außerhalb $\mathbb{Z}_m$). Man erhält sie, indem man auf beiden Seiten der Kongruenzgleichung das additive Inverse $-a$ von a in $\mathbb{Z}_m$ addiert:
$$x = (-a) + b \pmod{m}.$$

b) Wenn a und m teilerfremd sind, dann besitzt $a \cdot x = b \pmod{m}$ *genau eine* Lösung in $\mathbb{Z}_m$ (und unendlich viele dazu kongruente Lösungen). Man erhält sie, indem man beide Seiten der Kongruenzgleichung mit dem multiplikativen Inversen $\frac{1}{a}$ von a in $\mathbb{Z}_m$ multipliziert:
$$x = \frac{1}{a} \cdot b \pmod{m}.$$
Sind a und m jedoch nicht teilerfremd, so kann es keine oder auch mehrere Lösungen in $\mathbb{Z}_m$ geben (aber jedenfalls nicht genau eine). Wie viele Lösungen es gibt, sieht man mithilfe von $t = \mathrm{ggT}(a, m)$: Es gibt genau t Lösungen von $a \cdot x = b \pmod{m}$, falls t auch b teilt; ansonsten existiert keine Lösung.

Satz 3.18 sagt in b) also: Sind a und m nicht teilerfremd, ist also $t = \mathrm{ggT}(a, m) > 1$, so gibt es genau t Lösungen von $a \cdot x = b \pmod{m}$, falls t auch b teilt; ansonsten existiert keine Lösung. Warum? Ausgeschrieben lautet die Gleichung ja $a \cdot x = b + k \cdot m$. Gilt $a = t\tilde{a}$, $m = t\tilde{m}$, so folgt $t(\tilde{a} \cdot x - k \cdot \tilde{m}) = b$. Eine Lösung kann also nur existieren, falls $b = t\tilde{b}$. In diesem Fall können wir zunächst die eindeutige Lösung x_0 von $\tilde{a} \cdot x = \tilde{b} \pmod{\tilde{m}}$ bestimmen. Die Lösungen unserer ursprünglichen Gleichung sind dann $x_0 + j\tilde{m}$, $0 \le j < t$.

Beispiel 3.19 Gleichungen in $\mathbb{Z}_m$
Finden Sie alle $x \in \mathbb{Z}_m$, die die Gleichung lösen:
a) $4 + x = 3 \pmod{6}$ b) $5x = 2 \pmod{12}$ c) $3x = 6 \pmod{11}$
d) $2x = 3 \pmod{6}$ e) $2x = 4 \pmod{6}$

Lösung zu 3.19

a) Wir können wie gewohnt nach x auflösen, indem wir auf beiden Seiten der Kongruenzgleichung -4 addieren:
$$\underbrace{-4 + 4}_{=0} + x = -4 + 3 = -1 = 5 \pmod{6}.$$
Probe: $4 + 5 = 9 = 3 \pmod{6}$. Die eindeutige Lösung in $\mathbb{Z}_6$ ist also $x = 5$. (*Außerhalb* von $\mathbb{Z}_6$ ist jede zu $x = 5$ modulo 6 kongruente Zahl eine Lösung, zum Beispiel $11, 17, \ldots$ oder auch $-1, -7, \ldots$)

b) $a = 5$ und $m = 12$ sind teilerfremd, also gibt es $\frac{1}{5}$ in $\mathbb{Z}_{12}$. Wir multiplizieren beide Seiten der Gleichung damit, wodurch nach x aufgelöst wird und wir eine eindeutige Lösung erhalten:

$$\underbrace{\frac{1}{5} \cdot 5}_{=1} \cdot x = \frac{1}{5} \cdot 2 \,(\mathrm{mod}\, 12).$$

Da $\frac{1}{5} = \frac{1+12}{5} = \frac{1+2\cdot 12}{5} = 5$ in $\mathbb{Z}_{12}$, folgt $x = \frac{1}{5} \cdot 2 = 5 \cdot 2 = 10 \,(\mathrm{mod}\, 12)$. Probe: $5 \cdot 10 = 50 = 2 \,(\mathrm{mod}\, 12)$.

c) $a = 3$ und $m = 11$ sind teilerfremd, daher gibt es eine eindeutige Lösung:

$$x = 6 \cdot \frac{1}{3} = 2 \,(\mathrm{mod}\, 11).$$

Es war hier nicht notwendig, $\frac{1}{3} = \frac{1+11}{3} = 4$ zu berechnen, denn wir konnten $6 \cdot \frac{1}{3} = 2 \cdot 3 \cdot \frac{1}{3} = 2$ vereinfachen.

d) Da $a = 2$ und $m = 6$ nicht teilerfremd sind, gibt es keine *eindeutige* Lösung. Der größte gemeinsame Teiler von $a = 2$ und $m = 6$ ist $t = 2$. Da $t = 2$ kein Teiler von $b = 3$ ist gibt es nach Satz 3.18 keine Lösung.

e) Da nun $t = \mathrm{ggT}(2, 6) = 2$ die rechte Seite $b = 4$ teilt, gibt es nach Satz 3.18 zwei Lösungen in $\mathbb{Z}_6$. Wir finden sie durch Probieren: $x = 2$ und $x = 5$.

Falls Sie sich mit Probieren nicht zufrieden geben wollen, so gibt das Kleingedruckte nach Satz 3.18 eine Anleitung, wie die Lösungen berechnet werden können: Demnach finden wir die $t = 2$ Lösungen, indem wir zunächst $\tilde{a} \cdot x = \tilde{b} \,(\mathrm{mod}\, \tilde{m})$ lösen, also hier $x = 2 \,(\mathrm{mod}\, 3)$. Damit ist die erste Lösung gleich $x_0 = 2$ und die zweite Lösung gleich $x_0 + 1 \cdot \tilde{m} = 2 + 3 = 5$. ■

Da die Eigenschaft, ein multiplikatives Inverses zu besitzen, sehr wertvoll ist, führt man ein neues Symbol ein: Man bezeichnet mit $\mathbb{Z}_m^*$ die Menge der Zahlen aus $\mathbb{Z}_m$, für die es ein multiplikatives Inverses gibt. Das sind genau die Zahlen aus $\mathbb{Z}_m$, die zu m teilerfremd sind, also

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \mathrm{ggT}(a, m) = 1\}.$$

Wenn daher insbesondere der Modul eine Primzahl p ist, dann kann man für jede Zahl aus $\mathbb{Z}_p$ außer 0 ein Inverses bezüglich der Multiplikation finden. Dann ist also $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\}$.

Beispiel 3.20 $\mathbb{Z}_m$ **und** $\mathbb{Z}_m^*$
Geben Sie an: a) $\mathbb{Z}_4$ und $\mathbb{Z}_4^*$ b) $\mathbb{Z}_3$ und $\mathbb{Z}_3^*$

Lösung zu 3.20

a) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ sind alle möglichen Reste bei Division durch 4. Davon sind 1 und 3 teilerfremd zu 4. Also ist $\mathbb{Z}_4^* = \{1, 3\}$.

b) Es ist $\mathbb{Z}_3 = \{0, 1, 2\}$. Da 3 eine Primzahl ist, sind alle Zahlen in $\mathbb{Z}_3$ außer 0 teilerfremd zu 3, also $\mathbb{Z}_3^* = \{1, 2\}$. ■

Nun können wir auch die Frage beantworten, wann wir in einer Gleichung $a \cdot c = b \cdot c \,(\mathrm{mod}\, m)$ durch c kürzen können. Im Allgemeinen ist das nur für $c \in \mathbb{Z}_m^*$ möglich:

Satz 3.21 Ist $c \in \mathbb{Z}_m^*$, so folgt aus $a \cdot c = b \cdot c \,(\mathrm{mod}\, m)$ auch $a = b \,(\mathrm{mod}\, m)$.

Beispiel: $10 = 40 \,(\mathrm{mod}\, 6)$ kann durch 5 gekürzt werden, da $\frac{1}{5}$ in $\mathbb{Z}_6$ existiert: $2 = 8 \,(\mathrm{mod}\, 6)$. Weiter kann aber nicht gekürzt werden, da $\frac{1}{2}$ in $\mathbb{Z}_6$ nicht existiert.

Wir haben gesehen, dass man in $\mathbb{Z}_m$ so wie in $\mathbb{R}$ oder $\mathbb{Q}$ eine Addition und eine Multiplikation definieren kann. Wir haben aber auch gesehen, dass es Unterschiede gibt: In $\mathbb{R}$, $\mathbb{Q}$ oder $\mathbb{Z}_p$ (p Primzahl) gibt es ein multiplikatives Inverses für *jede* Zahl außer 0, es kann also jede Gleichung der Form $ax = b$ (eindeutig) gelöst werden. Das ist aber nicht so in $\mathbb{Z}_m$ (falls m keine Primzahl) oder in $\mathbb{Z}$. Um diese Unterschiede herauszukristallisieren und sich einen Überblick zu verschaffen, unterscheidet man allgemein verschiedene Strukturen von Mengen und ihren Verknüpfungen, von denen wir an dieser Stelle vier erwähnen möchten:

Definition 3.22 Sei G eine Menge mit einer Verknüpfung, die je zwei Elementen $a, b \in G$ ein Element $a \circ b \in G$ zuordnet. Dann wird $(G, \circ)$ eine **Gruppe** genannt, wenn folgendes gilt:

a) Es gilt $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in G$ (**Assoziativgesetz**).
b) Es gibt ein **neutrales Element** $n \in G$, das $n \circ a = a \circ n = a$ für alle $a \in G$ erfüllt.
c) Zu jedem $a \in G$ gibt es ein **inverses Element** $i(a) \in G$, das $a \circ i(a) = i(a) \circ a = n$ erfüllt.

Gilt zusätzlich

d) $a \circ b = b \circ a$ für alle $a, b \in G$ (**Kommutativgesetz**),

so spricht man von einer **kommutativen** oder **abelschen Gruppe** (benannt nach dem norwegischen Mathematiker Niels Abel, 1802–1829).

Die Anzahl der Elemente in G wird als **Ordnung** der Gruppe bezeichnet. Ist die Anzahl endlich, so spricht man von einer **endlichen Gruppe,** ansonsten von einer unendlichen Gruppe.

Man schreibt meistens nur kurz G (anstelle von $(G, \circ)$), wenn klar ist, welche Verknüpfung gemeint ist. Das neutrale Element und das inverse Element sind immer eindeutig bestimmt.

Warum? Sei n' ein weiteres neutrales Element, dann ist $n' = n \circ n' = n$. Sind b und c inverse Elemente zu a, so gilt $b = b \circ n = b \circ (a \circ c) = (b \circ a) \circ c = n \circ c = c$.

Außerdem folgt aus der Definition des Inversen sofort $i(i(a)) = a$, d.h. das Inverse des Inversen von a ist wieder a persönlich. Weiters gilt $i(a \circ b) = i(b) \circ i(a)$ (umgekehrte Reihenfolge!).

Eine Teilmenge $H \subseteq G$ heißt **Untergruppe** von G, wenn $(H, \circ)$ wieder eine Gruppe ist.

Satz 3.23 Um zu prüfen, ob $H \subseteq G$ eine Untergruppe ist, reicht es nachzuweisen, dass $n \in H$ ist und für alle $a, b \in H$ auch $a \circ b \in H$ und $i(a) \in H$ gilt.

Beispiel 3.24 Additive Gruppen

a) $(\mathbb{Z}, +)$, also die ganzen Zahlen $\mathbb{Z}$ mit der Addition, bilden eine kommutative Gruppe, denn:
   • Das Assoziativgesetz gilt: $a + (b + c) = (a + b) + c$ für alle ganzen Zahlen a, b, c.
   • Das neutrale Element bezüglich der Addition ist 0: $a + 0 = 0 + a = a$ für alle ganzen Zahlen a.
   • Zu jeder ganzen Zahl a gibt es ein Inverses $-a$ bezüglich der Addition (additives Inverses): $a + (-a) = (-a) + a = 0$.
   • Das Kommutativgesetz gilt: $a + b = b + a$ für alle ganzen Zahlen a, b.

b) Ebenso sind $(\mathbb{Z}_m, +)$ für beliebiges m, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ kommutative Gruppen.

c) Aber: $(\mathbb{N}_0, +)$ ist keine Gruppe. Assoziativgesetz, neutrales Element sind kein Problem, aber es gibt nicht für jede natürliche Zahl a ein additives Inverses. Zum Beispiel gibt es keine *natürliche* Zahl a, sodass $3 + a = 0$.

d) Die geraden Zahlen $H = \{2n \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z}$ bilden eine Untergruppe $(H, +)$ von $(\mathbb{Z}, +)$.

Als Verknüpfung kann man auch die Multiplikation wählen:

Beispiel 3.25 Multiplikative Gruppen

a) $(\mathbb{Q}\backslash\{0\}, \cdot)$, also die rationalen Zahlen $\mathbb{Q}$ ohne 0 mit der Multiplikation, bilden eine kommutative Gruppe, denn:
   • Das Assoziativgesetz gilt: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle rationalen Zahlen $a, b, c \neq 0$.
   • Das neutrale Element bezüglich der Multiplikation ist 1: $a \cdot 1 = 1 \cdot a = a$ für alle rationalen Zahlen $a \neq 0$.
   • Zu jeder rationalen Zahl $a \neq 0$ gibt es ein Inverses bezüglich der Multiplikation (multiplikatives Inverses) $\frac{1}{a}$: $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$.
   • Das Kommutativgesetz gilt: $a \cdot b = b \cdot a$ für alle rationalen Zahlen $a, b \neq 0$.

b) Ebenso sind $(\mathbb{Z}_p\backslash\{0\}, \cdot)$ (wobei p Primzahl), $(\mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{C}\backslash\{0\}, \cdot)$ kommutative Gruppen.

c) Aber: $(\mathbb{N}, \cdot)$ und auch $(\mathbb{Z}\backslash\{0\}, \cdot)$ sind keine Gruppen. Wieder sind Assoziativgesetz, neutrales Element kein Problem, aber es scheitert wieder am Inversen: In $\mathbb{Z}\backslash\{0\}$ gibt es nicht für jedes a ein multiplikatives Inverses. Zum Beispiel gibt es keine *ganze Zahl* a, sodass $3 \cdot a = 1$.

Aus diesen letzten Beispielen sehen wir, dass die reellen Zahlen sowohl bezüglich $+$ als auch (wenn man die 0 herausnimmt) bezüglich $\cdot$ eine kommutative Gruppe bilden. Dasselbe gilt für $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ oder $\mathbb{Z}_p$. Daher haben diese Mengen bezüglich Addition und Multiplikation dieselbe Struktur, es gelten also dieselben Rechenregeln! Man nennt diese Struktur einen Körper:

Definition 3.26 Eine Menge $\mathbb{K}$ mit zwei Verknüpfungen $+$ und $\cdot$, geschrieben $(\mathbb{K}, +, \cdot)$, heißt **Körper** (engl. *field*), wenn folgendes gilt:

a) $(\mathbb{K}, +)$ ist eine kommutative Gruppe mit neutralem Element 0.

b) $(\mathbb{K}\backslash\{0\}, \cdot)$ ist eine kommutative Gruppe mit neutralem Element 1.
c) Für alle $a, b, c \in \mathbb{K}$ gilt: $a \cdot b + a \cdot c = a \cdot (b + c)$ (**Distributivgesetz**).

(Das Distributivgesetz regelt, wie die beiden Verknüpfungen sich miteinander „vertragen".)

Wieder schreibt man nur kurz $\mathbb{K}$ (anstelle von $(\mathbb{K}, +, \cdot)$), wenn klar ist, welche Verknüpfungen gemeint sind.

Beispiel 3.27 Körper
a) Für eine Primzahl p ist $\mathbb{Z}_p$ ein Körper. Ebenso sind $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$ Körper.
b) Jedoch ist $\mathbb{Z}$ kein Körper, denn $(\mathbb{Z}\backslash\{0\}, \cdot)$ ist, wie wir in Beispiel 3.25 c) überlegt haben, keine Gruppe.

Hat nicht jedes Element ein multiplikatives Inverses, so wie z. B. in $\mathbb{Z}_m$, so spricht man von einem Ring:

Definition 3.28 Eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, geschrieben $(R, +, \cdot)$, heißt **Ring**, wenn folgendes gilt:

a) $(R, +)$ ist eine kommutative Gruppe mit neutralem Element 0.
b) Für alle $a, b, c \in R$ gilt: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (**Assoziativgesetz**).
c) Für alle $a, b, c \in R$ gilt: $a \cdot b + a \cdot c = a \cdot (b + c)$ (**Distributivgesetz**).

Gilt zusätzlich

d) das **Kommutativgesetz** $a \cdot b = b \cdot a$ für alle $a, b \in R$, so spricht man von einem kommutativen Ring, und wenn darüber hinaus
e) ein **neutrales Element** 1 **für die Multiplikation** existiert, also $a \cdot 1 = 1 \cdot a = a$ für alle $a \in R$,

so spricht man von einem **kommutativen Ring mit Eins**.

Wenn also jedes Element (außer der 0) eines kommutativen Ringes mit Eins ein multiplikatives Inverses besitzt, dann ist der Ring ein Körper. Wieder schreibt man kurz R (anstelle $(R, +, \cdot)$), wenn kein Zweifel besteht, welche Verknüpfungen gemeint sind.

Beispiel 3.29 Ringe
a) Die ganzen Zahlen $\mathbb{Z}$ sind ein kommutativer Ring mit Eins; kein Körper, da es nicht zu jeder ganzen Zahl ein Inverses bezüglich der Multiplikation gibt (der Kehrwert ist ja im Allgemeinen keine ganze Zahl).
b) $\mathbb{Z}_m$ ist ein kommutativer Ring mit Eins; er ist genau dann ein Körper, wenn $m = p$ eine Primzahl ist. So sind also z. B. $\mathbb{Z}_4$ oder $\mathbb{Z}_{256}$ nur Ringe, $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$ hingegen Körper.
c) Die Menge der Polynome $\mathbb{R}[x] = \{p(x) = p_n x^n + \cdots + p_1 x + p_0 \mid p_k \in \mathbb{R}\}$ ist ein kommutativer Ring mit Eins, aber kein Körper.

Denn: Die Addition und Multiplikation von Polynomen $p(x)+q(x)$ bzw. $p(x)\cdot q(x)$ erben das Kommutativ-, Assoziativ- und Distributivgesetz von den reellen Zahlen; neutrales Element

bezüglich der Addition von Polynomen ist das Nullpolynom $p(x) = 0$; neutrales Element bezüglich der Multiplikation ist das konstante Polynom $p(x) = 1$; es gibt für jedes Polynom $p(x)$ ein Inverses bezüglich der Addition, nämlich $-p(x)$; es gibt aber nicht zu jedem Polynom ein Inverses bezüglich der Multiplikation: Zum Beispiel gibt es zu $p(x) = x^2$ keines, denn für kein Polynom $q(x)$ ist $x^2 \cdot q(x) = 1$ (das wäre $q(x) = \frac{1}{x^2}$, das ist aber kein Polynom). $\mathbb{R}[x]$ ist daher kein Körper.

d) Allgemein ist die Menge der Polynome $\mathbb{K}[x] = \{p(x) = p_n x^n + \cdots + p_1 x + p_0 \mid p_k \in \mathbb{K}\}$ mit Koeffizienten aus einem Körper $\mathbb{K}$ ein kommutativer Ring mit Eins, aber kein Körper. Zum Beispiel sind $\mathbb{C}[x]$ oder $\mathbb{Z}_2[x]$ Ringe, aber keine Körper. Die Menge $\mathbb{K}[x]$ wird als der **Polynomring** über $\mathbb{K}$ bezeichnet.

Die Menge aller geraden Zahlen hat eine wichtige Eigenschaft: Die Summe zweier gerader Zahlen ist gerade und die Multiplikation einer beliebigen Zahl mit einer geraden Zahl ist ebenfalls gerade. Teilmengen eines Rings mit dieser Eigenschaft haben einen eigenen Namen:

Definition 3.30 Eine Teilmenge I eines Rings R heißt **Ideal**, wenn gilt:

a) Es ist $0 \in I$ und für alle $a, b \in I$ sind $a + b \in I$ und $-a \in I$.
b) Für alle $a \in I$ und $b \in R$ sind $a \cdot b \in I$ und $b \cdot a \in I$.

Ein Ideal $I \subseteq R$ ist also nach Satz 3.23 eine Untergruppe bezüglich der Addition und jedes Vielfache eines Elementes aus I liegt wieder in I.

Beispiel 3.31 Ideale
a) Alle geraden Zahlen bilden ein Ideal in $\mathbb{Z}$.
b) Alle Polynome $p(x)$, für die $p(0) = 0$ ist, bilden ein Ideal in $\mathbb{R}[x]$.

Diese Überlegungen und Definitionen erscheinen Ihnen vielleicht auf den ersten Blick als abstrakt und nutzlos. Es trifft aber das Gegenteil zu! Sie bilden die Basis für viele Anwendungen in der Kryptographie und der Codierungstheorie und sind damit von fundamentaler Bedeutung für die Informatik.

Nach diesem kurzen Ausflug in die **Zahlentheorie**, die sich mit den Eigenschaften der ganzen Zahlen beschäftigt, möchten wir noch einen kleinen Überblick über einige wichtige Teilgebiete der Mathematik geben: Die **Algebra** untersucht Gruppen, Ringe und Körper, im Gegensatz zur **Analysis**, die sich mit Differential- und Integralrechnung beschäftigt. Die **lineare Algebra** untersucht Vektorräume (z. B. $\mathbb{R}^n$) und verschmilzt im unendlichdimensionalen Fall von Funktionenräumen mit der Analysis zur **Funktionalanalysis**. Die **algebraische Geometrie** verwendet kommutative Ringe, um geometrische Objekte (also Kurven, Flächen, etc.) mit algebraischen Methoden zu untersuchen.

Die Menge aller Funktionen (mit bestimmten Eigenschaften), die auf einem geometrischen Objekt definiert sind, bilden nämlich auch einen Ring, der wichtige Informationen über die Geometrie enthält.

Untersucht man geometrische Objekte mit den Methoden der Analysis, so ist man in der **Differentialgeometrie**. Die **diskrete Mathematik**, einer unserer Schwerpunkte, befasst sich mit mathematischen Strukturen, die endlich oder abzählbar

sind. Sie ist ein junges Gebiet mit vielen Bezügen zur Informatik, da Computer von Natur aus diskret sind.

3.2.1 Anwendung: Welche Fehler erkennen Prüfziffern?

Im letzten Abschnitt haben wir gesehen, wie modulare Arithmetik für Prüfziffern verwendet werden kann. Eine gute Prüfziffer sollte die häufigsten Fehler erkennen, und das sind:

- Eingabe einer falschen Ziffer („Einzelfehler“)
- Vertauschung zweier Ziffern („Vertauschungsfehler“)

Wir wollen nun eine gute Prüfziffer konstruieren: Angenommen, die mit einer Prüfziffer zu versehende Ziffernfolge hat n Stellen, $x_1 \ldots x_n$. Ein allgemeiner Ansatz für die Prüfziffer wäre

$$P(x_1 \ldots x_n) = \sum_{j=1}^{n} g_j x_j \bmod q = g_1 x_1 + \ldots + g_n x_n \bmod q.$$

Dabei sind die Zahlen $g_j \in \mathbb{Z}_q$ beliebige Gewichte, die noch geeignet zu bestimmen sind. Welchen Wert soll der Modul q haben? Die Größe von q legt unseren Vorrat an Ziffern fest: $x_j \in \{0, 1, \ldots, q-1\} = \mathbb{Z}_q$.

Ist zum Beispiel $q = 9$, so könnten wir nur die Ziffern $\{0, 1, \ldots, 8\}$ verwenden. Denn würden wir bei $q = 9$ zum Beispiel auch die Ziffer 9 zulassen, so könnte zwischen den Ziffern 0 und 9 nicht unterschieden werden, da $9 = 0 \pmod 9$. Eine falsche Eingabe von 9 statt 0 würde von der Prüfziffer also nicht erkannt werden.

Wenn wir also jedenfalls die Ziffern $0, 1, \ldots, 9$ verwenden möchten, so muss q zumindest gleich 10 sein.

Überlegen wir als Nächstes, welche Eigenschaften die Prüfziffer haben muss, damit sie Einzel- bzw. Vertauschungsfehler immer erkennt. Beginnen wir mit dem Einzelfehler. Nehmen wir an, es wird anstelle von $x_1 \ldots x_n$ die Ziffernfolge $y_1 \ldots y_n$ eingegeben, wobei ein Fehler in der k-ten Stelle aufgetreten ist. Das heißt, es gilt $x_j = y_j$ für alle $j \neq k$ und $x_k \neq y_k$. Dann ist die Differenz der Prüfziffern

$$P(x_1 \ldots x_n) - P(y_1 \ldots y_n) = g_k(x_k - y_k) \bmod q.$$

Der Fehler wird erkannt, wenn die Differenz der Prüfziffern ungleich 0 ist. Damit ein Einzelfehler also immer erkannt wird, darf diese Differenz nur dann gleich 0 (modulo q) sein, wenn $x_k = y_k$. Die Gleichung $g_k(x_k - y_k) = 0 \pmod q$ muss also eine eindeutige Lösung, nämlich $x_k - y_k = 0 \pmod q$ haben. Nach Satz 3.18 b) ist das genau dann der Fall, wenn $g_k \in \mathbb{Z}_q^*$ (d.h., wenn g_k ein multiplikatives Inverses besitzt).

Kommen wir nun zur Erkennung von Vertauschungsfehlern: Nehmen wir an, es wird anstelle von $x_1 \ldots x_n$ die Ziffernfolge $y_1 \ldots y_n$ eingegeben, wobei die j-te und die k-te Stelle vertauscht wurden. Dann ist die Differenz der Prüfziffern

$$P(x_1 \ldots x_n) - P(y_1 \ldots y_n) = g_j x_j + g_k x_k - g_j x_k - g_k x_j = (g_j - g_k)(x_j - x_k) \bmod q.$$

Analog wie zuvor muss $g_j - g_k \in \mathbb{Z}_q^*$ gelten, damit der Fehler immer erkannt wird.

Satz 3.32 (Erkennung von Einzel- und Vertauschungsfehlern) Sei

$$P(x_1 \dots x_n) = \sum_{j=1}^{n} g_j x_j \bmod q$$

eine Prüfziffer für eine Ziffernfolge $x_1 \dots x_n$ mit Ziffern $x_j \in \mathbb{Z}_q$. Dann erkennt P genau dann alle Einzelfehler an der Stelle k, wenn $g_k \in \mathbb{Z}_q^*$, und genau dann alle Vertauschungsfehler an den Stellen j und k, wenn $(g_j - g_k) \in \mathbb{Z}_q^*$.

Eine besonders gute Wahl für q ist also eine Primzahl, denn dann ist $\mathbb{Z}_q^*$ besonders groß!

Leider ergibt sich nun ein kleines Dilemma: Wählen wir $q = 10$, so stehen für die Gewichte die Zahlen in $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ zur Verfügung, wenn alle Einzelfehler erkannt werden sollen. Da die Differenz zweier ungerader Zahlen aber gerade ist, können dann nicht mehr *alle* Vertauschungsfehler erkannt werden. Wählen wir $q = 11$ (Primzahl), so lassen sich die Bedingungen für die Erkennung aller Vertauschungs- und Einzelfehler erfüllen, aber dafür kann die Prüfziffer auch den Wert 10 haben, ist also nicht immer eine einstellige Dezimalziffer.

Zum Abschluss eine kleine Auswahl an Prüfzifferverfahren:

- Auf vielen Artikeln findet sich ein Strichcode bzw. die zugehörige 13-stellige oder 8-stellige Ziffernfolge, die **Europäische Artikelnummer (EAN)**. Mithilfe von Scannern wird der Strichcode an Computerkassen eingelesen. Bei der 13-stelligen Nummer *abcd efgh ikmn p* geben die beiden ersten Ziffern das Herkunftsland an, die folgenden 5 Ziffern stehen für den Hersteller, und die nächsten 5 Ziffern für das Produkt. Die letzte Ziffer p ist eine Prüfziffer, die

  $$a + 3b + c + 3d + e + 3f + g + 3h + i + 3k + m + 3n + p = 0 \bmod 10.$$

  erfüllt. Es werden alle Einzelfehler erkannt (da die Gewichte 1 bzw. 3 aus $\mathbb{Z}_{10}^*$ sind), aber nicht alle Vertauschungsfehler.
- Bei Banken wird das **Einheitliche Kontonummernsystem (EKONS)** verwendet. Die Kontonummern sind maximal zehnstellig: Die ersten (maximal 4) Ziffern stehen für die Klassifikation der Konten und die restlichen 6 Ziffern bilden die eigentliche Kontonummer, wobei die letzte Ziffer eine Prüfziffer ist. Es sind bei verschiedenen Banken verschiedene Prüfzifferverfahren üblich. Die Prüfziffer p der Kontonummer *abcd efghi p* berechnet sich zum Beispiel nach der Vorschrift

  $$2i + h + 2g + f + 2e + d + 2c + b + 2a + p = 0 \bmod 10.$$

  Es werden nicht alle Einzelfehler erkannt (da das Gewicht 2 nicht in $\mathbb{Z}_{10}^*$ liegt), aber alle Vertauschungsfehler benachbarter Ziffern, da die Differenz der zugehörigen Gewichte, 1, in $\mathbb{Z}_{10}^*$ liegt.
- Die zehnstellige **Internationale Standard-Buchnummer (ISBN)** hat die Form *a bcd efghi p*. Dabei ist a das Herkunftsland, *bcd* kennzeichnet den Verlag und p ist die Prüfziffer, die

  $$10a + 9b + 8c + 7d + 6e + 5f + 4g + 3h + 2i + p = 0 \bmod 11$$

erfüllt. Anstelle von 10 wird das Symbol X verwendet. Da alle Gewichte und auch die Differenzen von je zwei Gewichten in $\mathbb{Z}_{11}^*$ liegen, werden alle Einzelfehler und alle Vertauschungsfehler erkannt.

Beispiel 3.33 Prüfziffer

a) Anstelle der EAN 72*cd efgh ikmn p* wird die EAN 27*cd efgh ikmn p* eingegeben, es wurden also die ersten beiden Ziffern vertauscht. Erkennt die Prüfziffer diesen Fehler?

b) Anstelle der EAN 26*cd efgh ikmn p* wird nun die EAN 62*cd efgh ikmn p* eingegeben, es wurden also wieder die ersten beiden Ziffern vertauscht. Erkennt die Prüfziffer diesen Fehler?

