12. Juli 2024

Inhaltsverzeichnis

Teil I

Mathematik für Informatiker 1

Kapitel 1

Aussagenlogik

1.1 Aussagen und Aussageformen

Mathematik ist das Analysieren von Aussagen, wie zum Beispiel

- Die Zahl 3 ist eine Primzahl.
- Die Zahl 4 ist eine Primzahl.
- Es gibt unendlich viele Primzahlzwillinge, d.h. Zahlenpaare der Art

$$(3,5), \quad (5,7), \quad (11,13), \quad (17,19) \quad \text{usw.}$$

Die erste Aussage ist richtig, die zweite falsch. Über den Wahrheitsgehalt der dritten Aussage können wir nicht abschließend entscheiden, sind aber überzeugt, dass sie entweder *wahr* oder *falsch* ist.

Mit T. Zoglauer: *Einführung in die formale Logik für Philosophen* (2008) machen wir daher die folgende Definition:

> Eine *Aussage* ist ein gewöhnlicher, umgangssprachlicher Satz, der entweder *wahr* oder *falsch* ist.

Diese Definition beinhaltet die *Zweiwertigkeit* der Aussagenlogik und damit auch aller unserer Untersuchungen: Außer *wahr* und *falsch* gibt es keine weitere Möglichkeit.

Es gibt auch sprachliche Formulierungen, die keine Aussagen sind, da wir ihnen auf sinnvolle Weise keinen Wahrheitswert zuordnen können, wie Glückwünsche, Fragen oder Aufforderungen der folgenden Art:

- Herzlichen Glückwunsch!
- Wollen wir wetten?
- Komm jetzt endlich!

Mathematische Ausdrücke, wie

- $x + 7 = 28$
- $\mathcal{R}(0,3,1)$

bezeichnen wir als *Aussageformen.* Sie werden zu Aussagen, nachdem wir einmal den „Platzhalter“ x durch eine Zahl substituieren und so $x + 7 = 28$ zu einer wahren oder falschen Aussage machen, oder $\mathcal{R}(x,y,z)$ beispielsweise als die Relation $x < y < z$ interpretieren, was die Aussage $\mathcal{R}(x,y,z)$ in unserem Beispiel falsch macht.

Aufgaben

Aufgabe 1.1 Welche der folgenden Sätze sind Aussagen, welche sind keine Aussagen?

(i) Berlin ist die Hauptstadt der Bundesrepublik Deutschland.
(ii) Alle Studierenden sind fleißig.
(iii) Reisen bildet.
(iv) Hat die Vorlesung bereits begonnen?
(v) Mathematik soll also schwer sein!

Aufgabe 1.2 Formulieren Sie wenigstens

(i) fünf eigene Beispiele für Aussagen,
(ii) fünf eigene Beispiele für Sätze, die keine Aussagen sind.

Aufgabe 1.3 Geben Sie jeweils ein Beispiel einer mathematischen Aussageform $\mathcal{R}(x)$ mit einer, $\mathcal{S}(x, y)$ mit zwei und $\mathcal{T}(x, y, z)$ mit drei freien Variablen, so dass

(i) $\mathcal{R}(6)$ wahr und $\