Lösung zu 3.33

a) Um uns auf das Wesentliche konzentrieren zu können, betrachten wir nur den Beitrag der ersten beiden Stellen zur Prüfziffer (die weiteren Stellen sind in beiden EANs gleich und geben daher den gleichen Beitrag zur Prüfziffer). In der ersten EAN erhalten wir aus den ersten beiden Stellen

$$1 \cdot 7 + 3 \cdot 2 = 13 = 3 \bmod 10,$$

und bei der zweiten EAN ergibt sich ebenfalls

$$1 \cdot 2 + 3 \cdot 7 = 23 = 3 \bmod 10.$$

Dieser Vertauschungsfehler wird also nicht erkannt.

b) In der ersten EAN erhalten wir nun aus den ersten beiden Stellen

$$1 \cdot 6 + 3 \cdot 2 = 12 = 2 \bmod 10,$$

die zweite EAN liefert

$$1 \cdot 2 + 3 \cdot 6 = 20 = 0 \bmod 10.$$

Dieser Vertauschungsfehler wird also erkannt. ■

3.3 Der Euklid'sche Algorithmus und diophantische Gleichungen

Das multiplikative Inverse in $\mathbb{Z}_m$ kann für kleines m leicht durch Probieren gefunden werden. In praktischen Anwendungen, z. B. in der Kryptographie, hat man es aber oft mit großen Zahlen zu tun und benötigt daher ein besseres Verfahren. Wir beginnen mit einem effektiven Verfahren für die Bestimmung des größten gemeinsamen Teilers und werden sehen, dass wir damit gleichzeitig auch den gewünschten Algorithmus für das multiplikative Inverse erhalten.

Die einfachste Möglichkeit, um zum Beispiel den $\mathrm{ggT}(217, 63)$ zu finden, ist alle Zahlen von 1 bis 63 durchzuprobieren. Das ist allerdings ein sehr mühsames Verfahren und bereits der griechische Mathematiker Euklid (ca. 300 v. Chr.) hatte eine bessere Idee:

Dividieren wir zunächst 217, die größere der beiden Zahlen, durch 63, die kleinere der beiden:

$$217 = 3 \cdot 63 + 28.$$

Jeder gemeinsame Teiler von 217 und 63 muss auch $28 = 217 - 3 \cdot 63$ teilen.

Denn wenn t ein gemeinsamer Teiler von 217 und 63 ist, also $217 = kt$ und $63 = nt$, so folgt: $28 = 217 - 3 \cdot 63 = kt - 3 \cdot nt = t(k - 3n)$, also ist t auch ein Teiler von 28.

Analog muss jeder gemeinsame Teiler von 63 und 28 auch ein Teiler von $217 = 3 \cdot 63 + 28$ sein. Daher ist insbesondere der größte gemeinsame Teiler von 217 und 63 gleich dem größten gemeinsamen Teiler von 63 und 28. Das Problem, den $\mathrm{ggT}(217, 63)$ zu finden, reduziert sich also auf das Problem, den $\mathrm{ggT}(63, 28)$ zu finden! Als nächstes dividieren wir daher 63 durch 28,

$$63 = 2 \cdot 28 + 7.$$

Mit derselben Überlegung wie oben folgt, dass $\mathrm{ggT}(63, 28) = \mathrm{ggT}(28, 7)$. Wir dividieren nun nochmal:

$$28 = 4 \cdot 7 + 0.$$

Da 7 ein Teiler von 28 ist, ist $\mathrm{ggT}(28, 7) = 7$, und damit ist $7 = \mathrm{ggT}(28, 7) = \mathrm{ggT}(63, 28) = \mathrm{ggT}(217, 63)$ und das Problem ist gelöst!

Euklid hat den Algorithmus in seinem Werk, den *Elementen* beschrieben. Die *Elemente* bestehen aus 13 Bänden, ein Teil davon sind Euklids eigene Arbeiten, der Rest ist eine Sammlung des mathematischen Wissens der damaligen Zeit. Die *Elemente* sind eines der erfolgreichsten Lehrwerke aller Zeiten und waren bis ins 19. Jahrhundert das meistverkaufte Werk nach der Bibel.

Satz 3.34 (Euklid'scher Algorithmus) Die natürlichen Zahlen a, b seien gegeben. Setzt man $r_0 = a$, $r_1 = b$ und definiert man rekursiv r_k als Rest der Division von r_{k-2} durch r_{k-1},

$$r_k = r_{k-2} \bmod r_{k-1} \qquad (\text{also } r_{k-2} = q_k r_{k-1} + r_k),$$

so bricht diese Rekursion irgendwann ab, d.h. $r_{n+1} = 0$, und es gilt $r_n = \mathrm{ggT}(a, b)$. Der letzte nichtverschwindende Rest ist also der größte gemeinsame Teiler.

Für Informatiker ist es immer wichtig sicherzustellen, dass ein Algorithmus wohl irgendwann abbricht. Hier ist das leicht zu sehen, da $r_1 = b$ ist und r_k in jedem Schritt abnimmt. Daher ist nach spätestens b Schritten Schluss.

Es ist übrigens sinnvoll (aber nicht notwendig), $a > b$ zu wählen. Tut man das nicht, so tauschen im ersten Schritt des Algorithmus a und b Platz, man muss also einen Schritt mehr im Vergleich zum Fall $a > b$ ausführen.

Beispiel 3.35 (→CAS) Euklid'scher Algorithmus
Bestimmen Sie den $\mathrm{ggT}(75, 38)$.

Lösung zu 3.35 Wir setzen $r_0 = 75$ (die größere der beiden Zahlen) und $r_1 = 38$ und dividieren:

$$\begin{aligned} 75 &= 1 \cdot 38 + 37, \qquad (\text{also } q_2 = 1, r_2 = 37) \\ 38 &= 1 \cdot 37 + 1, \qquad (\text{also } q_3 = 1, r_3 = 1) \\ 37 &= 37 \cdot 1 + 0 \end{aligned}$$

Der letzte Rest ungleich 0 ist $r_3 = 1 = \mathrm{ggT}(75, 38)$. Die beiden Zahlen sind also teilerfremd. ■

Eine Erweiterung des Euklid'schen Algorithmus zeigt uns, wie eine ganzzahlige Lösung einer Gleichung der Form $ax + by = \mathrm{ggT}(a, b)$ gefunden werden kann. Eine Gleichung, bei der nur *ganzzahlige* Lösungen gesucht werden, bezeichnet man als **diophantische Gleichung**, benannt nach dem griechischen Mathematiker Diophant von Alexandrien (ca. 250 v. Chr.).

Die wohl bekannteste diophantische Gleichung ist $x^n + y^n = z^n$. Der Fall $n = 2$ entspricht dem Satz von Pythagoras und eine Lösung ist zum Beispiel $x = 3$, $y = 4$ und $z = 5$: $3^2 + 4^2 = 5^2$. Der französische Mathematiker Fermat (1607–1665) hat die Behauptung aufgestellt, dass diese Gleichung für natürliches $n > 2$ keine Lösungen mit ganzzahligen x, y und z besitzt; dass es also z. B. keine ganzen Zahlen x, y, z gibt, die $x^3 + y^3 = z^3$ erfüllen. Fermat ist auf diese Vermutung beim Studium eines Bandes von Diophants Lehrwerk, der *Arithmetica* gekommen, und hat am Rand einer Seite vermerkt: „Ich habe hierfür einen wahrhaft wunderbaren Beweis, doch ist dieser Rand hier zu schmal, um ihn zu fassen." Diese Notiz hat Generationen von Mathematikern und Mathematik-Begeisterten den Schlaf geraubt, und für den Beweis von Fermats Behauptung wurden viele Preise ausgesetzt. Er wurde erst 1995 erbracht und umfasst Hunderte von Seiten ... Mehr zur spannenden Geschichte von „Fermats letzter Satz" finden Sie im gleichnamigen Buch von S. Singh [43].

Wo treten Situationen auf, wo nur ganzzahlige Lösungen gebraucht werden? Ein Beispiel: Eine Firma erzeugt zwei Produkte A und B, für die 75 bzw. 38 kg eines bestimmten Rohstoffes benötigt werden. Wie viele Stücke von A bzw. B sollen erzeugt werden, wenn 10 000 kg Rohstoff vorhanden sind und der gesamte Rohstoff verbraucht werden soll? Wenn x die Stückzahl von Produkt A und y die Stückzahl von Produkt B bedeutet, dann suchen wir hier also nichtnegative ganze Zahlen x und y, mit

$$75x + 38y = 10\,000.$$

Wesentliche Zutaten, die wir für die Lösung dieses Problems brauchen, finden sich im folgenden Ergebnis, mit dem man beliebige Gleichungen der Form $ax + by = c$ im Griff hat:

Satz 3.36 (Erweiterter Euklid'scher Algorithmus) Gegeben ist die Gleichung

$$ax + by = \mathrm{ggT}(a, b)$$

mit beliebigen natürlichen Zahlen a und b. Eine ganzzahlige Lösung x, y kann mithilfe des erweiterten Euklid'schen Algorithmus rekursiv berechnet werden. Dazu wird der Euklid'sche Algorithmus wie in Satz 3.34 beschrieben durchgeführt, zusätzlich werden noch in jedem Schritt Zahlen x_k und y_k berechnet, mit den Anfangswerten $x_0 = 1$, $y_0 = 0$, $x_1 = 0$, $y_1 = 1$:

$$\begin{aligned} r_k &= r_{k-2} \bmod r_{k-1}, \quad q_k = r_{k-2} \operatorname{div} r_{k-1}, \qquad (\text{also } r_{k-2} = q_k r_{k-1} + r_k) \\ x_k &= x_{k-2} - q_k x_{k-1}, \quad y_k = y_{k-2} - q_k y_{k-1}. \end{aligned}$$

Die Abbruchbedingung ist wieder $r_{n+1} = 0$. Für $r_n = \text{ggT}(a, b)$ und das zugehörige x_n bzw. y_n gilt dann: $x_n a + y_n b = \text{ggT}(a, b)$. Daher haben wir mit $x = x_n$ und $y = y_n$ eine Lösung der gegebenen diophantischen Gleichung gefunden.

Die Idee ist hier, r_k in der Form $r_k = x_k a + y_k b$ zu schreiben. Für $k = 0, 1$ ist das leicht; wegen $r_0 = a$ bzw. $r_1 = b$ brauchen wir nur $x_0 = 1$, $y_0 = 0$ bzw. $x_1 = 0$, $y_1 = 1$ zu wählen. Also können wir Induktion versuchen. Dazu müssen wir nur noch die Formel für r_k zeigen und können voraussetzen, dass sie für r_{k-1} und r_{k-2} gilt: $r_k = r_{k-2} - q_k r_{k-1} = (x_{k-2}a + y_{k-2}b) - q_k(x_{k-1}a + y_{k-1}b) = (x_{k-2} - q_k x_{k-1})a + (y_{k-2} - q_k y_{k-1})b = x_k a + y_k b$.

Daraus folgt sofort: Wenn x, y die Gleichung $ax + by = \text{ggT}(a, b)$ löst, so löst nx, ny die Gleichung $a(nx) + b(ny) = n \cdot \text{ggT}(a, b)$. Mehr noch, die Gleichung $ax + by = c$ hat *genau dann* ganzzahlige Lösungen, wenn $c = n \cdot \text{ggT}(a, b)$, also wenn „die rechte Seite" c ein Vielfaches des $\text{ggT}(a, b)$ ist.

Denn: Existiert eine ganzzahlige Lösung, so ist $\text{ggT}(a, b)$ ein Teiler der linken Seite $ax + by$, muss also auch ein Teiler der rechten Seite c sein.

Beispiel 3.37 (→CAS) Erweiterter Euklid'scher Algorithmus
a) Finden Sie eine ganzzahlige Lösung x, y von

$$75x + 38y = 1.$$

b) Finden Sie eine ganzzahlige Lösung von

$$75x + 38y = 10000.$$

c) Besitzt die Gleichung $217x + 63y = 10$ eine ganzzahlige Lösung?

Lösung zu 3.37

a) Wir führen den Euklid'schen Algorithmus wie in Beispiel 3.35 durch und berechnen zusätzlich in jedem Schritt die x_k und y_k, wie im Satz 3.36 beschrieben (Startwerte $x_0 = 1$, $y_0 = 0$, $x_1 = 0$, $y_1 = 1$):

$$\begin{aligned} 75 &= 1 \cdot 38 + 37, && x_2 = 1 - 1 \cdot 0 = 1, \quad y_2 = 0 - 1 \cdot 1 = -1 \\ 38 &= 1 \cdot 37 + 1, && x_3 = 0 - 1 \cdot 1 = -1, y_3 = 1 - 1 \cdot (-1) = 2 \\ 37 &= 37 \cdot 1 \end{aligned}$$

Der letzte Rest ungleich 0 ist $r_3 = 1 = \text{ggT}(75, 38)$. Damit ist $x = x_3 = -1$ und $y = y_3 = 2$ eine Lösung der Gleichung. Probe: $75 \cdot (-1) + 38 \cdot 2 = 1$.

b) Da $x = -1$ und $y = 2$ eine Lösung von $75x + 38y = 1$, ist $x = -10000$ und $y = 20000$ eine Lösung von $75x + 38y = 10000$.

c) Wir wissen aus Beispiel 3.35, dass $\text{ggT}(217, 63) = 7$ ist. Da nun 10 kein Vielfaches von 7 ist, gibt es keine ganzzahlige Lösung. ■

Nun haben wir mit $x = -10000$ und $y = 20000$ zwar eine Lösung von $75x + 38y = 10000$, aber ein Problem, wenn wir x und y als Stückzahlen interpretieren möchten! Dafür können wir nämlich nur nichtnegative Werte für x und y brauchen. Gibt es noch weitere Lösungen von $75x + 38y = 10000$? Ja! Hier alles zusammengefasst:

Satz 3.38 (Lösung einer diophantischen Gleichung) Die diophantische Gleichung

$$ax + by = c$$

hat genau dann eine ganzzahlige Lösung, wenn c ein Vielfaches des größten gemeinsamen Teilers von a und b ist, also $c = n \cdot \mathrm{ggT}(a, b)$ mit $n \in \mathbb{Z}$.

Ist x_0, y_0 eine ganzzahlige Lösung von $ax_0 + by_0 = \mathrm{ggT}(a, b)$ (gefunden zum Beispiel mithilfe von Satz 3.36), so ist $x = nx_0$, $y = ny_0$ eine ganzzahlige Lösung von $ax+by = n\cdot\mathrm{ggT}(a, b)$. Alle weiteren ganzzahligen Lösungen von $ax+by = n\cdot\mathrm{ggT}(a, b)$ sind gegeben durch

$$\tilde{x} = x + \frac{kb}{\mathrm{ggT}(a, b)}, \qquad \tilde{y} = y - \frac{ka}{\mathrm{ggT}(a, b)}$$

mit einer beliebigen ganzen Zahl k.

Man kann sich durch Einsetzen leicht davon überzeugen, dass mit x, y auch $\tilde{x} = x + k\frac{b}{\mathrm{ggT}(a,b)}$, $\tilde{y} = y - k\frac{a}{\mathrm{ggT}(a,b)}$ eine Lösung ist. Umgekehrt muss jede Lösung auch so aussehen. Denn ist $\tilde{x}$, $\tilde{y}$ irgendeine weitere Lösung, also $\tilde{x}a+\tilde{y}b = n\cdot\mathrm{ggT}(a, b)$, so erhält man durch Subtraktion der beiden Gleichungen $(\tilde{x} - x)a = (y - \tilde{y})b$. Kürzt man durch $\mathrm{ggT}(a, b)$, so erhält man $(\tilde{x} - x)\tilde{a} = (y - \tilde{y})\tilde{b}$ mit $\tilde{a} = \frac{a}{\mathrm{ggT}(a,b)}$ und $\tilde{b} = \frac{b}{\mathrm{ggT}(a,b)}$. Da keiner der Primfaktoren von $\tilde{a}$ in $\tilde{b}$ steckt, müssen alle in $(y - \tilde{y})$ stecken, also ist $y - \tilde{y}$ ein Vielfaches von $\tilde{a}$. Analog ist $\tilde{x} - x$ ein Vielfaches von $\tilde{b}$.

Nun haben wir alle Zutaten, um unser Rohstoffproblem endgültig zu lösen:

Beispiel 3.39 Diophantische Gleichung
Finden Sie nichtnegative ganze Zahlen x und y mit

$$75x + 38y = 10000.$$

Lösung zu 3.39 Wir kennen aus Beispiel 3.37 bereits eine Lösung $x = -10000$ und $y = 20000$. Mithilfe von Satz 3.38 erhalten wir nun weitere ganzzahlige Lösungen $\tilde{x} = -10000 + k \cdot 38$ und $\tilde{y} = 20000 - k \cdot 75$ für beliebiges $k \in \mathbb{Z}$.

Nun suchen wir ein k so, dass $\tilde{x}$ und $\tilde{y}$ nichtnegativ sind: Aus der Bedingung $\tilde{x} \geq 0$ folgt, dass dieses $k \geq \frac{10000}{38} = 263.158$ sein muss, und aus $\tilde{y} \geq 0$ folgt $k \leq \frac{20000}{75} = 266.\overline{6}$. Dies trifft für $k = 264, 265$ oder 266 zu. Mit jedem dieser k's erhalten wir also wie gewünscht nichtnegative Lösungen. Zum Beispiel ergeben sich für $k = 264$ die Stückzahlen $\tilde{x} = 32$ und $\tilde{y} = 200$. Probe: $75 \cdot 32 + 200 \cdot 38 = 10000$. ■

Der erweiterte Euklid'sche Algorithmus kann nun auch verwendet werden, um das multiplikative Inverse einer Zahl e modulo m zu berechnen:

Satz 3.40 (Berechnung des multiplikativen Inversen) Seien e und m teilerfremd. Dann ist die Lösung $x \in \mathbb{Z}_m$ der diophantischen Gleichung

$$e\,x + m\,y = 1$$

(die zum Beispiel mit dem erweiterten Euklid'schen Algorithmus berechnet wird), das multiplikative Inverse $\frac{1}{e}$ in $\mathbb{Z}_m$.

Falls der erweiterte Euklid'sche Algorithmus ein x liefert, das nicht in $\mathbb{Z}_m$ liegt, so muss also noch der Rest von x modulo m aufgesucht werden. Der zweite Teil der Lösung (y), die der erweiterte Euklid'sche Algorithmus liefert, ist für die Berechnung des multiplikativen Inversen uninteressant.

Warum ist x das gesuchte multiplikative Inverse? Nun, x erfüllt ja $e\,x + m\,y = 1$, oder etwas umgeformt: $e\,x = 1 - m\,y$. Das bedeutet aber, dass sich $e\,x$ und 1 nur um ein Vielfaches von m unterscheiden, und das bedeutet nichts anderes als $e\,x = 1 \pmod m$.

Beispiel 3.41 (→CAS) Multiplikatives Inverses und Euklid'scher Algorithmus
Finden Sie das multiplikative Inverse von 75 modulo 38.

Lösung zu 3.41 Da $e = 75$ und $m = 38$ teilerfremd sind, gibt es ein multiplikatives Inverses zu e. Betrachten wir die diophantische Gleichung $75\,x + 38\,y = 1$. Aus Beispiel 3.39 wissen wir, dass $x = -1$ und $y = 2$ eine Lösung ist. Wir interessieren uns nur für $x = -1$ und suchen seinen Rest modulo 38: $x = -1 = 37 \pmod{38}$. Damit ist 37 das gesuchte multiplikative Inverse zu 75 in $\mathbb{Z}_{38}$, d.h. $\frac{1}{75} = 37$ in $\mathbb{Z}_{38}$. Probe: $75 \cdot 37 = 2775 = 1 \pmod{38}$. ■

3.3.1 Anwendung: Der RSA-Verschlüsselungsalgorithmus

Die Cäsarverschiebung aus Beispiel 3.14 ist das klassische Beispiel eines konventionellen, so genannten **symmetrischen Verschlüsselungsalgorithmus**: Sowohl dem Sender als auch dem Empfänger der geheimen Nachricht ist der Schlüssel e bekannt (und damit auch der zweite Schlüssel d, der sich leicht aus e berechnen lässt). Das bedeutet aber, dass der geheime Schlüssel e zwischen Sender und Empfänger zunächst ausgetauscht werden muss, bevor verschlüsselt werden kann. Steht nun für diesen Austausch kein sicherer Weg zur Verfügung, sondern nur ein öffentliches Medium wie z. B. das Internet, dann wird eine sichere Schlüsselvereinbarung zwischen Sender und Empfänger ein Problem.

Eine Alternative bieten so genannte **asymmetrische** oder **Public Key Verschlüsselungsverfahren**. Hier besitzt jeder Teilnehmer zwei Schlüssel: einen **privaten Schlüssel** (**private key**), den er geheim hält, und einen **öffentlichen Schlüssel** (**public key**), der aller Welt bekannt gegeben wird (wie eine Telefonnummer in einem Telefonbuch).

Wenn Sie mir nun eine geheime Nachricht senden möchten, schlagen Sie einfach im entsprechenden öffentlichen Verzeichnis meinen öffentlichen Schlüssel e (*encrypt* = engl. *verschlüsseln*) nach, verschlüsseln damit die Nachricht und senden sie dann z. B. als Email an mich. Da nur ich den zugehörigen geheimen Schlüssel d (*decrypt* = engl. *entschlüsseln*) kenne, bin nur ich in der Lage, dieses Email wieder zu entschlüsseln.

Nun liegt es aber in der Natur der Sache, dass der Zusammenhang zwischen der originalen und der verschlüsselten Nachricht eindeutig sein muss, und daraus kann man ableiten, dass auch der geheime Schlüssel d prinzipiell aus dem öffentlichen Schlüssel e berechenbar sein muss. Es scheint also, dass es ein solches Verschlüsselungsverfahren nicht geben kann. *Theoretisch* ist das auch so. *Praktisch* aber reicht

es schon aus, wenn die Berechnung von d aus e einfach so langwierig ist, dass man sie auch mit den schnellsten Computern nicht innerhalb praktischer Zeitgrenzen durchführen kann. Das lässt sich mit einer so genannten **Einwegfunktion** realisieren: Sie kann in eine Richtung ($x \mapsto y = f(x)$, also Ermittlung des Funktionswertes zu gegebenem x) leicht berechnet werden, in die andere Richtung ($y = f(x) \mapsto x$) praktisch nicht.

Ein Beispiel für eine Einwegfunktion ist die Zuordnung Name $x \mapsto$ Telefonnummer $f(x)$ in einem Telefonbuch. Die eine Richtung ist kein Problem, nämlich zu einem gegebenen Namen die zugehörige Telefonnummer zu finden. Die umgekehrte Richtung, also zu einer gegebenen Telefonnummer den zugehörigen Namen zu finden, dauert dagegen um ein Vielfaches länger!

Wo soll man aber eine solche Funktion hernehmen? Dazu hatten die Mathematiker Ronald Rivest und Adi Shamir und der Computerwissenschaftler Leonard Adleman im Jahr 1978 die zündende Idee: Die Einwegeigenschaft des nach ihnen benannten RSA-Verschlüsselungsalgorithmus beruht darauf, dass die *Multiplikation* von Primzahlen fast keine Rechenzeit in Anspruch nimmt, während aber die *Zerlegung* einer gegebenen Zahl in ihre Primfaktoren im Vergleich dazu um ein Vielfaches länger benötigt!

Hier nun der **RSA-Algorithmus**, der die eingangs geforderten Eigenschaften besitzt:

a) **Schlüsselerzeugung**: Möchten Sie verschlüsselte Nachrichten empfangen, so erzeugen Sie folgendermaßen einen öffentlichen und einen privaten Schlüssel:
   - Wählen Sie zwei verschiedene Primzahlen p, q.
   - Bilden Sie daraus die Zahlen $n = p\,q$ und $m = (p-1)(q-1)$.
   - Wählen Sie eine Zahl e, die teilerfremd zu m ist.
   - Berechnen Sie die Zahl d, die $e\,d = 1 (\mathrm{mod}\, m)$ erfüllt (also das multiplikative Inverse von e modulo m).
   - Geben Sie die Zahlen (n, e) als öffentlichen Schlüssel bekannt. Die Zahlen (n, d) behalten Sie als geheimen Schlüssel. p, q und m werden nicht mehr benötigt (bleiben aber geheim!).

b) **Verschlüsselung**: Wenn Ihnen nun jemand eine verschlüsselte Nachricht schicken möchte, so schlägt er Ihren öffentlichen Schlüssel (n, e) nach, verschlüsselt den Klartext x gemäß
$$y = x^e \ (\mathrm{mod}\, n),$$
und schickt den Geheimtext y an Sie.

   Die Verschlüsselungsvorschrift ist dabei eine Abbildung von $\mathbb{Z}_n$ nach $\mathbb{Z}_n$ und die Entschlüsselungsvorschrift ist die zugehörige Umkehrabbildung. Insbesondere muss also die Nachricht zuvor in eine Zahl kleiner als n umgewandelt werden (bzw. in eine Anzahl von Blöcken, die kleiner als n sind).

c) **Entschlüsselung**: Zum Entschlüsseln verwenden Sie Ihren geheimen Schlüssel (n, d) und berechnen damit den Klartext gemäß
$$x = y^d \ (\mathrm{mod}\, n).$$

Dass wirklich $y^d = (x^e)^d = x^{ed} (\mathrm{mod}\, n) = x$ gilt, ist an dieser Stelle noch nicht unmittelbar einsichtig, kann aber mithilfe eines Satzes des französischen Mathematikers Fermat (siehe Satz 3.43) bewiesen werden.

Natürlich ist es prinzipiell möglich, den geheimen Schlüssel (n, d) aus Kenntnis des öffentlichen Schlüssels (n, e) zu berechnen, indem man die Gleichung

$$e\,d = 1 \pmod{m}$$

löst. Da aber $m = (p-1)(q-1)$ geheim ist, muss man zur Ermittlung von m zuerst die Primfaktoren p und q von n bestimmen. Sind die beiden Primfaktoren geeignet gewählt (insbesondere genügend groß), so wird aber auch der heutzutage schnellste Computer das Zeitliche segnen, bevor er mit der Primfaktorzerlegung fertig ist. Die Sicherheit des RSA-Algorithmus hängt also von der verwendeten Schlüssellänge ab (die der Größe der Primzahlen entspricht). Das bedeutet natürlich, dass eine Schlüssellänge, die heute als sicher gilt, aufgrund der steigenden Rechnerleistung in einigen Jahren schon nicht mehr sicher ist!

Außerdem wäre es möglich, dass jemand einen schnelleren Algorithmus (der polynomial von der Größe der Zahl n abhängt) zur Primfaktorzerlegung findet, und in diesem Fall wäre die Sicherheit des RSA-Algorithmus endgültig dahin. Mathematiker versuchen deshalb zu beweisen, dass es einen solchen Algorithmus nicht geben kann.

Nun gleich zu einem Beispiel:

Beispiel 3.42 (→CAS) Verschlüsselung mit dem RSA-Algorithmus
Die Nachricht „KLEOPATRA" soll mit dem RSA-Algorithmus verschlüsselt an einen Empfänger geschickt werden, dessen öffentlicher Schlüssel $(n, e) = (1147, 29)$ ist. Wandeln Sie zuvor die Nachricht so wie in Beispiel 3.14 in Ziffern um.
a) Wie lautet der Geheimtext?
b) Entschlüsseln Sie den Geheimtext $(d = 149)$.
c) Versuchen Sie, den geheimen Schlüssel (n, d) aus der Kenntnis des öffentlichen Schlüssels (n, e) zu berechnen.

Lösung zu 3.42

a) In Zahlen lautet KLEOPATRA: $10, 11, 4, 14, 15, 0, 19, 17, 0$. Verschlüsseln wir jede dieser Zahlen x gemäß $y = x^{29} \pmod{1147}$:

x	10	11	4	14	15	0	19	17	0
$y = x^{29} \pmod{1147}$	803	730	132	547	277	0	979	42	0

Wir erhalten die verschlüsselte Nachricht: $803, 730, 132, 547, 277, 0, 979, 42, 0$.

b) Der Empfänger kann mit der Vorschrift $x = y^{149} \pmod{1147}$ entschlüsseln:

y	803	730	132	547	277	0	979	42	0
$x = y^{149} \pmod{1147}$	10	11	4	14	15	0	19	17	0

c) d ist eine Lösung der Gleichung $e\,d = 1 \pmod{m}$. e ist öffentlich bekannt, für die Berechnung von $m = (p-1)(q-1)$ benötigt man aber die Primfaktoren p und q von n (das auch bekannt ist). In der Praxis sollte die Primfaktorzerlegung innerhalb praktischer Zeitgrenzen nicht berechenbar sein, in unserem Beispiel sind die Primzahlen aber so klein, dass jeder Computer die Zerlegung ohne Mühe schafft: $1147 = 31 \cdot 37$, also $p = 31$ und $q = 37$. Damit können wir m berechnen: $m = (31-1)(37-1) = 1080$. Der geheime Schlüssel d ist nun eine Lösung der Gleichung $e\,d = 1 \pmod{m}$. Sie kann mit dem erweiterten Euklid'schen Algorithmus (siehe Satz 3.36) berechnet werden: $d = 149$.

■

Unser Beispiel hat – abgesehen von den zu kleinen Primzahlen – noch eine weitere Schwachstelle: Da jeder Buchstabe einzeln und immer auf dieselbe Weise verschlüsselt wird (**monoalphabetische Verschlüsselung**), kann der Code bei längeren Nachrichten mit statistischen Methoden gebrochen werden. Dabei verwendet man die Tatsache, dass die einzelnen Buchstaben in einem durchschnittlichen Text mit bestimmten Häufigkeiten vorkommen. Zum Beispiel kommt in einem deutschen Text im Schnitt der Buchstabe „e“ am häufigsten vor; das legt die Vermutung nahe, dass der häufigste Geheimtextbuchstabe zu „e“ zu entschlüsseln ist. Dieser Angriff kann verhindert werden, indem man mehrere Buchstaben zu Blöcken zusammenfasst und verschlüsselt.

In der Praxis ist der RSA-Algorithmus meist zu aufwändig zu berechnen und wird daher nur zum Austausch des geheimen Schlüssels eines konventionellen Verschlüsselungsalgorithmus verwendet. Die Verschlüsselung selbst geschieht dann mit dem schnelleren konventionellen Algorithmus. Diese Vorgangsweise wird als **Hybridverfahren** bezeichnet.

Eine wichtige Eigenschaft des RSA-Algorithmus ist die Symmetrie zwischen dem geheimen Schlüssel d und dem öffentlichen Schlüssel e. Sie bedeutet, dass ich umgekehrt mit meinem geheimen Schlüssel Datensätze verschlüsseln kann, die dann jeder mit meinem öffentlichen Schlüssel entschlüsseln kann. Diese Vorgangsweise wird für die **Digitale Signatur** und zur **Authentifizierung** angewendet. Eine digitale Signatur mit RSA besteht im Wesentlichen aus folgenden Schritten:

a) **Signatur**: Um das Dokument x digital zu signieren gehe ich wie folgt vor:
   - Ich verschlüssle x mit meinem geheimen Schlüssel:
   $$s = x^d \pmod{n}.$$
   (In der Praxis wird nicht x, sondern der digitale Fingerabdruck von x (d.h. der Hashwert von x unter einer kryptographischen Hashfunktion) signiert, damit die Signatur keine zu große Datenmenge darstellt.)
   - Ich gebe das unverschlüsselte Dokument x und die Signatur s öffentlich bekannt.

b) **Prüfung der Signatur**: Wenn Sie die Gültigkeit der Signatur („Echtheit der Unterschrift“) prüfen möchten, so:
   - Schlagen Sie meinen öffentlichen Schlüssel (n, e) nach.
   - Berechnen Sie
   $$x' = s^e \pmod{n}.$$
   - Vergleichen Sie, ob $x = x'$. Wenn das der Fall ist, dann können Sie sicher sein, dass das Dokument *von mir* signiert wurde (denn nur ich kenne den geheimen Schlüssel) und dass das Dokument *nicht verändert* wurde (denn Sie haben den Vergleich mit dem Klartext).

Die Authentifizierung mit RSA läuft im Wesentlichen so ab (auch hier ist in der Praxis wieder eine kryptographische Hashfunktion im Spiel):

a) **Aufforderung zur Authentifizierung**: Sie möchten, dass ich mich authentifiziere. Dazu:
   - Wählen Sie einen zufälligen Text x.
   - Verschlüsseln Sie x mit meinem öffentlichen Schlüssel:
   $$y = x^e \pmod{n}.$$

- Schicken Sie y mit der Bitte um Authentifizierung an mich.

b) **Authentifizierung**: Um meine Identität zu beweisen, wende ich meinen geheimen Schlüssel auf y an und erhalte damit x,

$$x = y^d \pmod{n},$$

das ich an Sie zurück schicke. Da nur ich (als Besitzer des geheimen Schlüssels) in der Lage bin, x zu berechnen, haben Sie die Gewissheit, mit mir zu kommunizieren.

Zum Abschluss wollen wir noch hinter die Kulissen des RSA-Algorithmus blicken. Die mathematische Grundlage dazu ist der kleine Satz von Fermat:

Satz 3.43 (Fermat) Sei p eine Primzahl. Für jede Zahl x, die teilerfremd zu p ist, gilt

$$x^{p-1} = 1 \pmod{p}.$$

Der Beweis ist etwas trickreich, aber auch nicht schwer: Sei x teilerfremd zu p und y das multiplikative Inverse von x in $\mathbb{Z}_p$. Betrachten wir die Abbildung $f : \mathbb{Z}_p \to \mathbb{Z}_p$, die gegeben ist durch $f(a) = x \cdot a \pmod{p}$. Diese Abbildung ist umkehrbar, denn durch Multiplikation mit y erhält man wieder a zurück: $b = x \cdot a \pmod{p} \Leftrightarrow a = y \cdot b \pmod{p}$. Jedes $a \in \mathbb{Z}_p$ wird durch f also auf genau ein $b \in \mathbb{Z}_p$ abgebildet. Also sind die Zahlen $x, 2x, \ldots, (p-1)x$ bis auf die Reihenfolge gleich den Zahlen $1, 2, \ldots, (p-1)$. Wenn wir diese Zahlen multiplizieren, so kommt es dabei auf die Reihenfolge nicht an, daher

$$x \cdot 2x \cdot 3x \cdot \ldots \cdot (p-1)x = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}.$$

Die linke Seite umgeformt liefert

$$x^{p-1} \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}.$$

Multiplizieren wir nun der Reihe nach mit den multiplikativen Inversen von $2, 3, \ldots, p-1$ so bleibt am Ende $x^{p-1} = 1 \pmod{p}$ übrig.

Nun wollen wir die Gültigkeit des RSA-Algorithmus mithilfe des kleinen Satzes von Fermat zeigen. Wir wählen die Zahlen $n = p\,q$, $m = (p-1)(q-1)$, e und d wie auf Seite 100 beschrieben und erinnern uns an die Vorschrift zum Verschlüsseln:

$$y = x^e \pmod{n}.$$

Wir wollen nun nachweisen, dass mit $y^d = x \pmod{n}$ entschlüsselt wird. Wegen $e\,d = 1 \pmod{m}$ wissen wir, dass $e\,d = 1 + km$ für irgendein $k \in \mathbb{N}_0$, und damit erhalten wir

$$y^d = (x^e)^d = x^{ed} = x^{1+km} \pmod{n}.$$

Wenn wir also $x^{1+km} = x \pmod{n}$ zeigen können, dann sind wir fertig. Nun gilt:

$$x^{1+\ell(p-1)} = x \pmod{p}$$

für beliebiges $\ell \in \mathbb{N}_0$.

Denn: $x^{1+\ell(p-1)} = x(x^{p-1})^\ell \pmod{p}$; sind x und p teilerfremd, so folgt $x^{p-1} = 1 \pmod{p}$ aus dem kleinen Satz von Fermat und daher $x^{1+\ell(p-1)} = x \cdot 1^\ell = x \pmod{p}$; sind x und p nicht teilerfremd, so ist x ein Vielfaches von p, also $x = 0 \pmod{p}$, d.h. beide Seiten sind 0 modulo p.

Speziell für $\ell = k(q-1)$ folgt also

$$x^{1+km} = x^{1+k(q-1)(p-1)} = x^{1+\ell(p-1)} = x \pmod{p}.$$

Analog erhalten wir $x^{1+km} = x \pmod{q}$. Also ist einerseits $x^{1+km} = x + k_1 p$ und andererseits $x^{1+km} = x + k_2 q$ für irgendwelche $k_1, k_2 \in \mathbb{N}_0$. Das bedeutet, dass $x^{1+km} - x$ sowohl durch p als auch durch q teilbar ist. Da p und q verschiedene Primzahlen sind, muss $x^{1+km} - x = k_3 pq$ gelten (für irgendein $k_3 \in \mathbb{N}_0$), und bringt man x wieder auf die rechte Seite, so ist das gerade die gesuchte Gleichung $y^d = x \pmod{n}$.

In vielen Texten über den RSA-Algorithmus wird der Satz von Euler und die Euler'sche φ-Funktion verwendet. Deshalb wollen wir kurz den Zusammenhang herstellen: Die **Euler'sche φ-Funktion** $\varphi(n)$ ist nichts anderes als die Anzahl der Elemente von $\mathbb{Z}_n^*$. Der **Satz von Euler** besagt nun, dass

$$x^{\varphi(n)} = 1 \pmod{n} \quad \text{für alle } x \in \mathbb{Z}_n^*.$$

Falls $n = p$ eine Primzahl ist, so gilt $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ und es gibt für alle Zahlen außer 0 ein Inverses bezüglich der Multiplikation. Insbesondere gilt $\varphi(p) = p - 1$. Der kleine Satz von Fermat ist also ein Spezialfall des Satzes von Euler. Beim RSA-Algorithmus ist $n = p\,q$ das Produkt von zwei verschiedenen Primzahlen, und es gibt für jede Zahl außer der Vielfachen von q (d.h. $q, 2q, \ldots, (p-1)q$), der Vielfachen von p $(p, 2p, \ldots, (q-1)p)$ und 0 ein Inverses bezüglich der Multiplikation. In diesem Fall gilt also $\varphi(n) = pq - (p-1) - (q-1) - 1 = (p-1)(q-1) = m$ und unsere Gleichung $y^d = x^{1+km} = x \pmod{n}$ ist ebenfalls ein Spezialfall des Satzes von Euler.

3.4 Der Chinesische Restsatz

Im 1. Jahrhundert v. Chr. stellte der chinesische Mathematiker Sun-Tsu folgendes Rätsel: „Ich kenne eine Zahl. Wenn man sie durch 3 dividiert, bleibt der Rest 2; wenn man sie durch 5 dividiert, bleibt der Rest 3; wenn man sie durch 7 dividiert, bleibt der Rest 2. Wie lautet die Zahl?" In unserer Schreibweise ist eine Zahl x gesucht, die die Kongruenzen $x = 2 \pmod{3}$, $x = 3 \pmod{5}$, $x = 2 \pmod{7}$ *gleichzeitig* löst.

Viele Anwendungen führen auf mehrere Kongruenzen, die gleichzeitig gelöst werden sollen. Man spricht von einem **System von Kongruenzen**. Wann ein solches System lösbar ist, sagt uns das folgende hinreichende (aber nicht notwendige) Kriterium:

Satz 3.44 (Chinesischer Restsatz) Sind $m_1, \ldots, m_n$ paarweise teilerfremde ganze Zahlen, dann hat das System von Kongruenzen

$$\begin{aligned} x &= a_1 \pmod{m_1} \\ &\vdots \\ x &= a_n \pmod{m_n} \end{aligned}$$

eine eindeutige Lösung $x \in \mathbb{Z}_m$, wobei $m = m_1 \cdot \ldots \cdot m_n$ das Produkt der einzelnen Module ist.

Die Lösung lässt sich auch leicht explizit konstruieren:

a) Wir berechnen die Zahlen $M_k = \frac{m}{m_k}$, das ist also jeweils das Produkt aller Module außer m_k.

b) Nun berechnen wir für jedes M_k das multiplikative Inverse $N_k \in \mathbb{Z}_{m_k}$.
c) Dann ist

$$x = \sum_{k=1}^{n} a_k M_k N_k = a_1 \cdot M_1 \cdot N_1 + \ldots + a_n \cdot M_n \cdot N_n$$

eine Lösung des Systems von Kongruenzen; wir müssen gegebenenfalls nur noch den dazu kongruenten Rest in $\mathbb{Z}_m$ berechnen.

Achtung: Der Chinesische Restsatz hilft nur, wenn die Module teilerfremd sind. Sind sie nicht teilerfremd, so kann das System keine oder mehrere Lösungen in $\mathbb{Z}_m$ haben.

Beispiel: $x = 1 \pmod 2$ und $x = 2 \pmod 4$ hat keine Lösung. Das kann man so überlegen: Wenn $x \in \mathbb{Z}$ eine Lösung von $x = 1 \pmod 2$ und $x = 2 \pmod 4$ wäre, so müsste $x = 1 + 2m$ und $x = 2 + 4n$ für irgendwelche ganzen Zahlen $m, n \in \mathbb{Z}$ gelten. Ziehen wir beide Darstellungen voneinander ab, so erhalten wir $1 = 2(2n - m)$, und das ist unmöglich!

Nun können wir das Rätsel von Sun-Tsu lösen:

Beispiel 3.45 (→CAS) Chinesischer Restsatz
Lösen Sie das System von Kongruenzen

$$\begin{aligned} x &= 2 \pmod 3 \\ x &= 3 \pmod 5 \\ x &= 2 \pmod 7. \end{aligned}$$

Lösung zu 3.45 Da die Module 3, 5, 7 Primzahlen sind, sind sie insbesondere paarweise teilerfremd. Das Produkt der Module ist $m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$. Es gibt also eine eindeutige Lösung x mit $0 \leq x < 105$, und jede weitere Zahl aus der Restklasse von x modulo 105 löst das System. Konstruktion der Lösung:
a) Wir berechnen $M_1 = m_2 \cdot m_3 = 5 \cdot 7 = 35$, $M_2 = m_1 \cdot m_3 = 3 \cdot 7 = 21$, $M_3 = m_1 \cdot m_2 = 3 \cdot 5 = 15$.
b) Berechnung der multiplikativen Inversen von M_1, M_2, M_3 modulo m_1, m_2 bzw. m_3: Das multiplikative Inverse von $M_1 = 35$ modulo $m_1 = 3$ erfüllt $35 \cdot N_1 = 1 (\mathrm{mod}\, 3)$ oder, wenn wir anstelle 35 einen kleineren Vertreter von 35 aus derselben Restklasse modulo 3 nehmen (damit wir das multiplikative Inverse besser finden können), $2 \cdot N_1 = 1 (\mathrm{mod}\, 3)$. Nun können wir leicht ablesen, dass $N_1 = 2$ ist. Analog berechnen wir das multiplikative Inverse $N_2 = 1$ zu $M_2 = 21$ modulo $m_2 = 5$ und das multiplikative Inverse $N_3 = 1$ zu $M_3 = 15$ modulo 7.
c) Damit berechnen wir $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 = 23 \pmod{105}$. Die gesuchte Lösung in $\mathbb{Z}_{105}$ ist also 23. ■

Eine „praktisch“ wichtige Anwendung des Chinesischen Restsatzes sind Kartentricks: Sie denken an irgendeine Karte (insgesamt 20 Karten). Ich lege die Karten der Reihe nach (sichtbar) auf 5 Stapel (nach dem letzten beginne ich wieder beim ersten). Sie sagen mir, in welchem Stapel die Karte liegt. Wir wiederholen das mit 4 Stapeln, und ich sage Ihnen dann, an welche Karte Sie gedacht haben.

3.4.1 Anwendung: Rechnen mit großen Zahlen

Zum Abschluss möchte ich Ihnen noch zeigen, wie man den Chinesischen Restsatz verwenden kann, um **mit großen Zahlen zu rechnen**. Dies kommt zum Beispiel in der Kryptographie (RSA-Algorithmus) zur Anwendung, wo mit großen Zahlen (mehr als 200 Stellen) gerechnet wird. Dabei ermöglicht die Verwendung des Chinesischen Restsatzes eine Beschleunigung um das mehr als 3-fache:

Bekanntlich können Computer ja nur natürliche Zahlen mit einer maximalen Größe verarbeiten, zum Beispiel $2^{32}-1$, wenn 32-Bit zur Verfügung stehen. Wie rechnet man nun aber mit Zahlen, die größer sind?

Eine einfache Lösung zu diesem Problem ist, eine Zahl in diesem Fall in zwei 16-Bit Blöcke zu zerlegen, und mit den einzelnen Blöcken zu rechnen. Wir betrachten einfachheitshalber nur zwei Blöcke, das Verfahren kann aber leicht auf beliebig viele Blöcke erweitert werden.

Warum 16-Bit, und nicht 32-Bit-Blöcke? Weil ansonsten das Produkt zweier Blöcke nicht in die 32-Bit passen würde, die zur Verfügung stehen.

Bei der Addition zweier Zahlen $x = 2^{16}x_1 + x_0$ und $y = 2^{16}y_1 + y_0$ müssen nur die Blöcke addiert werden: $x + y = 2^{16}p_1 + p_0$, wobei $p_0 = (x_0 + y_0) \bmod 2^{16}$ und $p_1 = (x_1 + y_1 + o_0) \bmod 2^{16}$ (wobei o_0 der eventuelle Überlauf aus der Addition von x_0 und y_0 ist).

Im Dezimalsystem überlegt: Angenommen, es stehen 6 Stellen zur Verfügung, und wir zerlegen eine Zahl in zwei dreistellige Blöcke, z. B. die Zahl $513\,489 = 513 \cdot 10^3 + 489 = x_1 \cdot 10^3 + x_0$ in die zwei Blöcke 513 und 489. Der erste Block $x_1 = 513$ gehört also hier zur Potenz 10^3, der zweite $x_0 = 489$ zur Potenz $10^0 = 1$. Haben wir eine zweite Zahl, z. B. $120\,721 = 120 \cdot 10^3 + 721 = y_1 \cdot 10^3 + y_0$, so ist die Summe der beiden Zahlen gleich $634 \cdot 10^3 + 210$. Hier ist 210 der Rest $(x_0 + y_0) \bmod 10^3 = (489 + 721) \bmod 10^3$, es bleibt der Überlauf 1 und $634 = x_1 + y_1 + o_0 = 513 + 120 + 1$.

Die Multiplikation ist schon aufwändiger: Es gilt $xy = 2^{48}q_3 + 2^{32}q_2 + 2^{16}q_1 + q_0$ mit $q_0 = (x_0y_0) \bmod 2^{16}$ und $q_1 = (x_1y_0 + x_0y_1 + o_0) \bmod 2^{16}$ wobei $o_0 = x_0y_0/2^{16}$ (ganzzahlige Division ohne Rest) ein eventueller Überlauf ist. Weiters ist $q_2 = (x_1y_1 + o_1) \bmod 2^{16}$ und $q_3 = x_1y_1/2^{16} + o_2$, wobei o_j der eventuelle Überlauf aus der Berechnung des j-ten Blocks ist. Die beiden letzten Blöcke q_2 und q_3 sollten allerdings gleich null sein, wenn zur Speicherung des Ergebnisses nur zwei Blöcke zur Verfügung stehen.
Das ist schon recht umständlich und wird natürlich bei noch mehr Blöcken noch umständlicher. Außerdem kann man sich überlegen, dass die Anzahl der notwendigen Multiplikationen quadratisch mit der Anzahl der Blöcke steigt.

Hier also der Alternativvorschlag mithilfe des Chinesischen Restsatzes: Wenn $m_1, m_2, \ldots, m_n$ paarweise teilerfremd sind, und $m = m_1 \cdots m_n$ bedeutet, so kann jede Zahl x mit $0 \le x < m$ eindeutig durch ihre Reste x_k modulo der m_k, $k = 1, \ldots, n$ repräsentiert werden:

$$x = (x_1, \ldots, x_n).$$

Beispiel: $m_1 = 9$, $m_2 = 8$. Dann ist etwa $39 = (3, 7)$, denn $39 = 3 \pmod 9$ und $39 = 7 \pmod 8$. Umgekehrt kann zu jedem Tupel sofort mithilfe des Chinesischen Restsatzes wieder die Zahl rekonstruiert werden. So erhält man $x = 39$ als eindeutige Lösung von

$$\begin{aligned} x &= 3 \,(\mathrm{mod}\, 9) \\ x &= 7 \,(\mathrm{mod}\, 8). \end{aligned}$$

Mit dieser Darstellung werden Addition und Multiplikation einfach (Satz 3.4): Sind $x = (x_1, \ldots, x_n)$ und $y = (y_1, \ldots, y_n)$ zwei Zahlen, so ist ihre Summe

$$x + y = ((x_1 + y_1) \bmod m_1, \ldots, (x_n + y_n) \bmod m_n)$$

und ihr Produkt

$$x \cdot y = ((x_1 y_1) \bmod m_1, \ldots, (x_n y_n) \bmod m_n)$$

(siehe Übungsaufgabe 8). Wir erhalten also die Reste der Summe durch Addition der Reste in $\mathbb{Z}_{m_k}$ und die Reste des Produktes durch Multiplikation der Reste in $\mathbb{Z}_{m_k}$. Insbesondere ist nun beim Produkt die Anzahl der notwendigen Multiplikationen gleich der Anzahl der Blöcke (und nicht quadratisch in der Anzahl der Blöcke wie zuvor). Außerdem können die einzelnen Reste getrennt berechnet werden, dieses Verfahren lässt sich somit gut auf Parallelrechnern umsetzen.

In der Praxis verwendet man für die Module m_k Zahlen der Form $2^\ell - 1$, da sich die modulare Arithmetik für diese Zahlen binär leicht implementieren lässt.

3.4.2 Anwendung: Verteilte Geheimnisse

Mit dem Chinesischen Restsatz lässt sich ein Geheimnis (z. B. ein Zugangscode oder Schlüssel) auf mehrere Personen verteilen. Auf diese Weise kennt jede der beteiligten Personen (aus Sicherheitsgründen) nur einen Teil des Geheimnisses.

Angenommen, Sie möchten ein Geheimnis, das als eine natürliche Zahl x gegeben ist, auf n Personen verteilen. Dann können Sie einfach n paarweise teilerfremde natürliche Zahlen $m_1, \ldots, m_n$ (mit $m_1 \cdots m_n > x$) wählen und jeder Person den Rest der Division von x durch ein m_k, also $a_k = x \bmod m_k$ $(k = 1, \ldots, n)$, mitteilen. Alle n Personen zusammen können dann x mithilfe des Chinesischen Restsatzes bestimmen und somit das Geheimnis rekonstruieren.

Was ist nun, wenn nur ein Teil der Personen verfügbar ist? Können wir ein Geheimnis auch so verteilen, dass r Personen ausreichen um das Geheimnis zu rekonstruieren (mit einem zuvor festgelegten $r \leq n$), nicht aber weniger Personen? Auch das ist möglich: Nach dem Chinesischen Restsatz reicht ja bereits ein Teil der Reste a_k aus um x eindeutig zu rekonstruieren, wenn nur das Produkt der zugehörigen Module größer als x ist. Damit *jedes* Produkt aus r Modulen (ausgewählt aus den n Modulen) größer als x ist, muss das Produkt der *kleinsten* r Module diese Bedingung erfüllen. Wenn die Module geordnet sind, $m_1 < m_2 < \cdots < m_n$, so muss also $x < m_1 \cdots m_r$ gelten, damit beliebige r Personen (unter den n Besitzern der Teilgeheimnisse) das Geheimnis rekonstruieren können. Damit auf der anderen Seite aber *weniger* als r Personen das Geheimnis nicht rekonstruieren können, muss x grösser oder gleich als das Produkt von $r-1$ oder weniger Modulen sein (ausgewählt aus den n Modulen). Diese Bedingung ist erfüllt, wenn $x \geq m_{n-r+2} \cdots m_n$ gilt (das ist das Produkt der größten $r-1$ Module).

In der Praxis ist das Geheimnis s als eine Zahl mit einer maximalen Größe m gegeben (z. B. der geheime Schlüssel eines Verschlüsselungsalgorithmus), also $s \in$

$\mathbb{Z}_m$. Da s beliebig klein sein kann, ersetzen wir s durch $x = m_{n-r+2} \cdots m_n + s$, damit obige Bedingungen erfüllt werden können. Dann ist klar, dass $m_{n-r+2} \cdots m_n \leq x$ gilt. Damit auch $x < m_1 \cdots m_r$ erfüllt ist muss $m_1 \cdots m_r - m_{n-r+2} \cdots m_n \geq m$. In diesem Fall können wir $a_k = x \bmod m_k$ verteilen. Aus r Geheimnissen kann dann x mithilfe des Chinesischen Restsatzes berechnet werden und das Geheimnis folgt aus $s = x - m_{n-r+2} \cdots m_n$.

Beispiel 3.46 Verteilte Geheimnisse
Das Geheimnis $s = 9 \in \mathbb{Z}_{16}$ soll unter 5 Vorstandsmitgliedern aufgeteilt werden. Für die Rekonstruktion des Geheimnisses sollen zumindest 3 der Vorstandsmitglieder notwendig sein.

Lösung zu 3.46 Wir versuchen es mit den Modulen $3, 5, 7, 8, 11$ und prüfen, ob die obigen beiden Bedingungen erfüllt sind: Es gilt $m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$ und $m_4 \cdot m_5 = 8 \cdot 11 = 88$. Wegen $105 - 88 = 17 \geq 16$ geht unsere Wahl in Ordnung. Wir berechnen $x = 88 + 9 = 97$ und verteilen die Teilgeheimnisse $a_1 = 97 \bmod 3 = 1$, $a_2 = 97 \bmod 5 = 2$, $a_3 = 97 \bmod 7 = 6$, $a_4 = 97 \bmod 8 = 1$, $a_5 = 97 \bmod 11 = 9$.

Nun reichen drei der Teilgeheimnisse a_1, a_2, a_3, a_4, a_5 aus, um mithilfe des Chinesischen Restsatzes x und damit $s = x - 88$ zu rekonstruieren. ■

Unser Verfahren hat einen praktischen Schönheitsfehler. Es ist in Beispiel 3.46 kein Zufall, dass das fünfte Teilgeheimnis a_5 gleich dem Geheimnis $s = 9$ ist! Das liegt daran, dass $a_5 = x \bmod 11 = (8 \cdot 11 + 9) \bmod 11 = 9 = s$ ist, da $s = 9 < 11 = m_5$. Um das zu verhindern müsste s größer als der größte Modul, also $s > m_n$ sein.

Auf der anderen Seite sollte aber $s < m_1$ sein, denn sonst könnten bekannte Teilgeheimnisse einen Angriff zumindest erleichtern: Wären im letzten Beispiel etwa a_2 und a_4 bekannt, so bräuchte man nur noch die $m_1 = 3$ Möglichkeiten für die zugehörigen Reste a_1 durchzuprobieren. Deshalb muss m_1 groß sein und insbesondere größer als s, damit das Durchprobieren aller möglichen a_1 zumindest genauso lange dauert wie das Durchprobieren aller möglichen s. Beide Forderungen, $s < m_1$ und $s > m_n$ lassen sich aber nur schwer unter einen Hut bringen.

Aus diesem Grund verwendet man folgendes modifizierte Verfahren (**Asmuth-Bloom Schema**), das hier nur kurz erwähnt sein soll: Um ein Geheimnis $s \in \mathbb{Z}_m$ zu verteilen, wählt man paarweise teilerfremde Zahlen $m < m_1 < m_2 < \cdots < m_n$ mit $m \cdot m_{n-r+2} \cdots m_n < m_1 \cdots m_r$. Nun wird zu s irgendein zufälliges Vielfaches $t \cdot m$ addiert (wobei t geheim bleibt — da es zur Rekonstruktion nicht benötigt wird, kann es nach dem Verteilen vernichtet werden), sodass $x = s + t \cdot m < m_1 \cdots m_r$ erfüllt ist und $a_k = x \bmod m_k$ wird verteilt. Aus r Geheimnissen kann dann x mithilfe des Chinesischen Restsatzes berechnet werden und das Geheimnis folgt aus $s = x \bmod m$.

Ist das verwendete t bekannt, so reicht ein Teilgeheimnis aus, um $s = a_k - t \cdot m \bmod m_k$ zu berechnen. Daher muss t geheim gehalten werden.

Die Bedingung $m \cdot m_{n-r+2} \cdots m_n < m_1 \cdots m_r$ bedeutet, dass das Verhältnis aus dem Produkt der kleinsten r Module und dem Produkt der größten $r-1$ Module größer als m ist. Damit kann man zeigen, dass auch bei Kenntnis beliebiger $r-1$ Teilgeheimnisse keinerlei Möglichkeiten für s ausgeschlossen werden können. Das Asmuth-Bloom Schema wird deshalb als **perfekt** bezeichnet.

3.5 Mit dem digitalen Rechenmeister

Rest modulo m

Der Rest von a modulo m wird mit `Mod[a,m]` berechnet:

```
In[1]:= Mod[17,5]
Out[1]= 2
```

Multiplikatives Inverses

Das multiplikative Inverse $\frac{1}{e}$ in $\mathbb{Z}_m$ kann mit `PowerMod[e,-1,m]` berechnet werden:

```
In[2]:= PowerMod[4,-1,9]
Out[2]= 7
```

also $\frac{1}{4} = 7$ in $\mathbb{Z}_9$. Allgemein berechnet `PowerMod[e,k,m]` die Potenz e^k modulo m. In `Mathematica` kann man nicht einfach e^{-1} schreiben, denn woher soll das arme Programm wissen, ob Sie in $\mathbb{R}$ oder in $\mathbb{Z}_m$ rechnen wollen!

Euklid'scher Algorithmus

Der Euklid'sche Algorithmus kann wie folgt implementiert werden:

```
In[3]:= Euklid[a_Integer,b_Integer]:=Module[{r=a,rr=b},
          While[rr!=0,{r,rr}={rr,Mod[r,rr]}];
        r];

In[4]:= Euklid[75,38]
Out[4]= 1
```

(„!=“ bedeutet „ungleich“). Der ggT$(75,38)$ ist also 1. Natürlich hätten wir auch gleich den internen `Mathematica`-Befehl `GCD` für den größten gemeinsamen Teiler verwenden können:

```
In[5]:= GCD[75,38]
Out[5]= 1
```

Analog kann der erweiterte Euklid'sche Algorithmus so programmiert werden:

```
In[6]:= ExtendedEuklid[a_Integer,b_Integer]:=
          Module[{r=a,rr=b,xx=1,x=0,yy=0,y=1,Q},
           While[rr!=0,
            Q=Quotient[r,rr];
            {r,rr,x,xx,y,yy}={rr,Mod[r,rr],xx,x-Q xx,yy,y-Q yy}
           ];
          {r,x,y}];

In[7]:= ExtendedEuklid[75,38]
```

```
Out[7]= {1, −1, 2}
```

Ausgegeben werden also der $\mathrm{ggT}(75, 38) = 1$ und ganzzahlige Lösungen $x = -1$ und $y = 2$ der diophantischen Gleichung $75x + 38y = \mathrm{ggT}(75, 38)$. Wieder gibt es einen internen `Mathematica`-Befehl dazu: `ExtendedGCD[a, b]` gibt die Liste `{g, {x, y}}` aus, wobei $g = \mathrm{ggT}(a, b)$ und x, y ganzzahlige Lösungen von $ax + by = g$ sind.

RSA-Algorithmus

Die Verschlüsselung mittels RSA-Algorithmus ist natürlich zu aufwändig, um sie von Hand durchzuführen (aber auch für langsame Computer – Stichwort Chipkarten – kann die Geschwindigkeit bei RSA zu einem Problem werden). Wir wollen uns hier von `Mathematica` helfen lassen: Der Befehl `ToCharacterCode` wandelt ein Zeichen (Buchstabe, Ziffer, ...) und sogar eine ganze Zeichenkette in eine Liste von Zahlen gemäß dem ASCII-Code um:

```
In[8]:= ToCharacterCode["KLEOPATRA"]
Out[8]= {75, 76, 69, 79, 80, 65, 84, 82, 65}
```

Da im ASCII-Code der Buchstabe A der Zahl 65, B der Zahl 66, usw. entspricht, müssen wir – um die gewünschte Zuordnung $A = 0$, $B = 1$ usw. zu erhalten – noch 65 subtrahieren:

```
In[9]:= x = % − 65
Out[9]= {10, 11, 4, 14, 15, 0, 19, 17, 0}
```

Das ist nun der in Zahlen codierte Klartext, der verschlüsselt werden soll. Für die Verschlüsselung von x benötigen wir den öffentlichen Schlüssel

```
In[10]:= n = 1147; e = 29;
```

Nun können wir mit der Vorschrift $y = x^e \pmod n$ verschlüsseln:

```
In[11]:= y = PowerMod[x, e, n]
Out[11]= {803, 730, 132, 547, 277, 0, 979, 42, 0}
```

Hier ist `PowerMod[x, e, n]` eine effektivere Variante von `Mod[x^e, n]`. Der Empfänger kann mit dem geheimen Schlüssel d und der Vorschrift $x = y^d \pmod n$ entschlüsseln:

```
In[12]:= d = 149; PowerMod[y, d, n]
Out[12]= {10, 11, 4, 14, 15, 0, 19, 17, 0}
```

Bei unserem kurzen Spielzeugschlüssel ist es natürlich für einen Angreifer kein Problem den Algorithmus zu knacken, d.h. n zu faktorisieren:

```
In[13]:= FactorInteger[n]
Out[13]= {{31, 1}, {37, 1}}
```

zerlegt den Modul $n = 1147$ in seine Primfaktoren $p = 31$ und $q = 37$. Damit können wir m berechnen:

```
In[14]:= m = (31 − 1)(37 − 1)
Out[14]= 1080
```

(m kann auch alternativ mittels `m = EulerPhi[n]` berechnet werden). Der geheime Schlüssel d ist nun die Lösung der Gleichung $e\,d = 1 \pmod{m}$, wobei $e = 29$ der öffentliche Schlüssel ist und $m = 1080$ gerade vom Angreifer gefunden wurde. d kann mit dem Befehl `PowerMod` berechnet werden:

```
In[15]:= PowerMod[e, -1, m]
Out[15]= 149
```

Chinesischer Restsatz

Das System von Kongruenzen $x = a_1 \pmod{m_1}, \ldots, x = a_k \pmod{m_k}$ kann mit dem Befehl `ChineseRemainder[{a1, ..., ak}, {m1, ..., mk}]` gelöst werden:

```
In[16]:= ChineseRemainder[{2, 3, 2}, {3, 5, 7}]
Out[16]= 23
```

Ausgegeben wird die kleinste nichtnegative Lösung x, hier $x = 23$.

3.6 Kontrollfragen

Fragen zu Abschnitt 3.1: Das kleine Einmaleins auf endlichen Mengen

Erklären Sie folgende Begriffe: Rest, kongruent modulo m, Restklasse.

1. Geben Sie den Rest modulo 3 der Zahlen $1, 2, 3, \ldots, 10$ an.
2. Geben Sie den Rest modulo 3 von $-1, -2, -3, \ldots, -10$ an.
3. Was trifft zu:
   a) $a = b \pmod 3$ bedeutet, dass $a - b$ ein Vielfaches von 3 ist.
   b) $a = 4 \pmod 3$ bedeutet, dass es ein $k \in \mathbb{Z}$ gibt, sodass $a = k \cdot 3 + 4$.
4. Richtig oder falsch?
   a) $3 = 0 \pmod 3$ b) $7 = 2 \pmod 3$ c) $-2 = 1 \pmod 3$
   d) $12 = 27 \pmod 5$ e) $17 = 9 \pmod 5$ f) $28 = 10 \pmod 9$
5. Geben Sie die Restklassen modulo 3 an.
6. Wo steckt der Fehler: $2 = 8 \pmod 6$, d.h. $1 \cdot 2 = 4 \cdot 2 \pmod 6$. Kürzen von 2 auf beiden Seiten ergibt $1 = 4 \pmod 6$!?

Fragen zu Abschnitt 3.2: Gruppen, Ringe und Körper

Erklären Sie folgende Begriffe: additives Inverses, multiplikatives Inverses, $\mathbb{Z}_m$, $\mathbb{Z}_m^*$, Gruppe, Körper, Ring, Ideal.

1. Geben Sie folgende Mengen an: a) $\mathbb{Z}_3$ b) $\mathbb{Z}_5$
2. Richtig oder falsch:
   a) In $\mathbb{Z}_m$ besitzt jede Zahl ein additives Inverses.
   b) In $\mathbb{Z}_m$ besitzt jede Zahl ein multiplikatives Inverses.
3. Finden Sie das additive Inverse von: a) 1 in $\mathbb{Z}_8$ b) 3 in $\mathbb{Z}_9$ c) 3 in $\mathbb{Z}_{11}$

4. Welche Zahlen besitzen ein multiplikatives Inverses? Geben Sie es gegebenenfalls an: a) 3 in $\mathbb{Z}_7$ b) 6 in $\mathbb{Z}_8$ c) 0 in $\mathbb{Z}_9$ d) 8 in $\mathbb{Z}_{11}$
5. Geben Sie an: a) $\mathbb{Z}_5^*$ b) $\mathbb{Z}_6^*$
6. Richtig oder falsch?
   a) Die Lösung von $4x = 8 \pmod{27}$ ist $x = 8 \cdot \frac{1}{4} = 2$ in $\mathbb{Z}_{27}$.
   b) Die Lösung von $6x = 18 \pmod{42}$ ist $x = 18 \cdot \frac{1}{6} = 3$ in $\mathbb{Z}_{42}$.
7. Was ist der Unterschied zwischen einem kommutativen Ring (mit Eins) und einem Körper?
8. Geben Sie ein Beispiel für einen Ring, der kein Körper ist.

Fragen zu Abschnitt 3.3: Der Euklid'sche Algorithmus und diophantische Gleichungen

Erklären Sie folgende Begriffe: größter gemeinsamer Teiler, Euklid'scher Algorithmus, diophantische Gleichung, erweiterter Euklid'scher Algorithmus.

1. Besitzen folgenden Gleichungen ganzzahlige Lösungen (sie brauchen nicht angegeben zu werden)?
   a) $36x + 15y = 3$ b) $36x + 15y = 12$ c) $36x + 15y = 5$
   d) $22x + 15y = 27$
2. Was ist der Zusammenhang zwischen dem Euklid'schen Algorithmus und dem multiplikativen Inversen?

Fragen zu Abschnitt 3.4: Der Chinesische Restsatz

Erklären Sie folgende Begriffe: System von Kongruenzen, Chinesischer Restsatz.

1. Hat das System von Kongruenzen $x = a_1 (\mathrm{mod}\, m_1)$, $x = a_2 (\mathrm{mod}\, m_2)$ immer eine Lösung in $\mathbb{Z}_{m_1 m_2}$?
2. Was sagt der Chinesische Restsatz über folgendes System von Kongruenzen aus?
   $x = 1 \pmod 4$, $x = 3 \pmod 6$.

Lösungen zu den Kontrollfragen

Lösungen zu Abschnitt 3.1

1.

a	1	2	3	4	5	6	7	8	9	10
$r = a \bmod 3$	1	2	0	1	2	0	1	2	0	1

2.

a	-1	-2	-3	-4	-5	-6	-7	-8	-9	-10
$r = a \bmod 3$	2	1	0	2	1	0	2	1	0	2

3. a) richtig b) richtig
4. a) richtig b) Falsch, denn $7 - 2 = 5$ ist nicht durch 3 teilbar. c) richtig
   d) richtig e) Falsch, denn $17 - 9 = 8$ ist nicht durch 5 teilbar. f) richtig
5. $R_0 = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$, $R_1 = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$, $R_2 = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$
6. $\mathrm{ggT}(6, 2) = 2$, also hat 2 kein multiplikatives Inverses in $\mathbb{Z}_6$ und es kann daher nicht gekürzt werden!

Lösungen zu Abschnitt 3.2

1. a) $\mathbb{Z}_3 = \{0, 1, 2\}$ b) $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$
2. a) richtig b) Falsch; nur wenn die Zahl teilerfremd zu m ist, besitzt sie ein multiplikatives Inverses.
3. a) $8 - 1 = 7$ b) $9 - 3 = 6$ c) $11 - 3 = 8$
4. a) 3 und 7 sind teilerfremd, daher gibt es $\frac{1}{3} = \frac{1+2\cdot 7}{3} = 5$ in $\mathbb{Z}_7$.
   b) 6 und 8 sind nicht teilerfremd, daher gibt es keinen Kehrwert von 6 in $\mathbb{Z}_8$, d.h., die Schreibweise $\frac{1}{6}$ macht in $\mathbb{Z}_8$ keinen Sinn.
   c) Zu 0 gibt es nie einen Kehrwert.
   d) 8 und 11 sind teilerfremd, daher gibt es $\frac{1}{8} = \frac{1+5\cdot 11}{8} = 7$ in $\mathbb{Z}_{11}$.
5. a) $\mathbb{Z}_5^* = \mathbb{Z}_5 \backslash \{0\} = \{1, 2, 3, 4\}$ b) $\mathbb{Z}_6^* = \{1, 5\}$
6. a) Richtig; $\frac{1}{4}$ existiert in $\mathbb{Z}_{27}$, daher kann eindeutig nach x aufgelöst werden: $x = 8 \cdot \frac{1}{4} = 2 \cdot 4 \cdot \frac{1}{4} = 2 \pmod{27}$.
   b) Falsch, denn $\frac{1}{6}$ existiert nicht in $\mathbb{Z}_{42}$, daher kann nicht *eindeutig* nach x aufgelöst werden. (Es gibt 6 Lösungen, $x = 3$ ist eine davon.)
7. Ein kommutativer Ring mit Eins ist ein Körper, wenn es zu jedem Element außer 0 ein multiplikatives Inverses gibt.
8. Zum Beispiel $\mathbb{Z}$, $\mathbb{Z}_4$ oder allgemein $\mathbb{Z}_m$ (wenn m keine Primzahl ist). Weitere Beispiele sind $\mathbb{Z}_2[x]$, $\mathbb{R}[x]$ oder allgemein der Polynomring $\mathbb{K}[x]$ ($\mathbb{K}$ ein Körper).

Lösungen zu Abschnitt 3.3

1. Die Gleichung $ax + by = c$ hat genau dann ganzzahlige Lösungen, wenn $c = n \cdot \mathrm{ggT}(a, b)$ (Satz 3.38):
   a) ja, da $3 = 1 \cdot \mathrm{ggT}(36, 15)$ b) ja, da $12 = 4 \cdot \mathrm{ggT}(36, 15)$ c) nein, da $\mathrm{ggT}(36, 15) = 3$ kein Teiler von 5 ist d) ja, denn $27 = 27 \cdot \mathrm{ggT}(22, 15)$
2. Der erweiterte Euklid'sche Algorithmus kann zur effektiven Berechnung des multiplikativen Inversen verwendet werden.

Lösungen zu Abschnitt 3.4

1. Nicht notwendigerweise. Es kann keine oder mehrere Lösungen geben. Wenn die Module m_1 und m_2 teilerfremd sind, so garantiert der Chinesische Restsatz genau eine Lösung zwischen 0 und $m_1 \cdot m_2$ (und unendlich viele dazu kongruente Lösungen modulo $m_1 \cdot m_2$). Sind die Module nicht teilerfremd, so gibt der Chinesische Restsatz keine Information.
2. Nichts, da die Module 4 und 6 nicht teilerfremd sind. Wir wissen also von vornherein nichts über das Lösungsverhalten dieses Systems.

3.7 Übungen

Aufwärmübungen

1. Berechnen Sie: $(23 \cdot 19 - 2 \cdot 8 + 10 \cdot 37) \bmod 5$
2. a) Zeigen Sie, dass 0-8176-4176-9 eine gültige ISBN ist.
   b) Ein Einzelfehler passiert an der zweiten Stelle und es wird daher die ISBN 0-1176-4176-9 eingegeben. Wird der Fehler erkannt?
3. Europäische Artikelnummer (EAN):
   a) Wie lautet die Prüfziffer p der „Penne Rigate“: 8 076802 08573-p?
   b) Bei den beiden Artikelnummern 8 076802 05573-p und 8 076802 50573-p wurden zwei aufeinander folgende Ziffern vertauscht. Wird dieser Fehler erkannt?
4. a) Berechnen Sie den Rest modulo 6 der Zahlen $25, -25, 2$ und 12.
   b) Geben Sie die Restklassen modulo 6 an.
   c) Geben Sie $\mathbb{Z}_6$ und die Verknüpfungstabellen für die Addition und die Multiplikation in $\mathbb{Z}_6$ an.
5. Finden Sie alle $x \in \mathbb{Z}_m$ mit:
   a) $5 + x = 3 \pmod 7$ b) $5 + x = 4 \pmod 7$ c) $3x = 4 \pmod 7$
   d) $4x = 5 \pmod 6$ e) $4x = 6 \pmod{10}$
6. Berechnen Sie mit dem Euklid'schen Algorithmus:
   a) $\mathrm{ggT}(261, 123)$ b) $\mathrm{ggT}(49, 255)$
7. Hat die Gleichung $36x+15y = 6$ ganzzahlige Lösungen? Geben Sie gegebenenfalls eine an.
8. Eine Lösung von $36x + 15y = 300$ ist $x = -200$ und $y = 500$. Gibt es weitere ganzzahlige Lösungen? Gibt es insbesondere eine Lösung mit positivem x und positivem y?
9. Ist die Gleichung mit ganzzahligen x und y lösbar? Wenn ja, geben Sie *alle* ganzzahligen Lösungen an:
   a) $13x + 7y = 1$ b) $13x + 7y = 5$ c) $25x + 35y = 45$
10. Berechnen Sie $\frac{1}{7}$ in $\mathbb{Z}_{13}$ mithilfe des erweiterten Euklid'schen Algorithmus.
11. Lösen Sie das folgende System von Kongruenzen:
    $x = 1 \pmod 2$, $x = 3 \pmod 5$, $x = 3 \pmod 7$.

Weiterführende Aufgaben

1. Es sei S_n die Ziffernsumme der natürlichen Zahl n. Zeigen Sie, dass $n = S_n \pmod 3$. Tipp: $10 = 1 \pmod 3$. (Wie kann man, ausgehend von diesem Ergebnis, mithilfe der Ziffernsumme feststellen, ob eine Zahl durch 3 teilbar ist?)
2. Geben Sie alle Lösungen $x \in \mathbb{Z}_m$, wobei m der jeweilige Modul ist, an:
   a) $6x = 3 \pmod 9$ b) $6x = 4 \pmod 9$ c) $9x = 1 \pmod{13}$
3. Lösen Sie das folgende Gleichungssystem in $\mathbb{Z}_{27}$:

$$\begin{aligned} 5x + 17y &= 12 \\ 14x + 12y &= 11 \end{aligned}$$

4. Ist 3-540-25782-9 eine gültige ISBN?
5. Bildet $\{n, a, b\}$ mit der im Folgenden definierten Verknüpfung „$\circ$“ eine Gruppe?

$\circ$	n	a	b
n	n	a	b
a	a	n	b
b	b	a	n

6. Finden Sie mithilfe des erweiterten Euklid'schen Algorithmus alle *natürlichen* Zahlen x und y, die die Gleichung $68x + 23y = 1000$ erfüllen.
7. Finden Sie das multiplikative Inverse von 9 in $\mathbb{Z}_{13}$ mithilfe des erweiterten Euklid'schen Algorithmus.
8. Angenommen, ein Computer kann nur ganze Zahlen mit zwei Dezimalstellen effizient verarbeiten. Sie möchten aber auch dreistellige Zahlen effizient darstellen, addieren und multiplizieren. Wählen Sie dazu drei passende möglichst große Module und stellen Sie zum Beispiel 203 und 125 durch ihre (zweistelligen) Reste bezüglich der Module dar. (Es sind drei Module ausreichend, da das Produkt aus zwei dreistelligen Zahlen höchstens sechsstellig ist.) Berechnen Sie mithilfe des Chinesischen Restsatzes die Summe und das Produkt von 203 und 125.
9. Zeigen Sie: Wenn p eine Primzahl ist, so hat die Gleichung $x^2 = 1 \pmod p$ nur die Lösungen $x = 1 \pmod p$ und $x = -1 \pmod p$ (Tipp: $x^2 - 1 = (x-1)(x+1)$).

   Das bedeutet, dass in $\mathbb{Z}_p$ nur 1 und $p-1$ gleich ihrem multiplikativen Inversen sind.

10. Zeigen Sie: Wenn p eine Primzahl ist, so gilt $(p-1)! = -1 \pmod p$ (Tipp: Fassen Sie die Terme in $(p-1)!$ zu Paaren von zueinander multiplikativ inversen Zahlen zusammen und verwenden Sie Übungsaufgabe 9).
11. Finden Sie alle Lösungen des Systems $x = 1 \pmod 2$, $x = 3 \pmod 4$ in $\mathbb{Z}_8$. (Achtung: Der Chinesische Restsatz ist nicht anwendbar.)
12. RSA-Algorithmus: Wenn eine Person A eine verschlüsselte Nachricht an eine Person B schicken möchte, so schlägt A den öffentlichen Schlüssel (n, e) von B nach (wobei n das Produkt von zwei sehr großen, geheimen Primzahlen ist), verschlüsselt den Klartext x gemäß $y = x^e \pmod n$, und schickt den Geheimtext y an B.
    Senden Sie mir die Nachricht „NEIN“ (d.h., in Zahlen angeschrieben, die Nachricht „$13, 4, 8, 13$“) verschlüsselt zu, wenn mein öffentlicher Schlüssel $(n, e) = (55, 3)$ ist.

Lösungen zu den Aufwärmübungen

1. Zur einfachen Berechnung wird jede vorkommende Zahl sofort durch ihren Rest modulo 5 ersetzt: $3 \cdot 4 - 2 \cdot 3 + 0 \cdot 2 = 12 - 6 + 0 = 2 - 1 = 1 \pmod 5$.
2. a) $10 \cdot 0 + 9 \cdot 8 + 8 \cdot 1 + 7 \cdot 7 + 6 \cdot 6 + 5 \cdot 4 + 4 \cdot 1 + 3 \cdot 7 + 2 \cdot 6 + 9 = 0 \pmod{11}$, daher ist die ISBN gültig.
   b) Ja, denn bei der ISBN wird jeder Einzelfehler erkannt.
3. a) $p = 8$ b) Die Prüfziffer ist beiden Fällen $p = 1$, der Fehler wird daher nicht erkannt.

4. a) 1, 5, 2, 0 b) $R_0 = \{k \cdot 6 \mid k \in \mathbb{Z}\}$; $R_1 = \{k \cdot 6 + 1 \mid k \in \mathbb{Z}\}$; ...; $R_5 = \{k \cdot 6 + 5 \mid k \in \mathbb{Z}\}$
   c)

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

5. a) Eindeutige Lösung $x = 5$.
   b) Eindeutige Lösung $x = 6$.
   c) Eindeutige Lösung $x = 6$, da 3 ein multiplikatives Inverses in $\mathbb{Z}_7$ hat.
   d) Keine Lösung, da 4 kein multiplikatives Inverses in $\mathbb{Z}_6$ hat (dann wäre die Lösung eindeutig) und da $\text{ggT}(4, 6) = 2$ kein Teiler von 5 ist.
   e) Zwei Lösungen in $\mathbb{Z}_{10}$, da $\text{ggT}(4, 10) = 2$ ist und dieser auch 6 teilt. Die beiden Lösungen $x = 4$, $x = 9$ finden wir mithilfe von Satz 3.18.
6. a) $\text{ggT}(261, 123) = 3$
   b) $\text{ggT}(49, 255) = 1$, die beiden Zahlen sind also teilerfremd.
7. Es gibt ganzzahlige Lösungen, da $6 = 2 \cdot \text{ggT}(36, 15)$. Mit dem erweiterten Euklid'schen Algorithmus kann zunächst die Lösung $x = -2$ und $y = 5$ von $36x + 15y = 3$ $(= \text{ggT}(36, 15))$ berechnet werden. (Probe: $-2 \cdot 36 + 5 \cdot 15 = 3$). Eine Lösung von $36x + 15y = 2 \cdot 3$ ist daher $x = 2 \cdot (-2) = -4$ und $y = 2 \cdot 5 = 10$ (Probe: $-4 \cdot 36 + 10 \cdot 15 = 6$).
8. Mit Satz 3.38 erhalten wir $\tilde{x} = -200 + 5 \cdot 41 = 5$, $\tilde{y} = 500 - 12 \cdot 41 = 8$ (Probe: $36 \cdot 5 + 15 \cdot 8 = 300$).
9. a) $\tilde{x} = -1 + 7k$, $\tilde{y} = 2 - 13k$ $(k \in \mathbb{Z})$ b) $\tilde{x} = -5 + 7k$, $\tilde{y} = 10 - 13k$ $(k \in \mathbb{Z})$
   c) $\tilde{x} = 27 + 7k$, $\tilde{y} = -18 - 5k$ $(k \in \mathbb{Z})$
10. Mithilfe des erweiterten Euklid'schen Algorithmus finden wir die Lösung $x = -1$ und $y = 2$ von $13x + 7y = 1$. In die Gleichung eingesetzt und etwas umgeformt erhalten wir $7 \cdot 2 = 1 - 13 \cdot (-1)$, d.h. $7 \cdot 2 = 1 \pmod{13}$. Damit ist $\frac{1}{7} = 2$ in $\mathbb{Z}_{13}$.
11. Da $m_1 = 2$, $m_2 = 5$ und $m_3 = 7$ teilerfremd sind, gibt es eine Lösung x mit $0 \leq x < 70$ (und jede dazu modulo 70 kongruente Zahl ist ebenfalls Lösung). Konstruktion:
    a) $M_1 = m_2 \cdot m_3 = 5 \cdot 7 = 35$; $M_2 = m_1 \cdot m_3 = 2 \cdot 7 = 14$; $M_3 = m_1 \cdot m_2 = 2 \cdot 5 = 10$.
    b) Multiplikative Inverse von M_1, M_2, M_3 modulo m_1, m_2, m_3: Gesucht sind N_1, N_2, N_3 mit $35 \cdot N_1 = 1 \cdot N_1 = 1 \pmod{2}$, $14 \cdot N_2 = 4 \cdot N_2 = 1 \pmod{5}$ und $10 \cdot N_3 = 3 \cdot N_3 = 1 \pmod{7}$. Es folgt, dass $N_1 = 1$, $N_2 = 4$ und $N_3 = 5$.
    c) $x = a_1 \cdot M_1 \cdot N_1 + a_2 \cdot M_2 \cdot N_2 + a_3 \cdot M_3 \cdot N_3 = 1 \cdot 35 \cdot 1 + 3 \cdot 14 \cdot 4 + 3 \cdot 10 \cdot 5 = 353 = 3 \pmod{70}$.

(Lösungen zu den weiterführenden Aufgaben finden Sie in Abschnitt B.3)

5

Relationen und Funktionen

5.1 Relationen

Relationen sind ein mathematisches Hilfsmittel, um Beziehungen zwischen einzelnen Objekten zu beschreiben. Sie werden zum Beispiel in relationalen Datenbanken und in der theoretischen Informatik (z. B. formale Sprachen) verwendet.

In der Umgangssprache versteht man unter einer „Relation“ eine Beziehung. Das ist auch in der Mathematik so. Personen, Gegenstände oder allgemein Objekte können zueinander in einer Beziehung stehen. Nehmen wir zum Beispiel die Menge der Städte „Wien“, „Berlin“, „Zürich“ und die Menge aller Staaten Europas her. Für die folgenden Paare (a, b) gilt dann: „Die Stadt a liegt im Land b“: (Wien, Österreich), (Berlin, Deutschland) und (Zürich, Schweiz). In diesem Sinn ist auch der mathematische Begriff einer Relation definiert:

Definition 5.1 Eine **Relation R zwischen den Mengen A und B** ist eine Teilmenge des kartesischen Produktes $A \times B$, also $R \subseteq A \times B$. Für $(a, b) \in R$ sagt man: „a steht in Relation R zu b“. Oft schreibt man auch $aR\,b$ statt $(a, b) \in R$.

Im Spezialfall $A = B$, also von Relationen $R \subseteq A \times A$, spricht man von einer **Relation in** A oder einer **Relation auf** A.

Beispiel 5.2 Relation

a) $R = \{(Wien, \ddot{O}), (Bonn, D), (Dresden, D)\}$ ist eine Relation zwischen der Städtemenge $A = \{Wien, Bonn, Dresden\}$ und der Ländermenge $B = \{\ddot{O}, D, CH\}$. In Worten bedeutet hier $(a, b) \in R$ bzw. $aR\,b$: „a liegt in b“. Es kann ohne weiteres vorkommen, dass ein Element in der Relation mehrfach vorkommt (so wie hier D) oder gar nicht (so wie hier CH).

b) $A = B = \{2, 3, 4, 5, 6\}$. Geben Sie die Paare der Relation „a ungleich b und a teilt b“ an.

Lösung zu 5.2 b) Es ist (a, b) in R, genau dann, wenn die Zahl a die Zahl b teilt, wobei nur Paare mit $a \neq b$ gewünscht sind. Daher lautet die Relation $R = \{(2, 4), (2, 6), (3, 6)\}$. Achtung: Es ist zwar $(2, 4) \in R$ (denn 2 teilt 4), nicht aber $(4, 2) \in R$ (denn 4 teilt 2 nicht). ■

Überlegen wir uns als Nächstes, wie man aus gegebenen Relationen neue Relationen bilden kann. Da Relationen Mengen sind, gelten für sie natürlich auch alle Mengenoperationen und man spricht in diesem Sinn von **Vereinigung, Durchschnitt, Differenz, Komplement** oder **Teilmengen von Relationen**. Beispiel: Die Vereinigung der Relation „kleiner ($<$)“ und der Relation „gleich ($=$)“ ist die Relation „kleiner oder gleich ($\leq$)“. Weiters ist es auch oft praktisch, von der **leeren Relation** $\{\}$ zwischen zwei Mengen zu sprechen (das ist also die leere Menge als Teilmenge von $A \times B$). Weiters definiert man:

Definition 5.3 Es sei $R \subseteq A \times B$ eine Relation. Dann heißt die Relation

$$R^{-1} = \{(b, a) \mid (a, b) \in R\} \subseteq B \times A$$

die zu R **inverse Relation** (oder **Umkehrrelation**).

Beispiel: Die Inverse der Relation „kleiner ($<$)“ ist die Relation „größer ($>$)“. Oder die Inverse der Relation „ist Kind von“ in der Menge aller Menschen ist die Relation „ist Elternteil von“. Weiters:

Definition 5.4 Aus zwei Relationen $R \subseteq A \times B$ und $S \subseteq B \times C$ kann man eine neue Relation, die **Verkettung** (oder **Verknüpfung** oder das **Produkt**), bilden:

$$S \circ R = \{(a, c) \mid \text{ es gibt ein } b \in B \text{ mit } (a, b) \in R \text{ und } (b, c) \in S\} \subseteq A \times C.$$

Beispiel: R sei die Relation „ist Mutter von“ und S ist die Relation „ist verheiratet mit“ in der Menge aller Menschen. Dann ist $S \circ R$ die Relation „ist Schwiegermutter von“. (Denn wenn a Mutter von b ist und b verheiratet mit c ist, so ist a Schwiegermutter von c.)

Die Schreibweise $S \circ R$ wird in der Literatur nicht ganz einheitlich verwendet. Bitte vergewissern Sie sich daher immer, was genau damit gemeint ist.

Beispiel 5.5 Verkettung von Relationen
Bilden Sie die Verknüpfung $S \circ R$ folgender Relationen:
a) $R = \{(1, a), (2, b), (3, c)\}$ und $S = \{(a, x), (a, y), (b, z)\}$
b) $R = \{(Huber, Wien), (Maier, Wien), (Schuster, Bonn)\}$ und
$S = \{(Wien, A), (Bonn, D), (Dresden, D)\}$

Lösung zu 5.5

a) Aus $(1, a) \in R$ und $(a, x) \in S$ wird $(1, x) \in S \circ R$. Weiters: Aus $(1, a)$ und (a, y) wird $(1, y)$. Und aus $(2, b)$ und (b, z) wird $(2, z)$. Für $(3, c) \in R$ kann kein zugehöriges Paar gefunden werden (denn kein Paar aus S beginnt mit c). Insgesamt: $S \circ R = \{(1, x), (1, y), (2, z)\}$.

b) Wie soeben erhalten wir $S \circ R = \{(Huber, A), (Maier, A), (Schuster, D)\}$. Die Verknüpfung der Relation „Person, Stadt“ mit der Relation „Stadt, Land“ ergibt also die Relation „Person, Land“. ■

Die Verknüpfung von Relationen ist **assoziativ**, d.h., es gilt $(R_3 \circ R_2) \circ R_1 = R_3 \circ (R_2 \circ R_1)$. Das bedeutet, dass die Klammern weggelassen werden können. Achtung: Die Verknüpfung ist nicht kommutativ, d.h., im Allgemeinen ist $R_1 \circ R_2 \neq R_2 \circ R_1$!

Wenn A und B endliche Mengen sind (und nicht zu viele Elemente haben), so kann eine Relation $R \subseteq A \times B$ z. B. gut durch einen *Graphen* dargestellt werden. Die Elemente der Mengen werden dazu als (beliebig angeordnete) Punkte (*Knoten*) gezeichnet und die Beziehung xRy durch einen Pfeil dargestellt, der vom Knoten x zum Knoten y geht. Abbildung 5.1 veranschaulicht so die Relation $R = \{(a,1),(b,1),(b,3),(c,2)\} \subseteq A \times B$ für $A = \{a,b,c,d\}$ und $B = \{1,2,3\}$.

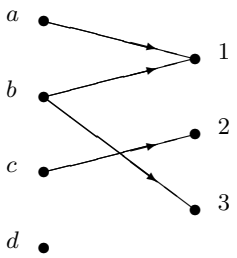


Abbildung 5.1. Graphische Darstellung einer Relation

Überlegen Sie, wie die inverse Relation R^{-1} bzw. die Verkettung zweier Relationen graphisch veranschaulicht werden können!

Es gibt auch noch andere Darstellungsmöglichkeiten von Relationen, zum Beispiel (in relationalen Datenbanken) mithilfe von Tabellen. Für's Erste genügt uns aber die gerade beschriebene graphische Darstellung, denn mit ihrer Hilfe können die nun folgenden verschiedenen Eigenschaften von Relationen gut veranschaulicht werden.

Bisher haben wir allgemein Relationen zwischen zwei Mengen A und B betrachtet (natürlich war immer der Fall $A = B$ eingeschlossen). Nun wollen wir uns auf den Spezialfall von Relationen $R \subseteq A \times A$ konzentrieren. Solche Relationen können bestimmte Eigenschaften haben:

Definition 5.6 Eine Relation R in A heißt

- **reflexiv**, wenn $(a,a) \in R$ für alle $a \in A$.
- **symmetrisch**, wenn für alle $a,b \in A$ gilt: $(a,b) \in R \Leftrightarrow (b,a) \in R$.
- **antisymmetrisch**, wenn für alle $a,b \in A$ gilt:
  $(a,b) \in R$ und $(b,a) \in R \Rightarrow a = b$
  (oder gleichbedeutend: $a \neq b \Rightarrow (b,a) \notin R$ oder $(a,b) \notin R$).
- **asymmetrisch**, wenn für alle $a,b \in A$ gilt: $(a,b) \in R \Rightarrow (b,a) \notin R$.
- **transitiv**, wenn für alle $a,b,c \in A$ gilt:
  $(a,b) \in R$ und $(b,c) \in R \Rightarrow (a,c) \in R$.

Eine reflexive Relation enthält also alle Paare $(a,a) \in A \times A$, oder kurz: $\mathbb{I}_A \subseteq R$, wobei $\mathbb{I}_A = \{(a,a) \mid a \in A\}$ die **Identitätsrelation** bezeichnet. Eine symmetrische Relation kann durch $R^{-1} = R$ charakterisiert werden, eine antisymmetrische in der

Form $R^{-1} \cap R \subseteq \mathbb{I}_A$, eine asymmetrische Relation durch $R^{-1} \cap R = \{\}$ und eine transitive Relation durch $R \circ R \subseteq R$.

Bei der **graphischen Veranschaulichung einer Relation auf** A wird üblicherweise jedes Element von A nur einmal als Knoten gezeichnet, die Knoten werden dabei irgendwie angeordnet. Beispiel: Abbildung 5.2 stellt die Relation $R = \{(a,b),(a,c),(b,a),(c,c)\}$ auf $A = \{a,b,c\}$ dar.

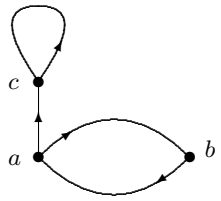


Abbildung 5.2. Relation auf der Menge A

Die Eigenschaften aus Definition 5.6 drücken sich im Graphen der Relation so aus: Eine *reflexive* Relation hat an jedem Knoten eine **Schlinge** (d.h., der Pfeil geht vom Knoten aus und mündet wieder in ihn ein), denn jedes Element steht mit sich selbst in Relation. Für den Graphen einer *symmetrischen* Relation gilt: Wenn es einen Pfeil von a nach b gibt, so gibt es gleichzeitig auch einen von b nach a. Beim Graphen einer *antisymmetrischen* Relation kann es zwischen zwei verschiedenen Knoten höchstens einen Pfeil geben (Schlingen können vorkommen). Beim Graphen einer *asymmetrischen* Relation kann es zwischen zwei verschiedenen Knoten höchstens einen Pfeil geben und Schlingen sind nicht zugelassen. Und wenn eine Relation *transitiv* ist, so bedeutet das für ihren Graphen: Wenn ein Pfeil von a nach b geht und einer von b nach c, so gibt es auch einen von a nach c.

Beispiel 5.7 Spezielle Eigenschaften einer Relation
Betrachten wir Beispiele von Relationen in der Menge aller Menschen:

a) Die Relation „ist gleich alt wie“ ist reflexiv, symmetrisch und transitiv (weder asymmetrisch noch antisymmetrisch).
b) Die Relation „ist verwandt mit“ ist reflexiv, symmetrisch und transitiv (weder asymmetrisch noch antisymmetrisch).
c) Die Relation „ist Mutter von“ ist asymmetrisch und antisymmetrisch (aber nicht reflexiv, nicht symmetrisch, nicht transitiv).
d) Die Relation „ist älter als“ ist asymmetrisch, antisymmetrisch und transitiv (aber nicht reflexiv, nicht symmetrisch).

Oft kann man Objekte bezüglich einer bestimmten Eigenschaft zusammenfassen und so zu einer besseren Übersicht gelangen. Mathematisch führt uns das auf den Begriff einer Äquivalenzrelation:

Definition 5.8 Eine Relation R auf einer Menge A heißt **Äquivalenzrelation**, wenn sie reflexiv, symmetrisch und transitiv ist. Für $(a,b) \in R$ sagt man auch: „a ist äquivalent zu b“.

Das einfachste Beispiel einer Äquivalenzrelation ist die Identitätsrelation $\mathbb{I}_A$. Andere Beispiele sind:

Beispiel 5.9 Äquivalenzrelation

a) Ist $R = \{(1,1), (1,-1), (-1,1), (-1,-1), (2,2), (2,-2), (-2,2), (-2,-2)\}$ eine Äquivalenzrelation auf $A = \{-2,-1,1,2\}$? Wie könnte man diese Relation z. B. in Worten beschreiben?

b) Ist die Relation R mit

$(a,b) \in R$, wenn a in der gleichen Gehaltsstufe wie b ist,

eine Äquivalenzrelation auf der Menge aller Mitarbeiter einer Firma?

c) Warum ist die Relation R mit

$(a,b) \in R$, wenn a in einem gleichen Projekt wie b arbeitet,

im Allgemeinen keine Äquivalenzrelation auf der Menge aller Mitarbeiter in einer Firma?

Lösung zu 5.9

a) Ja, denn: $(a,a) \in R$ für alle a (Reflexivität); für $(a,b) \in R$ ist auch $(b,a) \in R$ (Symmetrie); mit $(a,b) \in R$ und $(b,c) \in R$ ist auch $(a,c) \in R$ (Transitivität). In Worten: „a und b haben denselben Betrag“. Zwei Zahlen sind hier also äquivalent, wenn sie denselben Betrag haben.

b) Es ist leicht zu sehen, dass alle Eigenschaften einer Äquivalenzrelation erfüllt sind:
• Jeder ist in der gleichen Gehaltsstufe wie er selbst, d.h. es ist immer $(a,a) \in R$.
• Wenn a in der gleichen Gehaltsstufe ist wie b, dann ist auch b in der gleichen Gehaltsstufe wie a. Mathematisch formuliert: Wenn $(a,b) \in R$, dann ist auch $(b,a) \in R$.
• Wenn a in der gleichen Gehaltsstufe ist wie b, und b in der gleichen Gehaltsstufe ist wie c, dann ist auch a in der gleiche Gehaltsstufe wie c. Kurz gesagt: Wenn $(a,b) \in R$ und $(b,c) \in R$, dann ist auch $(a,c) \in R$.

c) Der Wurm steckt darin, dass es vorkommen kann, dass ein Mitarbeiter in mehreren Projekten gleichzeitig arbeitet: Angenommen, b arbeitet in einem Projekt mit a, und in einem anderen Projekt mit c zusammen. Daraus folgt aber nicht, dass auch a und c in einem gleichen Projekt arbeiten. Kurz: Es ist zwar $(a,b) \in R$ und $(b,c) \in R$, aber nicht $(a,c) \in R$ (d.h., die Transitivität ist nicht erfüllt). ■

Weitere Beispiele für Äquivalenzrelationen sind: „a ist gleich alt wie b“ in einer Menge von Personen, „a kostet gleich viel wie b“ in einer Menge von Produkten, „Seite a gehört zum selben Kapitel wie Seite b“ in der Menge aller Seiten eines Buches, usw. Anhand dieser Beispiele erkennen wir die interessanteste und gleichzeitig wichtigste Eigenschaft einer Äquivalenzrelation auf A: Sie unterteilt A in so genannte *Äquivalenzklassen*.

Definition 5.10 R sei eine Äquivalenzrelation auf A und $a \in A$. Dann heißt die Menge

$$[a] = \{x \in A \mid (a,x) \in R\}$$

die **Äquivalenzklasse** von a. Sie besteht also aus allen Elementen, die äquivalent zu a sind (und je zwei Elemente aus $[a]$ sind auch äquivalent zueinander). Man nennt a und jedes andere Element aus $[a]$ einen **Vertreter** aus dieser Äquivalenzklasse.

Eine Äquivalenzrelation hat folgende charakteristische Eigenschaften:

Satz 5.11 Sei R eine Äquivalenzrelation auf A. Dann gilt:

- Je zwei verschiedene Äquivalenzklassen sind disjunkt.
- Die Vereinigung aller Äquivalenzklassen ist gleich A.

So ist in Beispiel 5.9 a) $[1] = \{-1, 1\}$ die Äquivalenzklasse von 1 und $[2] = \{-2, 2\}$ ist die Äquivalenzklasse von 2. Die beiden Äquivalenzklassen haben keine gemeinsamen Elemente und ihre Vereinigung ist gleich A.

Beispiel 5.12 Äquivalenzklassen
Mitarbeiter A, B, C, D, E, F einer Firma: A und C sind in Gehaltsstufe 1; B, D und E sind in Gehaltsstufe 2; F ist in Gehaltsstufe 3. Wir haben in Beispiel 5.9 b) gesehen, dass „a ist in der gleichen Gehaltsstufe wie b“ eine Äquivalenzrelation auf $\{A, B, C, D, E, F\}$ ist. Geben Sie die Äquivalenzklassen an.

Lösung zu 5.12 Die Äquivalenzklassen sind gerade die drei Gehaltsstufen:

$$\begin{aligned} K_1 &= \{A, C\} \ \ldots \text{ Gehaltsstufe 1,} \\ K_2 &= \{B, D, E\} \ldots \text{ Gehaltsstufe 2,} \\ K_3 &= \{F\} \ \ldots \text{ Gehaltsstufe 3.} \end{aligned}$$

Diese Klasseneinteilung wird in Abbildung 5.3 veranschaulicht. ■

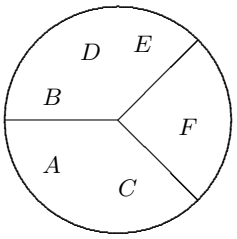


Abbildung 5.3. Äquivalenzklassen

Die Beziehung $a = b \pmod m$ ist eine Äquivalenzrelation auf $\mathbb{Z}$. Die Restklassen sind nichts anderes als die zugehörigen Äquivalenzklassen.

Wird eine Menge A in Teilmengen zerlegt, die a) disjunkt sind und b) deren Vereinigung die Menge A liefert, so spricht man von einer **Partition** oder **Zerlegung**

von A. Jede Äquivalenzrelation liefert also durch ihre Äquivalenzklassen eine Partition von A. Bemerkenswert ist, dass aber auch umgekehrt jede Partition von A eine Äquivalenzrelation auf A definiert: $(a, b) \in R$ genau dann, wenn $[a] = [b]$.

Ein weiterer wichtiger Typ von Relationen, der immer wieder vorkommt, sind die so genannten Ordnungsrelationen:

Definition 5.13 Eine Relation R in einer Menge A heißt **Ordnung(srelation)**, wenn sie reflexiv, antisymmetrisch und transitiv ist.

Eine typische Ordnung ist die Relation $\leq$ in den natürlichen Zahlen. Denn diese Relation ist reflexiv ($a \leq a$), antisymmetrisch (wenn $a \leq b$ und $b \leq a$, dann muss $a = b$ sein) und transitiv (wenn $a \leq b$ und $b \leq c$, dann ist $a \leq c$). Das ist das Paradebeispiel für eine Ordnung, daher verwendet man oft auch für andere Ordnungsrelationen R die Schreibweise $a \leq b$ statt $(a, b) \in R$.

Zu jeder Ordnung R gibt es eine zugehörige **strikte Ordnung**. Darunter versteht man jene Relation, die man aus R erhält, wenn man aus ihr alle Paare der Form (a, a) entfernt. Umgekehrt erhält man aus einer strikten Ordnung wieder die zugehörige Ordnung, indem man alle Paare der Form (a, a) hinzufügt. Beispiel: Die zu $\leq$ zugehörige strikte Ordnungsrelation ist $<$. Unabhängig von der zugehörigen Ordnung ist eine strikte Ordnung so definiert:

Definition 5.14 Eine Relation R in einer Menge A heißt **strikte Ordnung(srelation)**, wenn sie asymmetrisch und transitiv ist.

Beispiel 5.15 Ordnung

a) Die Teilmengenbeziehung $A \subseteq B$ auf einer Menge von Mengen ist eine Ordnung. Die zugehörige strikte Ordnung ist $A \subset B$ (echte Teilmenge, also $A \neq B$).
b) Die Relation „a teilt b “ ist eine Ordnung in den ganzen Zahlen. Die zugehörige strikte Ordnung ist „a teilt b und $a \neq b$“.
c) Die Menge aller Zeichenketten (Strings) kann mit der **lexikographischen Ordnung** versehen werden, indem man zunächst den einzelnen Zeichen natürliche Zahlen zuweist (z. B. gemäß dem ASCII-Code). Dann vergleicht man die Strings von links nach rechts Zeichen für Zeichen (unter Verwendung der Ordnung auf $\mathbb{N}$), wobei die erste Stelle, an der sich Strings unterscheiden, den Ausschlag gibt. Zum Beispiel: `abc` $\leq$ `aca` (da `b` $\leq$ `c`).

Definition 5.16 Zwei Elemente a und b aus A heißen **vergleichbar bezüglich der Ordnung** R, wenn aRb oder bRa gilt. Wenn bezüglich einer Ordnung je zwei verschiedene Elemente miteinander vergleichbar sind, so spricht man von einer **totalen Ordnung**, andernfalls von einer **partiellen Ordnung** (oder **Halbordnung**).

Total heißt also, dass – welche Elemente man auch immer aus A herausgreift – diese immer bezüglich R in Beziehung zueinander stehen: Entweder $(a, b) \in R$ oder

$(b, a) \in R$. Der Begriff „total“ bzw. „partiell“ kann auch analog für eine strikte Ordnung verwendet werden.

Beispiel 5.17 Totale Ordnung – Partielle Ordnung
a) $a \leq b$ ist eine totale Ordnung in den natürlichen Zahlen, denn für zwei Zahlen $a, b \in \mathbb{N}$ ist immer $a \leq b$ oder $b \leq a$.
b) Die Teilmengenbeziehung ist eine partielle Ordnung, denn bei zwei Mengen muss nicht notwendigerweise eine Menge eine Teilmenge der anderen sein.

Achtung: Die Begriffe Ordnung/totale Ordnung/Halbordnung werden nicht ganz einheitlich verwendet. Daher muss man beim Lesen in der Literatur immer zuerst feststellen, was genau gemeint ist.

Ordnungsrelationen spielen z. B. eine wichtige Rolle bei Projektplanungen:

Beispiel 5.18 Ordnungsrelation: Projektplanung
Sei $J = \{1, 2, 3, 4\}$ die Menge aller Teilschritte (*Jobs*) eines Ablaufes. Die Reihenfolge der Jobs kann durch die Relation „a muss vor b erledigt werden“ festgelegt werden. Wenn zum Beispiel Job 1 vor Job 2, und Job 2 sowohl vor Job 3 als auch vor Job 4 erledigt werden muss, so kann dies durch die strikte Ordnungsrelation: $H = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4)\} \subseteq J^2$ beschrieben werden. Die Ordnung ist nicht total, da zwischen Job 3 und Job 4 keine Relation besteht (d.h., die Reihenfolge, in der diese beiden Jobs ausgeführt werden, ist egal).

Am letzten Beispiel sehen wir, dass H eindeutig bestimmt ist durch die Forderungen, dass die Paare von $R = \{(1, 2), (2, 3), (2, 4)\}$ enthalten sein sollen *und* dass H transitiv sein soll. Denn aus $(1, 2), (2, 3) \in H$ folgt $(1, 3) \in H$ und aus $(1, 2), (2, 4) \in H$ folgt $(1, 4) \in H$. Formal sind wir gerade von R zu H gekommen, indem wir R um alle Paare aus $R \circ R$ erweitert haben: $H = R \cup (R \circ R)$. Man sagt, dass H die *transitive Hülle* von R ist.

Allgemein können wir eine beliebige Relation R in der Menge A solange um Elemente aus $R \circ R$, $R \circ R \circ R, \ldots$ erweitern, bis die entstehende Relation

$$[R]^{trans} = R \cup (R \circ R) \cup (R \circ R \circ R) \cup \cdots$$

transitiv ist. Ist A endlich, so reichen endlich viele Schritte.

Definition 5.19 Die Relation $[R]^{trans}$ ist die kleinste transitive Relation, die R enthält und wird als **transitive Hülle** von R bezeichnet. Analog definiert man die **reflexive Hülle**

$$[R]^{refl} = R \cup \mathbb{I}_A$$

und die **symmetrische Hülle**

$$[R]^{sym} = R \cup R^{-1}$$

als die kleinste Relation, die R enthält und reflexiv beziehungsweise symmetrisch ist.

Im Graphen der Relation R bedeutet die Bildung der *transitiven* Hülle, dass man zu den bereits bestehenden Pfeilen neue hinzufügt, und zwar dann einen neuen

Pfeil vom Knoten x zum Knoten y, wenn man von x längs irgendwelcher bereits bestehender (oder inzwischen hinzugekommenen) Pfeile nach y kommen kann. Die Bildung der *reflexiven* Hülle bedeutet, dass jeder Knoten eine Schlinge bekommt (falls nicht bereits vorhanden); und die Bildung der *symmetrischen* Hülle bedeutet, dass jeder Pfeil durch einen zweiten Pfeil in die entgegengesetzte Richtung ergänzt wird (sofern er nicht ohnehin schon da ist).

Beispiel 5.20 Transitive, reflexive, symmetrische Hülle
Geben Sie zur Relation $R = \{(a,b),(b,c),(c,d),(d,e)\}$ auf $A = \{a,b,c,d,e\}$ die reflexive, die symmetrische sowie die transitive Hülle an.

Lösung zu 5.20 Für die reflexive Hülle fügen wir alle Paare (x,x) mit $x \in A$ hinzu:

$$[R]^{refl} = \{(a,a),(a,b),(b,b),(b,c),(c,c),(c,d),(d,d),(d,e),(e,e)\}$$

Analog kommt für die symmetrische Hülle zu einem vorhandenen $(x,y) \in R$ jeweils (y,x) hinzu:

$$[R]^{sym} = \{(a,b),(b,a),(b,c),(c,b),(c,d),(d,c),(d,e),(e,d)\}$$

Für die transitive Hülle bilden wir solange Verkettungen $R \circ R$, $R \circ (R \circ R)$, $R \circ (R \circ R \circ R)$, bis kein neues Paar mehr entsteht. Das ist dann der Fall, wenn die leere Menge erreicht wird oder wenn eine Verknüpfung erreicht wird, die keine neuen Paare mehr enthält:

$$\begin{aligned} R \circ R &= \{(a,c),(b,d),(c,e)\} \\ R \circ (R \circ R) &= \{(a,d),(b,e)\} \\ R \circ (R \circ R \circ R) &= \{(a,e)\} \\ R \circ (R \circ R \circ R \circ R) &= \{\} \end{aligned}$$

Würde man die leere Menge nochmal mit R verknüpfen, so käme kein neues Paar hinzu. Also können wir abbrechen und die gebildeten Mengen vereinigen:

$$\begin{aligned} [R]^{trans} &= R \cup (R \circ R) \cup (R \circ R \circ R) \cup (R \circ R \circ R \circ R) = \\ &= \{(a,b),(b,c),(c,d),(d,e),(a,c),(b,d),(c,e),(a,d),(b,e),(a,e)\}. \end{aligned}$$

■

Bisher haben wir nur Relationen zwischen *zwei* Mengen (die verschieden oder gleich sein können) betrachtet. Man nennt diese Relationen auch **binäre Relationen** oder **2-stellige Relationen**. Allgemeiner kann man auch Relationen zwischen mehr als zwei Mengen betrachten. Sind das zum Beispiel n Mengen $A_1, \ldots, A_n$, so wird durch eine Teilmenge $R \subseteq A_1 \times \ldots \times A_n$ eine **n-stellige Relation** definiert. Die Elemente von n-stelligen Relationen sind n-Tupel. Beispiele folgen im nächsten Abschnitt.

5.1.1 Anwendung: Relationales Datenmodell

Relationen bilden die Grundlage des relationalen Datenmodells, das in modernen Datenbanken verwendet wird. In Datenbanken stellt man Relationen in Form von

Tabellen dar. Die einzelnen n-Tupel der Relation sind dabei die Zeilen der Tabelle. Ein Beispiel: Die Produkte eines Computerhändlers können übersichtlich in Tabellenform aufgelistet werden. Die einzelnen Spalten der Tabelle gehören dabei zu gewissen **Attributen** wie „Produkt“, „Preis“, usw.:

R_P

P.Nr.	*Produkt*	*Preis*	*H.Nr.*
1	iMac	990	1
2	PC	590	2
3	Server	2150	2
4	Drucker	95	3

Die Zeilen $(1, \text{iMac}, 990, 1), \ldots$ der Tabelle sind Elemente der Produktmenge $\mathbb{N} \times \texttt{CHAR}(20) \times \mathbb{N} \times \mathbb{N}$. (Hier bezeichnet $\texttt{CHAR}(20)$ die Menge aller Zeichenketten (Strings) mit maximal 20 Zeichen.) Damit stellt die Tabelle eine Relation $R_P \subseteq \mathbb{N} \times \texttt{CHAR}(20) \times \mathbb{N} \times \mathbb{N}$ dar. Die Mengen stehen hier also für den Datentyp.

Analog kann die Relation $R_H = \{(1, \text{Apple}, \text{Cupertino}), \ldots\} \subseteq \mathbb{N} \times \texttt{CHAR}(20) \times \texttt{CHAR}(20)$, die nähere Informationen zu den Herstellern enthält, folgendermaßen dargestellt werden:

R_H

H.Nr.	*Name*	*Ort*
1	Apple	Cupertino
2	IBM	New York
3	HP	Palo Alto

Die beiden Relationen R_P und R_H bilden eine kleine Datenbank. Damit haben wir aber noch nichts gewonnen, denn in der Praxis möchte man die Daten ja nicht nur speichern, sondern man möchte auch Abfragen durchführen, wie zum Beispiel: „Welche Produkte werden von IBM hergestellt?“

Nun ist es natürlich möglich, alle Abfragen, die man benötigt, einzeln zu implementieren. Steigen aber die Anzahl der Daten und die Anzahl der benötigten Abfragen, so wird das irgendwann zu mühsam. Deshalb versucht man alle möglichen Abfragen auf einige wenige zu reduzieren, und alle anderen dann auf diese zurückzuführen. Das führt direkt zur so genannten **relationalen Algebra**, die in den meisten Datenbanken als „Structured Query Language“ (**SQL**) implementiert ist. Hier eine Auswahl der wichtigsten Operationen:

- $\sigma_{Bedingung}$ **(SELECT)** wählt alle Zeilen aus, für die die *Bedingung* erfüllt ist (σ, gesprochen „sigma“, ist das kleine griechische s).
  Beispiel: Wählen wir aus R_H alle Zeilen aus, deren Attribut *Name* den Wert „IBM“ hat:
  $$\sigma_{Name=\text{IBM}}(R_H) = \{(2, \text{IBM}, \text{New York})\},$$
  bzw. in Tabellenform dargestellt:

$\sigma_{Name=\text{IBM}}(R_H)$

H.Nr.	*Name*	*Ort*
2	IBM	New York

- $\pi_{j_1,j_2,\ldots}$ (`PROJECT`) wählt die Spalten j_1, j_2, ... aus.
  Beispiel: Projizieren wir R_H auf die Spalten mit den Attributen *Name* und *Ort*:

  $$\pi_{Name,Ort}(R_H) = \{(\text{Apple}, \text{Cupertino}), (\text{IBM}, \text{New York}), (\text{HP}, \text{Palo Alto})\},$$

  bzw. in Tabellenform:

  $\pi_{Name,Ort}(R_H)$

Name	*Ort*
Apple	Cupertino
IBM	New York
HP	Palo Alto

- $R_1[j_1, j_2]R_2$ (`JOIN`) „verkettet“ die Relationen R_1 und R_2 bezüglich der gemeinsamen Attributwerte j_1 (von R_1) und j_2 (von R_2). Die Zeilen der neuen Relation entstehen durch Aneinanderfügung von je einer Zeile der ersten und der zweiten Relation, deren Attributwerte von j_1 und j_2 übereinstimmen.
  Beispiel: Die Relationen R_P und R_H können bezüglich des gemeinsamen Attributs *H.Nr.* verkettet werden:

  $R_P[H.Nr., H.Nr.]R_H$

P.Nr.	*Produkt*	*Preis*	*H.Nr.*	*Name*	*Ort*
1	iMac	990	1	Apple	Cupertino
2	PC	590	2	IBM	New York
3	Server	2150	2	IBM	New York
4	Drucker	95	3	HP	Palo Alto

Die Anfrage „Preisliste aller von IBM hergestellten Produkte“ könnte damit wie folgt formuliert werden:

$$\pi_{Produkt,Preis}(\sigma_{Name=\text{IBM}}(R_P[H.Nr., H.Nr.]R_H))$$

Das sieht auf den ersten Blick zwar wild aus, ist aber nicht so schlimm! Sehen wir es uns einfach Schritt für Schritt an:
Schritt 1: Verkettung $R_P[H.Nr., H.Nr.]R_H$:

$R_1 = R_P[H.Nr., H.Nr.]R_H$

P.Nr.	*Produkt*	*Preis*	*H.Nr.*	*Name*	*Ort*
1	iMac	990	1	Apple	Cupertino
2	PC	590	2	IBM	New York
3	Server	2150	2	IBM	New York
4	Drucker	95	3	HP	Palo Alto

Schritt 2: Auswahl der Zeilen mit „*Name* = IBM“:

$R_2 = \sigma_{Name=\text{IBM}}(R_1)$

P.Nr.	*Produkt*	*Preis*	*H.Nr.*	*Name*	*Ort*
2	PC	590	2	IBM	New York
3	Server	2150	2	IBM	New York

Schritt 3: Projektion auf die Spalten *Produkt* und *Preis*:

$R_3 = \pi_{Produkt,Preis}(R_2)$

Produkt	*Preis*
PC	590
Server	2150

Das Ergebnis unserer Datenbankabfrage ist also in der Tat die gewünschte Preisliste.

Sehen wir uns zuletzt noch an, wie das in der Praxis am Beispiel der Datenbanksoftware MySQL aussieht. In SQL sind Auswahl und Projektion in einem Befehl zusammengefasst:

`SELECT` Spalten `FROM` Tabelle `WHERE` Bedingung

Also zum Beispiel im Fall unserer Datenbank:

```
mysql> SELECT Name,Ort FROM Hersteller WHERE HNr=1;
+-------+-----------+
| Name  | Ort       |
+-------+-----------+
| Apple | Cupertino |
+-------+-----------+
1 row in set (0.00 sec)
```

Unsere Preisliste von vorher erhalten wir mit folgender Anfrage:

```
mysql> SELECT produkt,preis FROM
    -> Produkte INNER JOIN Hersteller ON Hersteller.HNr=Produkte.HNr
    -> WHERE Name="IBM";
+---------+-------+
| Produkt | Preis |
+---------+-------+
| PC      |   590 |
| Server  |  2150 |
+---------+-------+
2 rows in set (0.00 sec)
```

Bemerkung: Oft verwendet man in SQL anstelle von `INNER JOIN` folgende äquivalente Abfrage:

```
mysql> SELECT Produkt,Preis FROM Produkte,Hersteller
    -> WHERE Produkte.HNr=Hersteller.HNr AND Name="IBM";
+---------+-------+
| Produkt | Preis |
+---------+-------+
| PC      |   590 |
| Server  |  2150 |
+---------+-------+
2 rows in set (0.00 sec)
```

Hier bezeichnet „Produkte, Hersteller“ das kartesische Produkt der beiden Relationen (dabei wird jede Zeile der zweiten Relation an jede Zeile der ersten gefügt), aus dem dann jene Zeilen ausgewählt werden, die im Attribut „HNr“ übereinstimmen und deren Attribut *Name* gleich „IBM“ ist.

5.2 Funktionen

Definition 5.21 Eine **Abbildung** oder **Funktion** f von einer Menge D in eine Menge M ist eine Vorschrift, die jedem Element $x \in D$ genau ein Element $f(x) \in M$ zuordnet. Man schreibt dafür:

$$\begin{array}{rccl} f: & D & \to & M \\ & x & \mapsto & f(x) \end{array}$$

und sagt: „x wird auf $f(x)$ abgebildet“ bzw. „$f(x)$ ist das **Bild** (oder der **Funktionswert**) von x“. Die Menge D heißt **Definitionsbereich**, die Menge $f(D) = \{f(x) \mid x \in D\}$ heißt **Bildmenge** und die Menge M heißt **Wertebereich**.

Etwas allgemeiner bezeichnet man für eine beliebige Teilmenge $A \subseteq D$ die Menge $f(A) = \{f(x) \mid x \in A\}$ als Bildmenge von A bzw. für eine beliebige Teilmenge $B \subseteq M$ die Menge $f^{-1}(B) = \{x \in D \mid f(x) \in B\}$ als **Urbildmenge** von B. Die Menge $f^{-1}(\{y\}) = \{x \in D \mid f(x) = y\}$ aller Elemente, die auf y abgebildet werden, heißt **Urbild(menge)** von y. Zum Beispiel ist oben $f(\{1,2,3\}) = \{a,d\}$, $f^{-1}(\{a,d\}) = \{1,2,3,4\}$, $f^{-1}(\{a\}) = \{1,2\}$.

Überlegen wir uns noch einmal anhand eines Beispiels, worauf es bei der Definition einer Funktion ankommt, und betrachten dazu Abbildung 5.4. In diesem Beispiel ist

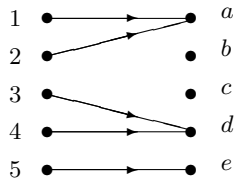


Abbildung 5.4. $f : D \to M$

der Definitionsbereich gleich $D = \{1,2,3,4,5\}$, der Wertebereich $M = \{a,b,c,d,e\}$ und die Bildmenge $f(D) = \{a,d,e\}$. Es ist $f(1) = a$, $f(2) = a$, $f(3) = d$, …, was hier durch „Zuordnungspfeile“ dargestellt wird. In Worten: „Das Bild von 1 ist a, usw.“ oder „Der Funktionswert von 1 ist a, usw.“. Von *jedem* Element des Definitionsbereiches D geht *genau ein* Pfeil weg, d.h., jedes Element aus D hat genau ein Bild. Es müssen aber nicht alle Elemente aus M von einem Pfeil „getroffen“ werden. Jene, die getroffen werden, bilden die Bildmenge $f(D)$. Diese Elemente können ohne weiteres von mehr als einem Pfeil getroffen werden. Zum Beispiel ist a das Bild sowohl von 1 als auch von 2.

Beispiel 5.22 Abbildungen

a) Die Abbildung $f : \mathbb{N} \to \mathbb{N}$ mit $f(n) = n^2$ ordnet jeder natürlichen Zahl ihr Quadrat zu. Also z. B. $f(1) = 1$, $f(2) = 4$, $f(3) = 9$, usw. Definitionsbereich und Wertebereich sind hier die natürlichen Zahlen. Bildmenge: $f(\mathbb{N}) = \{1,4,9,16,\ldots\} = \{n^2 \mid n \in \mathbb{N}\}$. Die Abbildung $g : \mathbb{Z} \to \mathbb{Z}$ mit $g(n) = n^2$

hat einen anderen Definitions- und Wertebereich als f. Bildmenge: $g(\mathbb{Z}) = \{0, 1, 4, 9, 16, \ldots\} = \{n^2 \mid n \in \mathbb{Z}\}$.

b) Die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}$ mit $f(x_1, x_2) = x_1 + x_2$ ordnet je zwei reellen Zahlen (x_1, x_2) ihre Summe zu. Beispiel: $f(1, 5) = 6$. Hier besteht der Definitionsbereich also aus den reellen Zahlenpaaren, der Wertebereich aus den reellen Zahlen. (Man schreibt $f(x_1, x_2)$ anstelle $f((x_1, x_2))$.)

c) Der ASCII-Code ist eine Abbildung, die den Zahlen 0 bis 127 bestimmte Steuerzeichen, Ziffern, Buchstaben und Sonderzeichen zuordnet.

d) Die Vorschrift, die jedem Menschen seine Staatsbürgerschaft zuordnet, ist *keine* Abbildung. Warum? Manche Menschen besitzen mehr als eine Staatsbürgerschaft und von diesen Menschen würde „mehr als ein Pfeil ausgehen“.

Zu einer Abbildung $f : D \to M$ kann man die Relation $G = \{(x, f(x)) \mid x \in D\} \subseteq D \times M$ betrachten. Diese Relation heißt **Graph** der Abbildung. Der Graph der Abbildung aus Abbildung 5.4 ist z. B. $G = \{(1, a), (2, a), (3, d), (4, d), (5, e)\}$. Die Bezeichnung ist kein Zufall: Der Graph einer *reellen Funktion* $f : \mathbb{R} \to \mathbb{R}$ ist (wenn im $\mathbb{R}^2$ gezeichnet) die „Funktionskurve“. Die Relation G hat die Eigenschaft, dass aus $(x, y_1) \in G$ und $(x, y_2) \in G$ immer $y_1 = y_2$ folgt (denn jedem x wird ja genau ein Element $y_1 = y_2 = f(x)$, und nicht mehrere, zugeordnet). Solche Relationen werden als **rechtseindeutig** bezeichnet. In diesem Sinn kann man eine Funktion also auch als eine rechtseindeutige Relation definieren.

Nun wollen wir uns überlegen, welche Eigenschaften Funktionen haben können. Die Abbildung, die jeder natürlichen Zahl $x \in \{0, 1, 2, 3\}$ ihre binäre Darstellung $f(x) \in \{00, 01, 10, 11\}$ zuordnet, hat zwei spezielle Eigenschaften: (1) Keine zwei x haben dieselbe binäre Darstellung. (2) *Jedes* $y \in \{00, 01, 10, 11\}$ ist Bild einer Zahl $x \in \{0, 1, 2, 3\}$. Die erste Eigenschaft nennt man *Injektivität*, die zweite *Surjektivität*.

Definition 5.23 Sei $f : D \to M$ eine Abbildung.

- f heißt **injektiv**, wenn *verschiedene* Elemente von D auf *verschiedene* Elemente von $f(D)$ abgebildet werden, kurz:

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \qquad \text{für alle } x_1, x_2 \in D.$$

  Anders gesagt: f ist injektiv, wenn $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ für alle $x_1, x_2 \in D$ gilt.
- f heißt **surjektiv**, wenn *jedes* Element von M das Bild eines Elements aus D ist, kurz: $f(D) = M$.
- f heißt **bijektiv**, oder **eins-zu-eins Abbildung**, wenn f sowohl injektiv als auch surjektiv ist.

Beispiel: Der ASCII-Code $f(Zahl) = Zeichen$ ist eine bijektive Abbildung.

In unserer „Pfeilsprechweise“ formuliert: Eine Funktion ist *injektiv*, wenn jedes Element aus $f(D)$ von höchstens einem Pfeil getroffen wird. Die Funktion aus Abbildung 5.4 ist nicht injektiv, weil z. B. a von zwei Pfeilen getroffen wird. Eine Funktion ist *surjektiv*, wenn jedes Element aus M von mindestens einem Pfeil getroffen wird. Die Funktion aus Abbildung 5.4 ist nicht surjektiv, weil z. B. c von keinem Pfeil getroffen wird. Und eine Funktion ist bijektiv, wenn *jedes* Element aus M von *genau einem* Pfeil getroffen wird.

Durch geeignete Einschränkung des Definitionsbereiches bzw. Wertebereiches kann eine Funktion immer injektiv bzw. surjektiv gemacht werden. Beispiel: Die Funktion in Abbildung 5.4 wird injektiv, wenn der Definitionsbereich z. B. auf $\{1, 3, 5\}$ eingeschränkt wird. Sie wird surjektiv, wenn der Wertebereich auf $\{a, d, e\}$ eingeschränkt wird.

Beispiel 5.24 Injektiv, surjektiv
Welche der folgenden Abbildungen ist injektiv bzw. surjektiv?
a) $f : \mathbb{Z} \to \mathbb{N}$, $n \mapsto n^2$ b) $g : \mathbb{N} \to \mathbb{N}$, $n \mapsto n^2$
c) $h : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto n + 1$ d) $k : \mathbb{Z}_5 \to \mathbb{Z}_5$, $n \mapsto n + 1$

Lösung zu 5.24
a) Die Abbildung f ist nicht injektiv, denn es gilt nicht, dass je zwei verschiedene Zahlen aus dem Definitionsbereich auch verschiedene Funktionswerte haben. Denn z. B. die Zahlen -2 und 2 aus D haben denselben Funktionswert $f(-2) = f(2) = 4$. Die Abbildung ist auch nicht surjektiv, da nicht alle Zahlen aus $\mathbb{N}$ Funktionswerte sind, d.h., $f(D) \neq M$. Denn z. B. die Zahl 3 tritt nicht als Funktionswert auf.
b) Die Abbildung g ist injektiv, denn zwei verschiedene $n_1, n_2 \in \mathbb{N}$ haben auch verschiedene Funktionswerte $n_1^2 \neq n_2^2$. Vergleich mit a) zeigt, dass die Vorschrift $n \mapsto n^2$ durch Einschränkung des Definitionsbereiches injektiv gemacht werden konnte. Wie vorher ist die Abbildung aber nicht surjektiv.
c) Diese Abbildung ist injektiv, weil zwei verschiedene ganze Zahlen $n_1 \neq n_2$ verschiedene Funktionswerte $n_1 + 1 \neq n_2 + 1$ haben. Sie ist auch surjektiv, weil jede ganze Zahl m Bild einer ganzen Zahl, nämlich von $n = m - 1$, ist. Somit ist die Abbildung bijektiv.
d) Diese Abbildung ist injektiv, weil zwei verschiedene Zahlen aus dem Definitionsbereich $n_1 \neq n_2$ verschiedene Funktionswerte $n_1 + 1 \neq n_2 + 1 \,(\mathrm{mod}\, 5)$ haben. Sie ist auch surjektiv, weil jedes $m \in \mathbb{Z}_5$ Funktionswert eines Elements aus $\mathbb{Z}_5$ ist, nämlich von $n = m + 4 \,(\mathrm{mod}\, 5)$ (4 ist das additive Inverse von 1 in $\mathbb{Z}_5$), ist. Somit ist die Abbildung bijektiv. ■

Die Eigenschaften „injektiv“ und „surjektiv“ sind mit der Lösbarkeit der Gleichung $f(x) = y$ verknüpft. Ist f injektiv, so gibt es für jedes vorgegebene y höchstens eine Lösung x. Ist f surjektiv, so gibt es für jedes y (mindestens) eine Lösung.

Im Fall von Funktionen $f : \mathbb{R} \to \mathbb{R}$ sind die Lösungen von $f(x) = y$ genau die Schnittpunkte des Graphen von $f(x)$ mit der waagrechten Geraden durch y. Das ist in Abbildung 5.5 veranschaulicht: Bei der ersten Funktion gibt es für jede Gerade

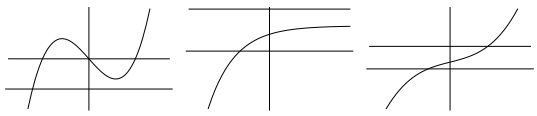


Abbildung 5.5. Injektive bzw. surjektive Funktionen

mindestens einen Schnittpunkt, im eingezeichneten Fall sogar drei; die Funktion ist

daher surjektiv, aber nicht injektiv. Bei der zweiten Funktion gibt es für jede Gerade höchstens einen Schnittpunkt, im eingezeichneten Fall aber keinen; die Funktion ist daher injektiv, aber nicht surjektiv. Bei der dritten Funktion gibt es für jede Gerade genau einen Schnittpunkt; die Funktion ist somit bijektiv.

Eine Funktion beschreibt oft eine Abhängigkeit. Daher nennt man x auch die **unabhängige Variable** oder das **Argument**, und $y = f(x)$ die **abhängige Variable** oder den **Funktionswert**. Im Fall $D \subseteq \mathbb{R}^n$ spricht man von einer **Funktion von mehreren Variablen** und schreibt $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ mit der Abkürzung $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$. Wir wollen uns im Folgenden zunächst auf Funktionen mit $D, M \subseteq \mathbb{R}$ konzentrieren, die man auch **reelle** Funktionen nennt. Um Schreibarbeit zu sparen, nehmen wir – wenn nichts anderes erwähnt ist – für den Definitionsbereich immer $D = \mathbb{R}$ an.

Beispiel 5.25 Reelle Funktionen

a) Die Funktion $f(x) = x^2$ ordnet jeder reellen Zahl x ihr Quadrat zu.
b) Der Definitionsbereich von $f(x) = \frac{1}{x-1}$ besteht aus allen reellen $x \neq 1$, denn für $x = 1$ ist der Bruch nicht definiert.
c) Die so genannte **Vorzeichenfunktion** $\operatorname{sign}(x) = \begin{cases} +1, & x \geq 0 \\ -1, & x < 0 \end{cases}$ hat den Funktionswert $+1$ für alle $x \geq 0$, und den Funktionswert -1 für alle $x < 0$. Die Funktion hat bei $x = 0$ einen „Sprung“.
d) Die Betragsfunktion $f(x) = |x|$ hat bei $x = 0$ einen „Knick“.

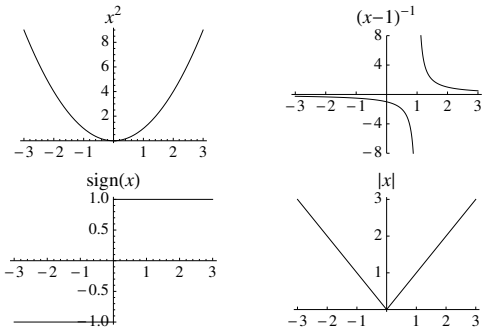


Abbildung 5.6. Die Funktionen aus Beispiel 5.25

Definition 5.26 Sei $n \in \mathbb{N} \cup \{0\}$. Eine Funktion der Form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad \text{mit } a_k \in \mathbb{R},\ k = 0, \ldots, n,$$

heißt **Polynom** vom **Grad** n (falls $a_n \neq 0$). Eine Funktion der Form $f(x) = \frac{p(x)}{q(x)}$, mit $p(x)$, $q(x)$ Polynomen, wird **rationale Funktion** genannt.

Die Lösungen der Gleichung $f(x) = 0$ werden als **Nullstellen** der Funktion f bezeichnet. Speziell im Fall einer quadratischen Funktion $f(x) = x^2 + p\,x + q$ erinnern wir an die Formel

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

für die Nullstellen x_1 und x_2.

Hergeleitet wird diese Formel durch **quadratisches Ergänzen**, $x^2 + p\,x + q = x^2 + 2\frac{p}{2}x + (\frac{p}{2})^2 - (\frac{p}{2})^2 + q = (x + \frac{p}{2})^2 - (\frac{p}{2})^2 + q = 0$, und Auflösen nach x.

Wir können die Formel natürlich auch für eine quadratische Gleichung der Form $a\,x^2 + b\,x + c = 0$ (mit $a \neq 0$) anwenden. Dazu muss nur die ganze Gleichung durch a dividiert werden: $x^2 + \frac{b}{a}x + \frac{c}{a} = 0$.

Wenn zwei Funktionen f und g denselben Definitionsbereich haben, so können wir daraus neue Funktionen $f + g$, $f \cdot g$ und $\frac{f}{g}$ bilden:

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (f \cdot g)(x) &= f(x) \cdot g(x) \\ \left(\frac{f}{g}\right)(x) &= \frac{f(x)}{g(x)} \quad \text{(Definitionsbereich bilden hier nur jene } x \text{ mit } g(x) \neq 0) \end{aligned}$$

Wir können aus zwei Funktionen auch eine neue Funktion bilden, indem wir die Funktionsvorschriften hintereinander ausführen.

Definition 5.27 Seien $f : D_f \to M$ und $g : D_g \to N$ Funktionen. Die **Hintereinanderausführung** oder **Verkettung** von f und g ist die Funktion $f \circ g : D_g \to M$ mit:

$$x \mapsto (f \circ g)(x) = f(g(x)).$$

Ein Element x aus dem Definitionsbereich von g wird also auf $g(x)$ abgebildet, und darauf wird dann f angewendet, woraus $f(g(x))$ resultiert. Damit die Hintereinanderausführung überhaupt Sinn macht, muss der zu x zugehörige Funktionswert $g(x)$ natürlich im Definitionsbereich von f liegen, es muss also $g(D_g) \subseteq D_f$ gelten.

Die Verkettung von Funktionen entspricht der Verkettung der zugehörigen Relationen, also dem Graphen $G_{f \circ g} = G_f \circ G_g$.

Beispiel 5.28 Hintereinanderausführung von Funktionen
Bilden Sie $f \circ g$:
a) $f(x) = x^2$, $g(x) = 3x$ b) $f(x) = \frac{1}{x}$, $g(x) = x^3$, wobei $x \neq 0$
Schreiben Sie als Hintereinanderausführung $f \circ g$ zweier Funktionen f und g:
c) $h(x) = (x+1)^5$ d) $h(x) = |x - 2|$

Lösung zu 5.28

a) Wir setzen in die Definition von $f \circ g$ ein und lösen nach und nach auf: $(f \circ g)(x) = f(g(x)) = (g(x))^2 = (3x)^2 = 9x^2$. Es ist übrigens gleichgültig, ob zuerst $f(x)$ oder $g(x)$ aufgelöst wird, d.h. auch $(f \circ g)(x) = f(g(x)) = f(3x) = (3x)^2 = 9x^2$ führt zum Ziel.

b) $(f \circ g)(x) = f(g(x)) = \frac{1}{g(x)} = \frac{1}{x^3} = x^{-3}$ für $x \neq 0$.

c) Wir fassen Teile der Vorschrift h unter neuen Namen g und f zusammen: $h(x) = (x+1)^5 = g(x)^5 = f(g(x))$ mit $f(x) = x^5$ und $g(x) = x+1$.
d) $h(x) = |x-2| = |g(x)| = f(g(x))$ mit $f(x) = |x|$ und $g(x) = x-2$. ■

Beispiel 5.29 Umrechnung von Einheiten
Der Benzinverbrauch B eines Fahrzeuges ist abhängig von der Geschwindigkeit v:

$$B(v) = 2 + 0.5v + 0.25v^2.$$

Dabei ist v in Meilen pro Stunde anzugeben und B ist in (US-)Gallonen pro Meile abzulesen. Wandeln Sie diese Formel in eine Formel um, bei der die Geschwindigkeit in Kilometer pro Stunde angegeben wird und der Verbrauch in Liter pro Kilometer abgelesen werden kann.

Lösung zu 5.29 Die Formel, von der wir ausgehen, lautet

$$B_G(v_M) = 2 + 0.5v_M + 0.25v_M^2,$$

wobei v_M die Geschwindigkeit in M/h ist und B_G den Benzinverbrauch in G/M bedeutet. Da eine Meile 1.60935 Kilometern entspricht, entspricht eine Meile pro Stunde 1.60935 Kilometern pro Stunde. Ist v_{km} die Geschwindigkeit in km/h, so gilt also $v_{km} = 1.60935 v_M$ bzw. $v_M = v_{km}/1.60935 = 0.621369 v_{km}$. Nennen wir die Funktion, die diese Umrechnung bewirkt, f:

$$v_M = f(v_{km}) = 0.621369 v_{km}.$$

Wir erhalten damit als ersten Schritt die Formel

$$(B_G \circ f)(v_{km}) = B_G(\underbrace{f(v_{km})}_{=v_M}) = B_G(0.621369 v_{km}) = 2 + 0.31 v_{km} + 0.1 v_{km}^2$$

(auf zwei Stellen gerundet), in die die Geschwindigkeit in km/h eingegeben wird (v_{km}) und die den Benzinverbrauch aber noch nach wie vor in Gallonen pro Meile liefert.

Im zweiten Schritt müssen wir die Formel noch so ändern, dass der berechnete Zahlenwert den Benzinverbrauch in Liter/Kilometer – nennen wir ihn B_L – bedeutet. Da eine Gallone 3.7853 Litern entspricht, ist 1 G/M = 3.7853 Liter/1.60935 Kilometer = 2.35207 L/km. Also ist $B_L = 2.35207 B_G$. Nennen wir die Funktion, die diese Umrechnung durchführt, g:

$$B_L = g(B_G) = 2.35207 B_G.$$

Damit lautet die gesuchte Formel

$$(g \circ B_G \circ f)(v_{km}) = g(2 + 0.31 v_{km} + 0.1 v_{km}^2) = 4.7 + 0.73 v_{km} + 0.23 v_{km}^2$$

(auf zwei Stellen gerundet). ■

Wir haben oben überlegt, dass der ASCII-Code jeder Zahl bijektiv ein Zeichen zuordnet. Zum Beispiel ist $f(65) = A$. Da die Abbildung bijektiv ist, ist es also möglich, von einem Zeichen wieder auf die zugehörige Zahl rückzuschließen. Jene Funktion, die diesen Rückschluss bewirkt, heißt *Umkehrfunktion* von f:

Definition 5.30 Ist die Funktion $f : D \to M$ bijektiv, dann heißt die Funktion, die jedem $y \in M$ das eindeutig bestimmte $x \in D$ mit $y = f(x)$ zuordnet, die **Umkehrfunktion** (oder **inverse Funktion**) von f. Sie wird mit f^{-1} bezeichnet.

Die Umkehrfunktion entspricht der inversen Relation: $G_{f^{-1}} = G_f^{-1}$.

Das ist also die Funktion $f^{-1} : M \to D$ mit folgender Eigenschaft: $f^{-1}(y) = x$ genau dann, wenn $y = f(x)$. Insbesondere gilt

$$(f^{-1} \circ f)(x) = x \qquad \text{und} \qquad (f \circ f^{-1})(y) = y$$

für alle $x \in D$ bzw. $y \in M$. Das bedeutet, dass f^{-1} die Wirkung von f rückgängig macht und analog f die Wirkung von f^{-1}. Beispiel: Da beim ASCII-Code $f(65) = A$, so folgt $f^{-1}(A) = 65$.

Achtung: Die Umkehrfunktion $f^{-1}(x)$ einer reellen Funktion f wird leicht mit der Funktion $\frac{1}{f(x)}$ verwechselt. Diese beiden Funktionen haben aber nichts miteinander zu tun!

Beispiel 5.31 Umkehrfunktion
Berechnen Sie die Umkehrfunktion der folgenden bijektiven Funktionen:
a) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x + 1$ b) $g : \mathbb{Z}_8 \to \mathbb{Z}_8$, $n \mapsto 3n$

Lösung zu 5.31

a) Zu jedem $y \in f(\mathbb{R}) = \mathbb{R}$ gibt es ein eindeutig bestimmtes $x \in \mathbb{R}$ mit $y = f(x) = 2x + 1$. Dieses x erhalten wir als Funktion von y, indem wir die Beziehung $y = 2x + 1$ nach x auflösen: $x = f^{-1}(y) = \frac{1}{2}(y - 1)$. Manchmal vertauscht man noch die Bezeichnung der Variablen, um wieder mit x das Argument, und mit y den Funktionswert zu bezeichnen. Dann ist $f^{-1}(x) = \frac{1}{2}(x - 1)$. Probe: $(f^{-1} \circ f)(x) = f^{-1}(2x + 1) = \frac{1}{2}((2x + 1) - 1) = x$.

b) Wir müssen die Gleichung $m = 3n$ in $\mathbb{Z}_8$ nach n auflösen. Das geschieht durch Multiplikation mit dem Kehrwert in $\mathbb{Z}_8$, also mit $\frac{1}{3} = \frac{1+8}{3} = 3$ in $\mathbb{Z}_8$: $n = 3m \pmod 8$. Also gilt $g^{-1}(m) = 3m$, d.h., die Funktion g ist gleich ihrer Umkehrfunktion. (Hätte das multiplikative Inverse von 3 *nicht* existiert, so wäre die Gleichung nicht eindeutig lösbar gewesen; in diesem Fall wäre die Funktion nicht invertierbar gewesen.) ■

Eine Funktion, die wie g im letzten Beispiel gleich ihrer Umkehrfunktion ist, wird als **Involution** oder **selbstinverse Funktion** bezeichnet. Weitere Beispiele für selbstinverse Funktionen sind $f(x) = -x$, die Negation in der Schaltalgebra oder die komplexe Konjugation.

Bei reellen bijektiven Funktionen erhält man den Graphen der Umkehrfunktion f^{-1}, indem man den Graph von f an der Geraden $g(x) = x$ spiegelt. Abbildung 5.7 zeigt die Graphen einer Funktion $f(x)$, ihrer Umkehrfunktion $f^{-1}(x)$, und der Geraden $g(x) = x$.

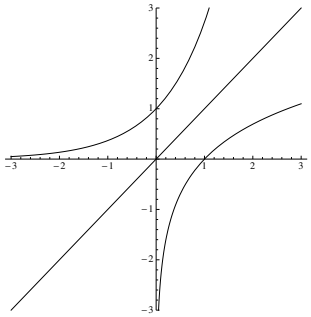


Abbildung 5.7. Eine Funktion und ihre Umkehrfunktion

Satz 5.32 Sind die Funktionen f und g beide bijektiv, so ist auch ihre Verkettung $f \circ g$ bijektiv. Die Umkehrfunktion erhält man, indem man zuerst f und dann g umkehrt. Es gilt also

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}.$$

Beispiel 5.33 Umkehrung einer Verkettung
Gegeben sind die einfachen Verschlüsselungsvorschriften $f, g : \mathbb{Z}_{11} \to \mathbb{Z}_{11}$ mit $f(x) = x + 3$ und $g(x) = 7x$. Geben Sie die Verschlüsselungsvorschrift $f \circ g$ sowie die Vorschrift zum Entschlüsseln an.

Lösung zu 5.33 Aus Schreibfaulheit lassen wir den Zusatz „mod 11“ weg, es ist aber jede Rechnung modulo 11 zu verstehen: $(f \circ g)(x) = f(g(x)) = f(7x) = 7x + 3$ ist die Verschlüsselungsvorschrift. Entschlüsselt wird mit $(f \circ g)^{-1}(x) = (g^{-1} \circ f^{-1})(x)$ $= g^{-1}(f^{-1}(x)) = g^{-1}(x - 3) = \frac{1}{7}(x - 3) = 8(x - 3) = 8x - 24 = 8x + 9$ (hier haben wir verwendet, dass der Kehrwert von 7 in $\mathbb{Z}_{11}$ gleich 8 ist). ■

Injektivität (und damit die Umkehrbarkeit einer Funktion) ist eng mit folgender Eigenschaft verbunden:

Definition 5.34 Sei $f : D \subseteq \mathbb{R} \to M \subseteq \mathbb{R}$ eine Funktion.

- f heißt **streng monoton wachsend**, wenn für wachsende x-Werte stets die zugehörigen Funktionswerte wachsen, wenn also

$$x_1 < x_2 \quad \Rightarrow \quad f(x_1) < f(x_2) \quad \text{für alle } x_1, x_2 \in D.$$

- f heißt **streng monoton fallend**, wenn für wachsende x-Werte stets die zugehörigen Funktionswerte fallen, wenn also

$$x_1 < x_2 \quad \Rightarrow \quad f(x_1) > f(x_2) \quad \text{für alle } x_1, x_2 \in D.$$

- Wenn anstelle von $<$ und $>$ jeweils $\leq$ bzw. $\geq$ gilt, dann nennt man die Funktion nur **monoton wachsend** bzw. **monoton fallend**.

Ob eine reelle Funktion injektiv ist, kann daran erkennen, ob sie streng monoton ist:

Satz 5.35 Eine reelle Funktion $f : D \subseteq \mathbb{R} \to f(D) \subseteq \mathbb{R}$ ist injektiv, wenn sie entweder *streng* monoton wachsend oder *streng* monoton fallend ist. Die Umkehrfunktion ist dann ebenfalls streng monoton im gleichen Sinn.

Es gilt also: Streng monoton wachsend oder fallend $\Rightarrow$ injektiv.

Wenn die Funktionswerte nämlich streng wachsen oder fallen, dann haben ja zwei verschiedene Argumente x_1, x_2 immer zwei verschiedene Bilder $f(x_1) < f(x_2)$ bzw. $f(x_1) > f(x_2)$, die Abbildung ist also injektiv. Die Umkehrung (injektiv $\Rightarrow$ streng monoton) gilt nur, wenn f *stetig* ist (das bedeutet anschaulich, dass f keine Sprünge hat – eine genaue Definition folgt in Band 2).

Beispiel 5.36 Streng monoton wachsend/fallend
Welche der folgenden Funktionen sind streng monoton wachsend oder fallend?
a) $p(x) = 2x + 1$ b) $g(x) = -2x + 1$ c) $h(x) = 1$ d) $f(x) = x^2$

Lösung zu 5.36 Die Funktionen sind in Abbildung 5.8 gezeichnet.

a) Die Gerade p ist streng monoton wachsend. Denn für alle $x_1, x_2 \in \mathbb{R}$ gilt: Wenn $x_1 < x_2$, dann gilt auch für die zugehörigen Funktionswerte: $p(x_1) = 2x_1 + 1 < p(x_2) = 2x_2 + 1$.
b) Die Gerade g ist streng monoton fallend, denn aus $x_1 < x_2$ folgt: $g(x_1) = -2x_1 + 1 > g(x_2) = -2x_2 + 1$. Bei einer Geraden gibt das Vorzeichen der Steigung (hier -2, im Beispiel a) $+2$) an, ob sie streng monoton wächst oder fällt.
c) Die konstante Funktion h ist weder streng monoton wachsend noch streng monoton fallend.
d) Wenn f auf ganz $\mathbb{R}$ definiert ist, dann ist diese Funktion weder streng monoton wachsend noch streng monoton fallend. Wenn wir den Definitionsbereich aber einschränken, zum Beispiel auf $x \geq 0$, dann ist die Funktion hier streng monoton wachsend (und daher injektiv), denn aus $x_1 < x_2$ folgt $x_1^2 < x_2^2$. Analog ist sie für $x \leq 0$ streng monoton fallend (und injektiv), denn aus $x_1 < x_2$ folgt dann $x_1^2 > x_2^2$. ■

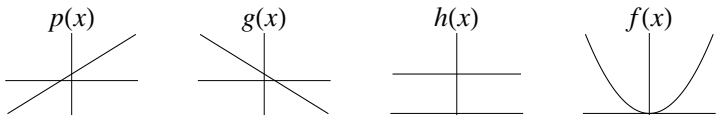


Abbildung 5.8. Die Funktionen aus Beispiel 5.36

Wir haben im Beispiel 5.36 d) gesehen, dass die Funktion $f : [0, \infty) \to [0, \infty)$ mit $f(x) = x^2$ umkehrbar ist, da sie hier streng monoton wächst. Die Umkehrfunktion ist gerade die Wurzelfunktion $f^{-1} : [0, \infty) \to [0, \infty)$ mit $f^{-1}(x) = \sqrt{x}$. Auch diese Funktion ist streng monoton wachsend. Allgemein gilt:

Satz 5.37 Die **Potenzfunktion** $f : [0,\infty) \to [0,\infty)$ mit $f(x) = x^n$ ist für beliebiges $n \in \mathbb{N}$ streng monoton wachsend und damit injektiv. Da $f([0,\infty)) = [0,\infty)$ gilt, ist sie auch surjektiv, und somit insgesamt bijektiv. Die Umkehrfunktion ist $f^{-1} : [0,\infty) \to [0,\infty)$ mit $f^{-1}(x) = \sqrt[n]{x}$.

Beispiel: $f(x) = x^3$ hat die Umkehrfunktion $f^{-1}(x) = \sqrt[3]{x}$ (beide Funktionen haben Definitionsbereich $[0,\infty)$). In diesem Fall könnten wir die Funktion und ihre Umkehrfunktion sogar auf ganz $\mathbb{R}$ definieren, indem wir $f^{-1}(x) = -\sqrt[3]{|x|}$ für $x < 0$ setzen. Das geht natürlich mit jeder ungeraden Potenz. Zeichnen Sie die zugehörigen Graphen!

Satz 5.38 Die **Exponentialfunktion** $f : \mathbb{R} \to (0,\infty)$ mit $f(x) = a^x$ ist für $0 < a < 1$ streng monoton fallend und für $a > 1$ streng monoton wachsend. Ihre Umkehrfunktion wird als **Logarithmusfunktion** bezeichnet: $f^{-1} : (0,\infty) \to \mathbb{R}$ mit $f^{-1}(x) = \log_a(x)$.

Besonders wichtig ist der Fall $a = \mathrm{e} = 2.718\ldots$ (Euler'sche Zahl), in dem man von *der* Exponentialfunktion $\exp(x) = \mathrm{e}^x$ und vom *natürlichen* Logarithmus $\ln(x) = \log_{\mathrm{e}}(x)$ spricht. Sie sind in Abbildung 5.7 dargestellt.

Streng monoton wachsende Funktionen erhalten die Ordnung: Das bedeutet, dass man eine streng monoton wachsende Funktion auf beiden Seiten einer Ungleichung anwenden kann. Die neue Ungleichung ist genau dann richtig, wenn es auch die ursprüngliche war, d.h.: $a < b \;\Leftrightarrow\; f(a) < f(b)$ für eine streng monoton wachsende Funktion f. Analoges gilt für die Anwendung von streng monoton fallenden Funktionen auf beiden Seiten einer Ungleichung, nur muss dann die Richtung des Ungleichungszeichens umgedreht werden: $a < b \;\Leftrightarrow\; f(a) > f(b)$ für eine streng monoton fallende Funktion f. Streng monoton fallende Funktionen kehren die Ordnung also um.

Beispiel 5.39 Anwendung einer streng monotonen Funktion auf beiden Seiten einer Ungleichung

a) $f(x) = x^2$ ist für $x \geq 0$ streng monoton wachsend. Daher gilt:

$$a < b \quad \Leftrightarrow \quad a^2 < b^2 \quad \text{für } a, b \geq 0.$$

b) $f(x) = x^2$ für $x \leq 0$ streng monoton fallend. Somit gilt:

$$a < b \quad \Leftrightarrow \quad a^2 > b^2 \quad \text{für } a, b \leq 0.$$

Beispiel: $-4 < -3 \quad \Leftrightarrow \quad 16 > 9.$

Wenden wir hintereinander zwei Funktionen an, die die Ordnung erhalten, so bleibt die Ordnung auch insgesamt erhalten. Kehrt eine der beiden Funktionen die Ordnung um, so wird die Ordnung insgesamt umgedreht. Drehen *beide* Funktionen die Ordnung um, so bleibt die Ordnung erhalten:

Satz 5.40 Die Verkettung monotoner Funktionen ist wieder monoton, und zwar

- monoton wachsend, wenn beide Funktionen monoton im gleichen Sinn sind, und
- monoton fallend, wenn die Funktionen monoton in verschiedenem Sinn sind.

Beispiel 5.41 Verkettung monotoner Funktionen

a) $f(x) = x^2$ ist streng monoton wachsend für $x \geq 0$, $g(x) = 3x + 4$ ist streng monoton wachsend für alle $x \in \mathbb{R}$. Dann ist $(f \circ g)(x) = f(3x+4) = (3x+4)^2$ für $3x + 4 \geq 0$, also $x \geq -\frac{4}{3}$ streng monoton wachsend; ebenso ist $(g \circ f)(x) = g(x^2) = 3x^2 + 4$ streng monoton wachsend für alle $x \geq 0$.

b) $f(x) = x^2$ ist streng monoton wachsend für $x \geq 0$, $g(x) = -3x + 4$ ist streng monoton fallend für alle $x \in \mathbb{R}$. Daher ist $(f \circ g)(x) = f(-3x+4) = (-3x+4)^2$ für $-3x + 4 \geq 0$, also $x \leq \frac{4}{3}$ streng monoton fallend; ebenso ist $(g \circ f)(x) = g(x^2) = -3x^2 + 4$ streng monoton fallend für alle $x \geq 0$.

Das Beispiel $f(x) = x^2$ führt uns zu einer weiteren Eigenschaft, die eine Funktion besitzen kann. Die Funktionswerte dieser Funktion sind *nach oben unbeschränkt* und *nach unten beschränkt*:

Definition 5.42 Sei $f : D \to \mathbb{R}$ eine Funktion.

- f heißt **nach oben beschränkt**, wenn es ein $K \in \mathbb{R}$ gibt, sodass

  $$f(x) \leq K \quad \text{für alle } x \in D.$$

  Man nennt dann K eine **obere Schranke** von f. Anschaulich bedeutet das, dass der Funktionsgraph von f unterhalb der Geraden $y = K$ verläuft.
- f heißt **nach unten beschränkt**, wenn es ein $k \in \mathbb{R}$ gibt, sodass

  $$k \leq f(x) \quad \text{für alle } x \in D.$$

  Man nennt dann k eine **untere Schranke** von f. Anschaulich bedeutet das, dass der Funktionsgraph von f oberhalb der Geraden $y = k$ verläuft.
- f heißt **beschränkt**, wenn sie nach oben *und* nach unten beschränkt ist. In diesem Fall gilt also

  $$k \leq f(x) \leq K \quad \text{für alle } x \in D.$$

  Eine Funktion, die nicht beschränkt ist, heißt **unbeschränkt**.

Graphisch veranschaulicht: Eine Funktion ist beschränkt genau dann, wenn der Funktionsgraph zwischen zwei Geraden $y = k$ und $y = K$ verläuft. Das ist gleichbedeutend damit, dass es eine Konstante $a > 0$ gibt, sodass alle Funktionswerte $f(x) \geq -a$ und $f(x) \leq a$ sind, kurz: $|f(x)| \leq a$ für alle $x \in D$.

Beispiel 5.43 Beschränkte Funktion

Sind die folgenden Funktionen für $x \in \mathbb{R}$ beschränkt?

a) $f(x) = x^2 + 1$ b) $g(x) = \frac{1}{x^2+1}$

Lösung zu 5.43

a) Die Funktion ist nach unten beschränkt, da $f(x) = x^2 + 1 \geq 1$ für alle $x \in \mathbb{R}$. Aber sie ist nach oben unbeschränkt, denn für jede noch so große Schranke $K > 0$ ist der Funktionswert an der Stelle $x = \sqrt{K}$ größer als K: $f(\sqrt{K}) = K + 1 > K$. Graphisch veranschaulicht in Abbildung 5.9: Der Funktionsgraph kann zwar nach unten durch die Gerade $y = 1$ begrenzt werden, jedoch kann er nach oben hin durch keine Gerade $y = K$ begrenzt werden.

b) Die Funktion ist in Abbildung 5.9 dargestellt. g ist nach oben beschränkt, da für alle reellen x gilt, dass $x^2 + 1 \geq 1$ ist und somit $g(x) = \frac{1}{x^2+1} \leq 1$ folgt. Die Funktion ist auch nach unten beschränkt, da $g(x) \geq 0$ für alle $x \in \mathbb{R}$. g ist also, kurz gesagt, beschränkt. Graphisch veranschaulicht: Der Funktionsgraph verläuft zwischen den Geraden $y = 1$ und $y = 0$. ■

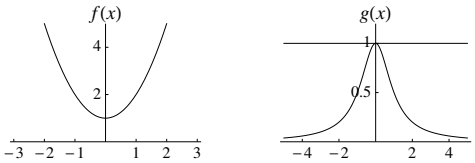


Abbildung 5.9. Die Funktionen aus Beispiel 5.43

Zuletzt wollen wir noch an die trigonometrischen Funktionen Sinus und Kosinus erinnern: Sei x die Länge des Bogenstückes am Einheitskreis, die vom Punkt $(1, 0)$ beginnend im positiven Sinn (d.h. entgegen dem Uhrzeigersinn) gemessen wird, und

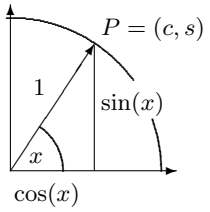


Abbildung 5.10. Definition von Sinus und Kosinus am Einheitskreis

$P = (c, s)$ der zugehörige Punkt (vergleiche Abbildung 5.10). Dann definieren wir

$$\sin(x) = s \quad \text{bzw.} \quad \cos(x) = c$$

und nennen die beiden Funktionen **Sinus** bzw. **Kosinus** (Abbildung 5.11). Dabei kann x als Maß für den Winkel aufgefasst werden (**Bogenmaß**). Eine volle Umdrehung auf dem Einheitskreis entspricht dem Winkel 2π. Um Sinus und Kosinus für alle $x \in \mathbb{R}$ zu definieren, lassen wir auch Mehrfachumdrehungen zu ($x = 4\pi$ entspricht also zwei Umdrehungen) und *negatives* x soll bedeuten, dass um $|x|$ im negativen Sinn (d.h. im Uhrzeigersinn) gedreht wird.

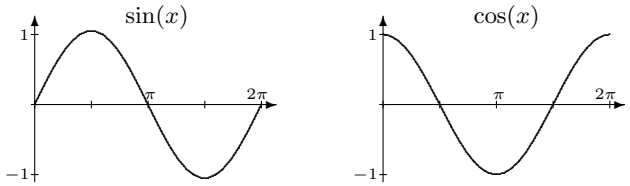


Abbildung 5.11. Sinus- und Kosinusfunktion

Aus der Definition am Einheitskreis folgt $\sin^2(x) + \cos^2(x) = 1$ (Satz von Pythagoras). Insbesondere sind die trigonometrischen Funktionen beschränkt: $|\sin(x)| \leq 1$ bzw. $|\cos(x)| \leq 1$. Außerdem ist der Sinus auf $[-\frac{\pi}{2}, \frac{\pi}{2}]$ streng monoton wachsend und der Kosinus auf $[0, \pi]$ streng monoton fallend. Die zugehörigen Umkehrfunktionen heißen **Arcusfunktionen**, $\arcsin(x)$ bzw. $\arccos(x)$, und sind auf dem Intervall $x \in [-1, 1]$ definiert.

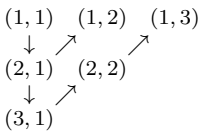
Wir gehen davon aus, dass Ihnen Potenz-, Exponential- und Logarithmusfunktionen sowie trigonometrische Funktionen bereits bekannt sind.

Abschließend noch ein kleiner Ausflug zu Mengen: Zwei endliche Mengen heißen **gleich mächtig**, wenn sie die gleiche Anzahl von Elementen haben. Für unendliche Mengen lässt sich diese Definition erweitern, indem man zwei Mengen A, B gleich mächtig nennt, wenn es eine bijektive Abbildung $f : A \to B$ gibt, die jedem Element aus A ein Element aus B zuordnet. Damit erhalten wir eine Äquivalenzrelation, für die man $|A| = |B|$ schreibt. Die Mächtigkeit $|A|$ einer Menge wird auch als **Kardinalzahl** bezeichnet. Achtung: Für unendliche Mengen kann es passieren, dass eine strikte Teilmenge gleich mächtig wie die Originalmenge ist. Zum Beispiel kann man mit Hilfe der Funktion $\tan(\pi x)$ zeigen, dass das reelle Intervall $[-1, 1]$ gleich mächtig wie $\mathbb{R}$ ist.

Der deutsche Mathematiker David Hilbert (1862–1943) hat vorgeschlagen, ein Hotel mit unendlich vielen Zimmern zu bauen, denn dann könnte man alle Gäste unterbringen: Ist das Hotel voll belegt und es kommt ein weiterer Gast, so gibt man dem neuen Gast das erste Zimmer, verlegt den Gast aus dem ersten ins zweite, den vom zweiten ins dritte, usw., und schon hat jeder Gast wieder ein Zimmer. Genial, nicht? Angeblich wird sogar schon daran gebaut; ein Eröffnungstermin steht aber noch nicht fest.

Eine Menge, die höchstens gleich mächtig wie die natürlichen Zahlen ist, wird als **abzählbar** bezeichnet. Anders gesagt: Die Elemente einer abzählbaren Menge lassen sich mit Hilfe der natürlichen Zahlen durchnummerieren. Beispiel: Alle geraden natürlichen Zahlen sind abzählbar (betrachte die Abbildung $n \mapsto 2n$), ebenso alle ganzen Zahlen ($n \mapsto \frac{n}{2}$, falls n gerade, und $n \mapsto -\frac{n-1}{2}$, falls n ungerade). Es ist sogar $A \times B$ abzählbar, falls A und B abzählbar sind. Daraus folgt, dass die Menge der rationalen Zahlen abzählbar ist (denn $\mathbb{Q}$ kann als Teilmenge der Paare $(p, q) \in \mathbb{Z} \times \mathbb{N}$ aufgefasst werden).

Um zu sehen, dass $A \times B$ abzählbar ist, können wir annehmen, dass wir A und B schon abgezählt haben. Dann können wir alle Paare (a_m, b_n) mit einer verschachtelten FOR-Schleife abzählen (**Cantor'sches Diagonalverfahren**), indem die äußere Schleife über alle m läuft, und die innere Schleife die Paare (a_{m-n+1}, b_n) von $n = 1$ bis $n = m$ zählt:



Man kann zeigen, dass die reellen Zahlen *nicht* abzählbar sind.

Wären sie abzählbar, so wären insbesondere die reellen Zahlen zwischen 0 und 1 abzählbar. Sei also x_n eine Aufzählung der reellen Zahlen zwischen 0 und 1. Nun konstruieren wir eine irrationale Zahl $y \in [0,1]$, indem wir ihre Dezimalstellen nach dem Komma so wählen, dass die n-te Stelle verschieden ist von der n-ten Dezimalstelle von x_n. Ist also z. B. $x_4 = 0.259\mathbf{3}24\ldots$, so können wir für die vierte Dezimalstelle von y eine der Zahlen $0, 1, 2, 4, 5, 6, 7, 8, 9$ (nicht aber 3) wählen. Insbesondere ist $y \neq x_n$ für alle n (y und x_n unterscheiden sich ja an der n-ten Dezimalstelle), und damit fehlt y in unserer Aufzählung – ein Widerspruch.

5.3 Kontrollfragen

Fragen zu Abschnitt 5.1: Relationen

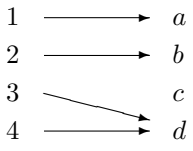
Erklären Sie folgende Begriffe: binäre Relation, n-stellige Relation, inverse Relation, Verkettung von Relationen, reflexiv, symmetrisch, asymmetrisch, antisymmetrisch, transitiv, Identitätsrelation, Äquivalenzrelation, Äquivalenzklassen, Vertreter einer Äquivalenzklasse, Ordnung, strikte Ordnung, vergleichbar, totale/partielle Ordnung, reflexive/symmetrische/transitive Hülle.

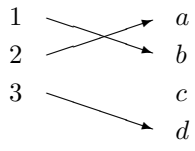
1. R sei eine Relation zwischen A und B. Richtig oder falsch:
   a) $R \in A \times B$
   b) Wenn $a \in A$ zu $b \in B$ in Relation steht, so schreibt man: $\{a, b\} \in R$ oder aRb.
2. Geben Sie alle Elemente der Relation $a < b$ auf der Menge $A = \{1, 2, 3\}$ an.
3. Wenn R die Relation „m beherrscht Instrument i“ zwischen einer Menge M von Musikern und einer Menge I von Instrumenten ist, was sagt $R = M \times I$ dann aus?
4. $R = \{(Max, Anna), (Max, Hans), (Moritz, Max)\}$ sei die Relation „v ist Vater von k“ auf der Menge $\{Max, Moritz, Anna, Hans\}$. Wie viele Kinder hat Max? Wie stehen Max und Moritz zueinander?
5. Richtig oder falsch:
   a) Wenn $R \subseteq A \times B$, dann ist $R^{-1} \subseteq B \times A$.
   b) Wenn $R \subseteq A \times B$ und $S \subseteq B \times C$, dann ist $S \circ R \subseteq A \times C$ und $R \circ S$ ist nicht definiert.
6. $R = \{(1, 1), (2, 2)\}$ und $S = \{(1, 1), (2, 2), (1, 2)\}$ seien Relationen auf $A = \{1, 2\}$. Geben Sie die Vereinigung und den Durchschnitt von R und S, sowie das Komplement von R in $A \times A$ an. Ist eine Relation eine Teilmenge der anderen?
7. Geben Sie an:
   a) Durchschnitt der Relationen „größer oder gleich“ ($\geq$) und „kleiner oder gleich“ ($\leq$) auf $\mathbb{N}$.
   b) Durchschnitt der Relationen „größer“ ($>$) und „kleiner“ ($<$) auf $\mathbb{N}$.
   c) Komplement der Relation „größer oder gleich“ ($\geq$) auf $\mathbb{N}$.

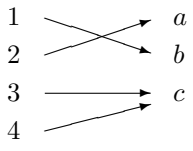
8. Gegeben sind die Relationen $R = \{(a, b)\}$ und $S = \{(a, b), (c, a)\}$ auf $A = \{a, b, c\}$. Geben Sie $S \circ R$ und $R \circ S$ an.
9. Erklären Sie, was
   a) nicht reflexiv b) nicht symmetrisch c) nicht asymmetrisch d) nicht antisymmetrisch e) nicht transitiv
   bedeutet.
10. Gegeben sind die Menge $A = \{a, b, c\}$ und die Relation $R = \{(a, a), (a, b), (b, a), (b, b), (c, c)\}$. Was muss aus der Relation R zum Beispiel entfernt werden, damit R a) antisymmetrisch b) asymmmetrisch wird?
11. Gegeben sind die Menge $A = \{a, b, c\}$ und die Relation $S = \{(a, a), (a, c), (c, c)\}$. Ist S reflexiv, symmetrisch, asymmetrisch, antisymmetrisch oder transitiv?
12. Richtig oder falsch:
    asymmetrisch $\Rightarrow$ antisymmetrisch; die Umkehrung gilt aber nicht.
13. Geben Sie die Äquivalenzklassen der Äquivalenzrelation „a hat bei Division durch 2 den gleichen Rest wie b“ auf $\mathbb{Z}$ an. Liegt jede ganze Zahl in irgendeiner Äquivalenzklasse? Gibt es eine ganze Zahl, die gleichzeitig in zwei verschiedenen Äquivalenzklassen liegt?
14. Zwei vierstellige Dualzahlen sollen als äquivalent betrachtet werden, wenn sie in den linken ersten beiden Stellen übereinstimmen. Geben Sie die Äquivalenzklassen an.
15. Was ist der Unterschied zwischen einer Ordnung und einer strikten Ordnung?
16. Ist $\{(1, 2), (1, 1), (2, 2), (3, 3)\}$ eine totale Ordnung oder eine partielle Ordnung auf $A = \{1, 2, 3\}$?
17. Richtig oder falsch: Die transitive Hülle von R zu bilden bedeutet, R um jene Paare zu erweitern, die notwendig sind, damit die Eigenschaft „transitiv“ gegeben ist. Es werden aber nur die dafür unbedingt notwendigen Paare hinzugefügt, und keines mehr. Die transitive Hülle ist eindeutig bestimmt.

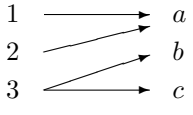
Fragen zu Abschnitt 5.2: Funktionen

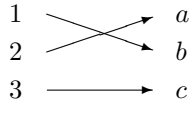
Erklären Sie zunächst die folgenden Begriffe: Funktion (Abbildung), Definitionsbereich, Wertebereich, Bildmenge, Funktionswert (Bild) von x, injektiv, surjektiv, bijektiv, Verkettung (Hintereinanderausführung) von Funktionen, Umkehrfunktion; streng monoton fallend/wachsend, beschränkt.

1. Handelt es sich um eine Abbildung? Wenn ja, geben Sie die Bildmenge an und stellen Sie weiters fest, ob die Abbildung surjektiv, injektiv oder bijektiv ist.
   a)
   

   b)
   

   c)
   

   d)
   

   e)
   

2. Wie hängen Relationen und Funktionen zusammen?
3. Was bedeutet: a) nicht injektiv b) nicht surjektiv c) nicht bijektiv
4. Sei D die Menge aller Staaten und M die Menge aller Städte. Ist die Abbildung $f : D \to M$, *Staat* $\mapsto$ *Hauptstadt dieses Staates* injektiv und/oder surjektiv?
5. Gegeben ist $f : x \mapsto x^2$. Richtig oder falsch:
   a) $f : \mathbb{R} \to \mathbb{R}$ ist injektiv. b) $f : (0, \infty) \to \mathbb{R}$ ist injektiv.
   c) $f : \mathbb{R} \to \mathbb{R}$ ist surjektiv. d) $f : \mathbb{R} \to (0, \infty)$ ist surjektiv.
   e) $f : (0, \infty) \to (0, \infty)$ ist bijektiv.
6. Finden Sie einen geeigneten Definitions- und Wertebereich aus $\mathbb{R}$, sodass f bijektiv ist: a) $f(x) = x + 1$ b) $f(x) = \frac{1}{x}$ c) $f(x) = \frac{1}{x^2}$
7. Gilt $g = f^{-1}$ (Definitions- und Wertebereich seien jeweils so, dass die Funktion bijektiv ist)? Wenn nicht, wie lautet die richtige Vorschrift zur Umkehrung?
   a) $f(x) = x + 1$ und $g(x) = x - 1$ b) $f(x) = \frac{1}{x}$ und $g(x) = x^2$
   c) $f(x) = 2x$ und $g(x) = \frac{1}{2x}$ d) $f(x) = x^2 + 1$ und $g(x) = \sqrt{x - 1}$
8. Richtig oder falsch: Eine Funktion, die streng monoton wächst, ist immer nach oben unbeschränkt.
9. Was trifft zu: „unbeschränkte Funktion“ bedeutet:
   a) nach oben und unten nicht beschränkt
   b) nach oben oder unten nicht beschränkt (d.h., zumindest in eine Richtung nicht beschränkt)

Lösungen zu den Kontrollfragen

Lösungen zu Abschnitt 5.1

1. a) falsch; richtig ist: $R \subseteq A \times B$
   b) Die Schreibweise mit geschwungenen Klammern (= Mengenklammern) ist falsch; richtig ist $(a, b) \in R$.
2. $R = \{(1, 2), (1, 3), (2, 3)\}$
3. Das bedeutet, dass *jeder* Musiker *jedes* Instrument beherrscht.
4. Max hat 2 Kinder. Max ist der Sohn von Moritz.
5. a) richtig b) richtig
6. $R \cup S = \{(1, 1), (2, 2), (1, 2)\}$, $R \cap S = \{(1, 1), (2, 2)\}$, Komplement $A \times A \backslash R = \{(1, 2), (2, 1)\}$ und $R \subseteq S$.
7. a) Relation „gleich“ (=) b) leere Relation ($\{\}$) c) Relation „kleiner“ ($<$)
8. $S \circ R = \{\}$ und $R \circ S = \{(c, b)\}$
9. a) Es gibt (mindestens) ein $x \in A$ mit $(x, x) \notin R$.
   b) Es gibt ein Paar $(x, y) \in R$ mit $(y, x) \notin R$; d.h. x steht in Beziehung zu y, jedoch y steht nicht in Beziehung zu x.
   c) Es gibt in R gleichzeitig (x, y) und (y, x) mit x, y verschieden oder gleich (also insbesondere zerstören auch Schlingen (x, x) die Asymmetrie).
   d) Es gibt in R gleichzeitig (x, y) und (y, x) mit x, y verschieden (Schlingen sind kompatibel mit Antisymmetrie).
   d) Es gibt (x, y) und (y, z) in R, aber nicht $(x, z) \in R$.
10. a) Es muss eines der beiden Paare (a, b) oder (b, a) entfernt werden.
    b) Es muss eines der beiden Paare (a, b) oder (b, a) entfernt werden, und auch alle Schlingen.

11. • nicht reflexiv, denn $(b, b) \notin S$
    • nicht symmetrisch, denn $S \neq S^{-1}$ ((c, a) fehlt zur Symmetrie)
    • antisymmetrisch, denn: $(a, c) \in S$ aber $(c, a) \notin S$
    • nicht asymmetrisch, denn die Schlingen zerstören die Asymmetrie
    • transitiv, denn $S \circ S = \{(a, c)\} \subseteq S$
12. Richtig; denn $R^{-1} \cap R = \{\} \Rightarrow R^{-1} \cap R \subseteq \mathbb{I}_A$ und die Umkehrung des Pfeils gilt nicht.
13. $K_0 = \{2k \mid k \in \mathbb{Z}\}$ (= alle Zahlen, mit Rest 0); $K_1 = \{2k + 1 \mid k \in \mathbb{Z}\}$ (= alle Zahlen mit Rest 1). Jede ganze Zahl liegt entweder in K_0 oder in K_1 (die Äquivalenzklassen sind ja disjunkt und ihre Vereinigung ist $\mathbb{Z}$).
14. Es gibt vier Äquivalenzklassen:
    $[0000] = \{0000, 0001, 0010, 0011\}$ $[0100] = \{0100, 0101, 0110, 0111\}$
    $[1000] = \{1000, 1001, 1010, 1011\}$ $[1100] = \{1100, 1101, 1110, 1111\}$
15. Eine Ordnung auf der Menge A enthält alle Paare (a, a) mit $a \in A$, während die zugehörige strikte Ordnung diese Paare nicht enthält.
16. partielle Ordnung, denn z. B. 1 und 3 sind nicht vergleichbar
17. richtig

Lösungen zu Abschnitt 5.2

1. a) Abbildung; $f(D) = \{a, b, d\}$; nicht surjektiv, weil $f(D) \neq M$; nicht injektiv, weil d das Bild von mehr als einem Element von D ist.
   b) Abbildung; injektiv, denn jedes Element aus $f(D) = \{a, b, d\}$ ist Bild von *genau einem* Element aus D; nicht surjektiv, weil $f(D) \neq M$.
   c) Abbildung; surjektiv, weil jedes Element von M Bild eines Elementes aus D ist, d.h., $f(D) = M$; nicht injektiv, weil c Bild von zwei Elementen von D ist.
   d) *Keine* Abbildung, weil $3 \in D$ kein eindeutiges Bild besitzt.
   e) Abbildung; bijektiv, weil *jedes* Element aus M Bild *genau eines* Elementes aus D ist.
2. Jede Funktion definiert eine Relation (= Graph der Funktion). Umgekehrt ist aber nur eine *rechtseindeutige* Relation der Graph einer Funktion.
3. a) Es gibt (mindestens) ein y, das Funktionswert von zwei verschiedenen x-Werten aus dem Definitionsbereich ist.
   b) Es gibt (mindestens) ein y, das kein Funktionswert eines x aus dem Definitionsbereich ist.
   c) nicht injektiv oder nicht surjektiv
4. Die Abbildung ist injektiv, weil es zu jeder Hauptstadt genau einen Staat gibt. Die Abbildung ist aber nicht surjektiv, weil es Städte gibt, die keine Hauptstadt sind.
5. a) Falsch, denn zum Beispiel $x_1 = -\frac{1}{2}$ und $x_2 = \frac{1}{2}$ haben denselben Funktionswert $f(x_1) = f(x_2) = \frac{1}{4}$.
   b) Richtig; auf $D = (0, \infty)$ ist die Funktion injektiv, weil für alle $x_1, x_2 \in (0, \infty)$ gilt: Wenn $x_1 \neq x_2$, dann ist auch $x_1^2 \neq x_2^2$ (in Worten: Verschiedene Werte aus dem Definitionsbereich haben auch verschiedene Funktionswerte).
   c) Falsch, denn zum Beispiel $y = -4$ ist zu keinem $x \in \mathbb{R}$ Funktionswert.
   d) Richtig; jedes $y \in (0, \infty)$ ist Funktionswert von einem $x \in \mathbb{R}$, nämlich von

$x = \sqrt{y}$.
e) Richtig, denn die Funktion ist injektiv und surjektiv.

6. Es ist ein Definitionsbereich zu suchen, auf dem f streng monoton fallend oder streng monoton wachsend ist. Als Wertebereich ist die Menge aller Funktionswerte zu wählen: a) $D = \mathbb{R}$, $M = \mathbb{R}$ b) $D = \mathbb{R}\backslash\{0\}$, $M = \mathbb{R}\backslash\{0\}$
c) $D = (0, \infty)$, $M = (0, \infty)$
7. Die Umkehrfunktion von f macht die Wirkung von f wieder rückgängig, wenn man f^{-1} mit f verkettet: $(f^{-1} \circ f)(x) = x$. Wenn f also ein x zu $y = f(x)$ „verschlüsselt“, so entschlüsselt f^{-1} wieder: $f^{-1}(y) = x$:
a) $(f \circ g)(x) = f(g(x)) = g(x) + 1 = x - 1 + 1 = x$. Daher ist g die Umkehrfunktion zu f.
b) $(f \circ g)(x) = f(g(x)) = \frac{1}{g(x)} = \frac{1}{x^2}$. Daher ist g nicht die Umkehrfunktion zu f. Die Umkehrfunktion wäre $g(x) = \frac{1}{x}$.
c) $(f \circ g)(x) = f(g(x)) = 2g(x) = 2\frac{1}{2x} = \frac{1}{x}$. Daher ist g nicht die Umkehrfunktion zu f. Die Umkehrfunktion wäre $g(x) = \frac{x}{2}$.
d) $(f \circ g)(x) = f(g(x)) = g(x)^2 + 1 = (\sqrt{x-1})^2 + 1 = x$, also ist g die Umkehrfunktion.
8. Falsch; die Funktion $f(x) = 1 - \frac{1}{x}$ mit $D = (0, \infty)$ ist z. B. streng monoton wachsend, denn $x_1 < x_2 \Rightarrow 1 - \frac{1}{x_1} < 1 - \frac{1}{x_2}$; aber sie ist auch gleichzeitig nach oben beschränkt: $f(x) \leq 1$ für alle x. Eine Skizze zeigt, dass der Graph sich mehr und mehr an die Gerade $g(x) = 1$ anschmiegt.
9. a) falsch b) richtig

5.4 Übungen

Aufwärmübungen

1. Geben Sie die inverse Relation zu $R = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$ an.
2. Gegeben sind die Mengen $A = \{a, b, c\}$, $B = \{x, y, z\}$, $C = \{u, v\}$ und die Relationen $R = \{(a, x), (b, x), (c, y), (c, z)\}$ und $S = \{(x, u), (z, v)\}$. Geben Sie an: a) R^{-1} b) $S \circ R$ c) $\mathbb{I}_A \circ R$ ($\mathbb{I}_A$ ... identische Relation) d) $R \circ \mathbb{I}_A$
3. Gegeben sind die Menge $A = \{a, b, c\}$ und die Relation $R = \{(a, a), (a, b), (b, a), (b, b), (c, c)\}$. Ist R reflexiv, symmetrisch, asymmetrisch, antisymmetrisch oder transitiv?
4. Gegeben sind die Menge $A = \{a, b, c\}$ und die Relation $S = \{(a, a), (a, c), (c, c)\}$. Geben Sie a) die reflexive und b) die symmetrische Hülle von S an.
5. Gegeben ist die Relation $R = \{(a, b), (b, a), (b, c)\}$ in $A = \{a, b, c\}$. Geben Sie ihre transitive Hülle an.
6. Geben Sie alle Elemente der Relation „x liegt im Alphabet vor y“ in der Menge $A = \{a, b, c, d\}$ an. Ist diese Relation eine Ordnung/strikte Ordnung? Wenn ja: Ist sie total oder partiell?
7. Ist die Relation a teilt b auf der Menge $A = \{2, 3, 4, 5\}$ eine Ordnung/strikte Ordnung? Wenn ja: Ist sie total oder partiell?

8. Geben Sie für folgende Funktionen den (bzw. einen) größtmöglichen Definitionsbereich D an (x reelle Zahl):
   a) $f(x) = |x|$ b) $f(x) = \frac{1}{x^2-1}$ c) $f(x) = \sqrt{x+3}$
9. Seien $f, g : \mathbb{R} \to \mathbb{R}$ Funktionen mit $f(x) = 1 - x^2$ und $g(x) = x^2$. Geben Sie an:
   a) $(f+g)(x)$ b) $(f \cdot g)(x)$ c) $(\frac{f}{g})(x)$ d) $(f \circ g)(x)$ e) $(g \circ f)(x)$
10. a) Schreiben Sie $h : \mathbb{R} \to \mathbb{R}$ mit $h(x) = (3x+1)^2$ als Hintereinanderausführung von zwei Funktionen f und g.
    b) Schreiben Sie $h : \mathbb{R}\backslash\{-3\} \to \mathbb{R}$ mit $h(x) = \frac{1}{3+x}$ als Hintereinanderausführung von zwei Funktionen f und g.
11. Geben Sie für folgende Funktionen $f : D \to M$ die Bildmenge $f(D)$ an. Ist die Funktion surjektiv?
    a) $f : \mathbb{N} \to \mathbb{N}$, $f(x) = 2x$ b) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x$
    c) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ d) $f : \mathbb{R}\backslash\{0\} \to \mathbb{R}$, $f(x) = \frac{1}{x^2}$
    e) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x + 3$ f) $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x + y$
    g) $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x^2 + y^2$
12. Ist die Funktion injektiv?
    a) $f : \mathbb{N} \to \mathbb{N}$, $f(x) = 2x$ b) $f : [0, \infty) \to \mathbb{R}$, $f(x) = x^2$
    c) $f : \mathbb{R}\backslash\{0\} \to \mathbb{R}$, $f(x) = \frac{1}{x^2}$ d) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x + 3$
    e) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = |x|$ f) $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x + y$
13. Ist die Funktion bijektiv? Geben Sie in diesem Fall die Umkehrfunktion an.
    a) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x$ b) $f : [0, \infty) \to \mathbb{R}$, $f(x) = x^2$
    c) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x + 3$ d) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = |x|$
    e) $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x + y$ f) $f : \mathbb{Z}_5 \to \mathbb{Z}_5$, $f(x) = 3x$
    g) $f : \mathbb{Z}_8 \to \mathbb{Z}_8$, $f(x) = 2x$
14. Geben Sie die Umkehrfunktion an und machen Sie die Probe:
    a) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = -2x + 1$ b) $f : [0, \infty) \to [0, \infty)$, $f(x) = x^2$
    c) $f : (-\infty, 0] \to [0, \infty)$, $f(x) = x^2$
15. Geben Sie an, wo die Funktion streng monoton wachsend bzw. streng monoton fallend ist. a) $f(x) = \frac{1}{x}$ b) $f(x) = |x|$ c) $f(x) = \frac{1}{x^2+1}$
16. Untersuchen Sie, ob die Funktion beschränkt ist.
    a) $f(x) = 2x$ b) $f(x) = |x|$ c) $f(x) = x^3$
    d) $f(x) = \frac{1}{x^2}$ e) $f(x) = \frac{1}{x}$ für $x > 0$
    f) $f(x) = \frac{x}{x^2+1}$ für $x \geq 0$ g) $f(x) = \frac{1}{x^2+1}$ für $x \geq 0$
17. Suchen Sie einen geeigneten (möglichst großen) Definitionsbereich, auf dem die Funktion umkehrbar ist, und geben Sie die zugehörige Umkehrfunktion an.
    a) $f(x) = 2x$ b) $f(x) = \frac{1}{x^2}$ c) $f(x) = x^3$
18. Die Umrechung von Grad Celsius in Grad Fahrenheit erfolgt mit der Formel $F = 1.8C + 32$. Finden Sie die Formel für die Umrechung von Fahrenheit in Celsius.

Weiterführende Aufgaben

1. Geben Sie die Relationen $<$, $>$, $\geq$, $\leq$, $=$, $\neq$ in $A = \{0, 1, 2, 3\}$ an und untersuchen Sie jeweils, ob die Relation reflexiv, symmetrisch, antisymmetrisch, asymmetrisch oder transitiv ist.

2. a) Geben Sie ein Beispiel für eine Relation, die weder symmetrisch noch asymmetrisch noch antisymmetrisch ist.
   b) Gibt es eine Relation, die symmetrisch und antisymmetrisch ist?
   c) Gibt es eine Relation, die symmetrisch und asymmetrisch ist?
   d) Gibt es eine Relation, die antisymmetrisch und asymmetrisch ist?
3. Angenommen, Huber (H) spricht die Sprachen Englisch und Deutsch, Meier (M) spricht nur Deutsch, und Smith (S) nur Englisch. Geben Sie die Relation „a und b sprechen eine gemeinsame Sprache“ auf der Menge $\{H, M, S\}$ an. Handelt es sich um eine Äquivalenzrelation?
4. Können die Werte (x, y), die $x^2 + y^2 = 4$ erfüllen, auch durch eine Funktion $y = f(x)$ beschrieben werden? Wo liegen die Punkte (x, y), die diese Relation erfüllen?
5. Gegeben ist $f(x) = \frac{x^2}{x^2+1}$.
   a) Wo ist f streng monoton wachsend bzw. streng monoton fallend?
   b) Ist f (nach unten/oben) beschränkt?
6. Geben Sie für folgende Funktionen $f : D \to M$ die Bildmenge $f(D)$ an. Ist die Funktion surjektiv?
   a) $f : \mathbb{N} \to \mathbb{N}$, $f(x) = x^2$ b) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 1$
   c) $f : [0, \infty) \to \mathbb{R}$, $f(x) = \sqrt{x}$ d) $f : \mathbb{R}\backslash\{0\} \to \mathbb{R}$, $f(x) = \frac{1}{x}$
7. Ist die Funktion injektiv?
   a) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ b) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 1$
   c) $f : [0, \infty) \to \mathbb{R}$, $f(x) = \sqrt{x}$ d) $f : \mathbb{R}\backslash\{0\} \to \mathbb{R}$, $f(x) = \frac{1}{x}$
8. Schränken Sie den Definitions- und Wertebereich von $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 1$ geeignet ein, damit die Funktion bijektiv wird. Geben Sie die Umkehrfunktion an.
9. Gegeben sind $f, g : \mathbb{R} \to \mathbb{R}$ mit $f(x) = a \cdot x$ und $g(x) = x + b$ (wobei $a, b \in \mathbb{R}$ sind, $a \neq 0$). Geben Sie an:
   a) $g \circ f$ b) $f \circ g$ c) f^{-1} und g^{-1} d) $(f \circ g)^{-1}$
10. Zeigen Sie: Wenn f und g injektiv sind, dann ist auch $f \circ g$ injektiv.

Lösungen zu den Aufwärmübungen

1. $R^{-1} = \{(y, x) \in \mathbb{R}^2 \mid y = x^2\}$ bzw. nach Umbenennung der Variablen: $R^{-1} = \{(x, y) \in \mathbb{R}^2 \mid x = y^2\}$, d.h., $R^{-1} = \{(x, y) \in \mathbb{R}^2 \mid y = \sqrt{x} \text{ oder } y = -\sqrt{x}\}$.
2. a) $R^{-1} = \{(x, a), (x, b), (y, c), (z, c)\}$ b) $S \circ R = \{(a, u), (b, u), (c, v)\}$
   c) $\mathbb{I}_A \circ R = \{\}$ d) $R \circ \mathbb{I}_A = R$
3. - $\mathbb{I}_A \subseteq R$, daher reflexiv.
   - $R = R^{-1}$, daher symmetrisch.
   - $R \cap R^{-1} \not\subseteq \mathbb{I}_A$, daher nicht antisymmetrisch.
   - $R \cap R^{-1} \not\subseteq \{\}$, daher nicht asymmetrisch.
   - $R \circ R = \{(a, a), (a, b), (b, a), (b, b), (c, c)\} \subseteq R$, daher transitiv.
4. a) $[S]^{refl} = S \cup \mathbb{I}_A = \{(a, a), (b, b), (a, c), (c, c)\}$.
   b) $[S]^{sym} = S \cup S^{-1} = \{(a, a), (a, c), (c, a), (c, c)\}$.
5. Wir bilden $R \circ R = \{(a, a), (b, b), (a, c)\}$ und weiter $R \circ (R \circ R) = \{(a, b), (b, a), (b, c)\}$. Da nun keine neuen Paare entstanden sind, bringt auch eine weitere Verknüpfung mit R nichts mehr, und damit können wir abbrechen. Es ist also $[R]^{trans} = R \cup R \circ R = \{(a, b), (b, a), (b, c), (a, a), (b, b), (a, c)\}$.

6. $R = \{(a,b),(a,c),(a,d),(b,c),(b,d),(c,d)\}$ ist antisymmetrisch und transitiv, aber nicht reflexiv, daher keine Ordnung. Sie ist aber asymmetrisch (und transitiv), daher eine strikte Ordnung. Die strikte Ordnung ist total, weil je zwei Elemente von A bezüglich R vergleichbar sind (entweder ist das eine oder das andere vorher im Alphabet).
7. $R = \{(2,2),(3,3),(4,4),(5,5),(2,4)\}$ reflexiv, antisymmetrisch und transitiv, daher eine Ordnung. Sie ist nur partiell, da zum Beispiel die Elemente 3 und 5 nicht in einer Teilbarkeitsbeziehung zueinander stehen.
8. Es sind alle Werte auszuschließen, für die die Funktionsvorschrift nicht definiert ist (Division durch 0, Wurzel aus einer negativen Zahl, ...):
   a) $D = \mathbb{R}$ b) $D = \mathbb{R}\backslash\{\pm 1\}$ c) $D = \{x \in \mathbb{R} \,|\, x \geq -3\}$
9. a) $(f+g)(x) = f(x) + g(x) = 1 - x^2 + x^2 = 1$.
   b) $(f \cdot g)(x) = f(x) \cdot g(x) = (1-x^2)x^2$.
   c) $(\frac{f}{g})(x) = \frac{1-x^2}{x^2} = \frac{1}{x^2} - 1$, $x \neq 0$.
   d) $(f \circ g)(x) = f(g(x)) = 1 - (g(x))^2 = 1 - (x^2)^2 = 1 - x^4$.
   e) $(g \circ f)(x) = g(f(x)) = (f(x))^2 = (1-(x^2))^2 = 1 - 2x^2 + x^4$.
10. a) $h(x) = (3x+1)^2 = (g(x))^2 = f(g(x))$ mit $g(x) = 3x+1$ und $f(x) = x^2$
    b) $h(x) = \frac{1}{3+x} = \frac{1}{g(x)} = f(g(x))$ mit $g(x) = 3 + x$ und $f(x) = \frac{1}{x}$
11. a) Die Menge aller Funktionswerte ist $f(D) = \{2x \mid x \in \mathbb{N}\} = \{2,4,6,\ldots\} \neq \mathbb{N}$. D.h., es ist zum Beispiel $y = 3$ kein Funktionswert. Daher nicht surjektiv.
    b) $f(D) = \{2x \mid x \in \mathbb{R}\} = \mathbb{R}$, also surjektiv (d.h., jedes $y \in \mathbb{R}$ ist Funktionswert von einem x, nämlich (hier von genau einem:) $x = \frac{y}{2}$).
    c) $f(D) = \{x^2 \mid x \in \mathbb{R}\} = \{x \in \mathbb{R} \mid x \geq 0\} \neq \mathbb{R}$, daher nicht surjektiv
    d) $f(D) = \{\frac{1}{x^2} \mid x \in \mathbb{R}\} = \{x \in \mathbb{R} \mid x > 0\} \neq \mathbb{R}$, daher nicht surjektiv
    e) $f(D) = \mathbb{R}$, daher surjektiv
    f) $f(D) = \mathbb{R}$, daher surjektiv
    g) $f(D) = \{x^2 + y^2 \mid x, y \in \mathbb{R}\} = \{x \in \mathbb{R} \mid x \geq 0\}$, daher nicht surjektiv
12. a) injektiv, da $x_1 \neq x_2 \Rightarrow 2x_1 \neq 2x_2$ (verschiedene x-Werte haben auch immer verschiedene Funktionswerte)
    b) injektiv, da $x_1 \neq x_2 \Rightarrow x_1^2 \neq x_2^2$ für $x_1, x_2 \in [0,\infty)$
    c) nicht injektiv, denn z. B. $x_1 = 3$ und $x_2 = -3$ sind verschiedene Werte aus dem Definitionsbereich, haben aber denselben Funktionswert $f(3) = f(-3) = \frac{1}{9}$
    d) injektiv, da $x_1 \neq x_2 \Rightarrow x_1 + 3 \neq x_2 + 3$
    e) nein, denn z. B. $f(-1) = f(1) = 1$
    f) nein, denn z. B. $f(0,1) = f(1,0) = 1$
13. a) ja, da sie injektiv und surjektiv ist; $f^{-1}(x) = \frac{x}{2}$
    b) nein, nicht surjektiv ($f([0,\infty)) = [0,\infty)$)
    c) ja, $f^{-1}(x) = x - 3$
    d) nein, weder injektiv ($f(-1) = f(1) = 1$) noch surjektiv ($f(\mathbb{R}) = [0,\infty)$)
    e) nein, nicht injektiv ($f(0,0) = f(-1,1) = 0$)
    f) ja; $f^{-1}(x) = 2x$
    g) nein; weder injektiv ($f(0) = f(4) = 0$) noch surjektiv ($f(\mathbb{Z}_8) = \{0,2,4,6\}$)
14. a) $g : \mathbb{R} \to \mathbb{R}$, g: $g(x) = -\frac{1}{2}(x-1)$. Probe: $(f \circ g)(x) = f(g(x)) = -2g(x) + 1 = \frac{-2}{-2}(x-1) + 1 = x$.
    b) $g : [0,\infty) \to [0,\infty)$ mit: $g(x) = \sqrt{x}$. Probe: $(f \circ g)(x) = f(g(x)) = g(x)^2 = (\sqrt{x})^2 = x$.

c) $g : [0, \infty) \to (-\infty, 0]$ mit: $g(x) = -\sqrt{x}$. Probe: $(f \circ g)(x) = f(g(x)) = g(x)^2 = (-\sqrt{x})^2 = x$.

15. a) f ist streng monoton fallend auf $\mathbb{R}\backslash\{0\}$, denn wenn $x_1 < x_2$, dann ist $\frac{1}{x_1} > \frac{1}{x_2}$ (d.h., wenn x größer wird, so wird $f(x)$ kleiner).
b) Die Betragsfunktion ist streng monoton wachsend auf dem Definitionsbereich $D = [0, \infty)$, denn für $x_1, x_2 \in [0, \infty)$ mit $x_1 < x_2$ gilt: $f(x_1) = x_1 < f(x_2) = x_2$. Sie ist streng monoton fallend für $D = (-\infty, 0]$, denn für $x_1, x_2 \in (-\infty, 0]$ mit $x_1 < x_2$ gilt: $f(x_1) = -x_1 > f(x_2) = -x_2$.
c) Für $x_1, x_2 \in (-\infty, 0]$ mit $x_1 < x_2$ gilt: $x_1^2 > x_2^2$, daher $x_1^2 + 1 > x_2^2 + 1$, daraus folgt $\frac{1}{x_1^2+1} < \frac{1}{x_2^2+1}$, daher ist die Funktion hier streng monoton wachsend. Analog gilt für $x_1, x_2 \in [0, \infty)$ mit $x_1 < x_2$, dass: $x_1^2 < x_2^2$, daher $\frac{1}{x_1^2+1} > \frac{1}{x_2^2+1}$. Also ist die Funktion hier streng monoton fallend.

16. a) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x$ ist (nach oben und unten) unbeschränkt, da die Funktionswerte größer als jede noch so große Zahl $K > 0$ werden bzw. kleiner als jede noch so kleine Zahl $k < 0$.
b) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = |x|$ ist nach unten beschränkt, da $|x| \geq 0$ für alle $x \in \mathbb{R}$, und nach oben unbeschränkt.
c) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$ ist (nach unten und oben) unbeschränkt.
d) $f : \mathbb{R}\backslash\{0\} \to \mathbb{R}$, $f(x) = \frac{1}{x^2}$ ist nach unten beschränkt (z. B. ist $k = 0$ eine untere Schranke), und nach oben unbeschränkt.
e) Die Funktion ist nach unten beschränkt, da $\frac{1}{x} \geq 0$ für $x > 0$, und nach oben unbeschränkt.
f) Nach unten beschränkt, da $\frac{x}{x^2+1} \geq 0$ für $x \geq 0$. Eine Skizze legt nahe, dass die Funktion auch nach oben beschränkt ist. Versuchen wir daher $K = 1$ als obere Schranke, das sollte laut Skizze funktionieren: $\frac{x}{x^2+1} \leq 1$ ist gleichbedeutend mit $x \leq x^2 + 1$, und das ist für $x \in [0, \infty)$ der Fall. Also ist die Funktion auch nach oben beschränkt.
g) Nach unten beschränkt, da $\frac{1}{1+x^2} \geq 0$ für $x \geq 0$; Eine Skizze legt nahe, dass sie auch nach oben beschränkt, ist. Versuchen wir $\frac{1}{x^2+1} \leq 1$: Das ist gleichbedeutend mit $1 \leq x^2 + 1$, also $0 \leq x^2$ und das ist für alle $x \in \mathbb{R}$ der Fall.

17. Die Funktion ist umkehrbar auf jedem Teil ihres Definitionsbereiches, wo sie streng monoton wachsend (bzw. fallend) ist.
a) Streng monoton wachsend auf $\mathbb{R}$, da $x_1 < x_2 \Rightarrow 2x_1 < 2x_2$; daher umkehrbar auf ganz $\mathbb{R}$; Wertebereich: $f(D) = \{2x \mid x \in \mathbb{R}\} = \mathbb{R}$; Umkehrfunktion ist $g : \mathbb{R} \to \mathbb{R}$ mit $g(x) = \frac{x}{2}$. Probe: $(f \circ g)(x) = f(g(x)) = 2g(x) = x$.
b) Streng monoton wachsend auf $D = (-\infty, 0)$, da für $x_1, x_2 \in (-\infty, 0)$ gilt: $x_1 < x_2 \Rightarrow \frac{1}{x_1^2} < \frac{1}{x_2^2}$; Wertebereich ist $f(D) = \{\frac{1}{x^2} \mid x \in (-\infty, 0)\} = (0, \infty)$. Umkehrfunktion: $g : (0, \infty) \to (-\infty, 0)$ mit $g(x) = \frac{-1}{\sqrt{x}}$. Probe: $(f \circ g)(x) = f(g(x)) = f(\frac{-1}{\sqrt{x}}) = x$. Streng monoton fallend auf $D = (0, \infty)$, da für $x_1, x_2 \in (0, \infty)$ gilt: $x_1 < x_2 \Rightarrow \frac{1}{x_1^2} > \frac{1}{x_2^2}$; Wertebereich ist $f(D) = \{\frac{1}{x^2} \mid x \in (0, \infty)\} = (0, \infty)$; Umkehrfunktion: $g : (0, \infty) \to (0, \infty)$ mit $g(x) = \frac{1}{\sqrt{x}}$.
c) Streng monoton wachsend auf ganz $\mathbb{R}$, da für $x_1, x_2 \in \mathbb{R}$ gilt: $x_1 < x_2 \Rightarrow x_1^3 < x_2^3$; daher umkehrbar auf ganz $\mathbb{R}$; Umkehrfunktion $g : \mathbb{R} \to \mathbb{R}$, $g(x) = \sqrt[3]{x}$.

18. Die Umrechnung erfolgt mit der Umkehrfunktion: $C(F) = (F - 32)/1.8$.

(Lösungen zu den weiterführenden Aufgaben finden Sie in Abschnitt B.5)

B

Lösungen zu den weiterführenden Aufgaben

B.1 Logik und Mengen

1. a) Für alle $x \in A$ gilt: $x \geq 5$. b) Es gibt einen Pinguin, der nicht gerne schwimmt. c) Das Auto ist nicht blau oder wurde im Jahr 2005 oder später zugelassen. d) $(x \notin A)$ und $(x \notin B)$
2. a) richtig b) falsch (die Augen können dann offen oder geschlossen sein) c) falsch (ich kann dann wach sein oder schlafen)
3. Es gibt hier jemanden, der nicht Deutsch und nicht Englisch spricht.
4. Die Wahrheitstabelle ergibt, dass nur B als Mörder in Frage kommt. Logisch gleichwertig ist die Formel $(V \wedge S) \vee (N \wedge F)$ (Das sieht man durch Vergleich der Wahrheitstabellen für alle 16 Kombinationen der Eingangsvariablen S, F, V, N).
5. a) $A \cup U$ b) $K \backslash (A \cup U) = \overline{A} \cap \overline{U}$ c) $K \backslash (A \cup U \cup G) = \overline{A} \cap \overline{U} \cap \overline{G}$ d) $A \cap \overline{U}$
6. a) $A \cap B$ b) B
7. a) b b) 1 c) $\overline{b}$
8. Verneinung beider Seiten der DNF und Anwendung der de Morgan'schen Regeln liefert die KNF für die Verneinung von f und damit auch für f (da f für eine beliebige Funktion steht). Man erhält die KNF auch, wenn man das Dualitätsprinzip auf die DNF anwendet und dabei alle Nullen (auch im Funktionsargument!) durch Einsen ersetzt und umgekehrt.
9. $c_1 = a + \overline{b}$, $c_2 = \overline{a} \cdot \overline{b}$, $c_3 = 1$, $c_4 = a$, $c_5 = \overline{b}$, $c_6 = \overline{a} + b$ und $c_7 = a + \overline{b}$
10. $\text{if}(t, a, b) = t \cdot a + \overline{t} \cdot b$
11. Die Regeln können leicht durch eine Wahrheitstabelle mit den drei Zeilen $a < b$, $a = b$ und $a > b$ und den Spalten $a \vee b$, $\overline{a \vee b}$ usw. nachgewiesen werden.

B.2 Zahlenmengen und Zahlensysteme

1. a) ja b) ja
2. Tipp: Gehen Sie analog wie für $\sqrt{2}$ vor.
3. –
4. –
5. –
6. –

7. Hinweis: $n(n+1)$ ist immer eine gerade Zahl, es lässt sich also 2 herausheben.
8. a) $(51.25)_{10}$ b) $(101100111.\overline{0011})_2$ c) $(21422)_8$ d) $(43981)_{10}$
9. exakt: $x = 2d = 205117922$, $y = 2c = 83739041$
   abgerundet: $x = d = 102558961$ und $y = c = 41869520.5$
   aufgerundet: $ad - bc = 0$, also keine Lösung

B.3 Elementare Begriffe der Zahlentheorie

1. –
2. –
3. $x = 1, y = 2$.
4. Ja.
5. Nein, denn das Assoziativgesetz gilt nicht.
6. $x = 12$ und $y = 8$.
7. 3
8. Bei der Wahl $m_1 = 97$, $m_2 = 98$ und $m_3 = 99$ folgen für $203 + 125$ bzw. $203 \cdot 125$ die Darstellungen $(37, 34, 31)$ bzw. $(58, 91, 31)$.
9. –
10. –
11. Durch Probieren: $x = 3$ und $x = 7$.
12. $52, 9, 17, 52$

B.4 Relationen und Funktionen

1.

	reflexiv	symm.	antisymm.	asymmetrisch	transitiv
$<$	nein	nein	ja	ja	ja
$>$	nein	nein	ja	ja	ja
$\leq$	ja	nein	ja	nein	ja
$\geq$	ja	nein	ja	nein	ja
$=$	ja	ja	ja	nein	ja
$\neq$	nein	ja	nein	nein	nein

2. –
3. nein
4. nein; $y = \sqrt{4 - x^2}$ und $y = -\sqrt{4 - x^2}$
5. streng monoton fallend für $(-\infty, 0]$ und streng monoton wachsend für $[0, \infty)$; beschränkt
6. a) nicht surjektiv b) surjektiv c) nicht surjektiv d) nicht surjektiv
7. a) nein b) ja c) ja d) ja
8. $[0, \infty)$ oder $(-\infty, 0]$
9. –
10. –

Literatur

Mathematische Vorkenntnisse

1. A. Adams et al., *Mathematik zum Studieneinstieg*, 5. Auflage, Springer, Berlin, 2008.
2. K. Fritzsche, *Mathematik für Einsteiger*, 4. Auflage, Spektrum, Heidelberg, 2007.
3. A. Kemnitz, *Mathematik zum Studienbeginn*, 10. Auflage, Vieweg, Braunschweig, 2011.
4. M. Knorrenschild, *Vorkurs Mathematik*, 3. Auflage, Carl Hanser, München, 2009.
5. W. Purkert, *Brückenkurs Mathematik für Wirtschaftswissenschaftler*, 7. Auflage, Teubner, Stuttgart, 2011.
6. P. Stingl, *Einstieg in die Mathematik für Fachhochschulen*, 4. Auflage, Carl Hanser, München, 2009.
7. W. Timischl und G. Kaiser, *Ingenieur-Mathematik I-IV*, E. Dorner, Wien, 1997–2012.

Mathematik für Informatiker

8. M. Brill, *Mathematik für Informatiker*, 2. Auflage, Carl Hanser, München, 2005.
9. W. Dörfler und W. Peschek, *Einführung in die Mathematik für Informatiker*, Carl Hanser, München, 1988.
10. D. Hachenberger, *Mathematik für Informatiker*, 2. Auflage, München, Pearson, 2008.
11. P. Hartmann, *Mathematik für Informatiker*, 5. Auflage, Vieweg, Braunschweig, 2012.
12. B. Kreußler und G. Pfister, *Mathematik für Informatiker*, Springer, Berlin, 2009.
13. M. Oberguggenberger und A. Ostermann, *Analysis für Informatiker*, 2. Auflage, Springer, Berlin, 2009.
14. W. Struckmann und D. Wätjen, *Mathematik für Informatiker*, Elsevier, München, 2007.

Mathematik für Technik oder Wirtschaft

15. T. Ellinger et al., *Operations Research*, 6. Auflage, Springer, Berlin, 2003.
16. E. Kreyszig, *Advanced Engineering Mathematics*, 10th edition, John Wiley, New York, 2011.
17. P. Stingl, *Mathematik für Fachhochschulen: Technik und Informatik*, 8. Auflage, Carl Hanser, München, 2009.
18. P. Stingl, *Operations Research*, Fachbuchverlag Leipzig, München, 2003.

19. K. Sydsæter und P. Hammond, *Mathematik für Wirtschaftswissenschaftler*, 3. Auflage, Pearson, München, 2008.
20. J. Tietze, *Einführung in die angewandte Wirtschaftsmathematik*, 16. Auflage, Vieweg, Braunschweig, 2011.

Diskrete Mathematik und Lineare Algebra – einführend

21. A. Beutelspacher und M.-A. Zschiegner, *Diskrete Mathematik für Einsteiger*, 4. Auflage, Vieweg, Braunschweig, 2011.
22. R. Garnier und J. Taylor, *Discrete Mathematics for New Technology*, 2nd edition, IOP Publishing, Bristol, 2001.
23. K.H. Rosen, *Discrete Mathematics and its Applications*, 7th edition, McGraw-Hill, Boston, 2012.
24. G. Strang, *Lineare Algebra*, Springer, Berlin, 2003.
25. P. Tittmann, *Graphentheorie*, 2. Auflage, Fachbuchverlag Leipzig, München, 2011.

Diskrete Mathematik und Lineare Algebra – weiterführend

26. M. Aigner, *Diskrete Mathematik*, 6. Auflage Vieweg, Braunschweig, 2006.
27. R. Diestel, *Graph Theory*, 4th edition, Springer, New York, 2012.
28. R.L. Graham, D. Knuth und O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, 11th printing, Addison Wesley, 2002.
29. J.L. Gross und J. Yellen, *Handbook of Graph Theory*, CRC Press, 2003.
30. J.L. Gross und J. Yellen, *Graph Theory and its Applications*, 2nd edition, CRC Press, 2005.
31. T. Ihringer, *Diskrete Mathematik*, Teubner, Stuttgart, 1994.
32. K. Jänich, *Lineare Algebra*, 11. Auflage, Springer, Berlin, 2010.
33. A. Steger, *Diskrete Strukturen 1*, 2. Auflage, Springer, Berlin, 2007.

Kryptographie und Codierungstheorie

34. J. Buchmann, *Einführung in die Kryptographie*, 5. Auflage, Springer, Berlin, 2010.
35. G.A. Jones und J.M. Jones, *Information and Coding Theory*, Springer, London, 2000.
36. S. Roman, *Introduction to Coding and Information Theory*, Springer, New York, 1997.
37. B. Schneier, *Angewandte Kryptographie*, Addison-Wesley, München, 1996.
38. A.S. Tanenbaum, *Computernetzwerke*, 5. Auflage, Pearson, München, 2012.

Populärwissenschaftliches

39. E. Behrends, M. Aigner (Eds.), *Alles Mathematik – von Pythagoras zum CD-Player*, 3. Auflage, Vieweg, 2009.
40. D. Guedj, *Das Theorem des Papageis*, Bastei Lübbe, Bergisch Gladbach, 1999.
41. D. Harel, *Das Affenpuzzle und weitere bad news aus der Computerwelt*, Springer, Berlin, 2002.
42. D. Kehlmann, *Die Vermessung der Welt*, Rowohlt, 2008.
43. S. Singh, *Fermats letzter Satz*, Carl Hanser, München, 1998.
44. S. Singh, *Geheime Botschaften*, Carl Hanser, München, 1999.

Ressourcen im Internet

45. F. Embacher und P. Oberhuemer, mathe online, http://www.mathe-online.at/
46. E.W. Weisstein et al., *MathWorld – A Wolfram Web Resource*, http://mathworld.wolfram.com/

47. Wikipedia Mathematik, http://de.wikipedia.org/wiki/Mathematik
48. *Wolfram|Alpha: Computational Knowledge Engine*, http://www.wolframalpha.com

Verzeichnis der Symbole

Index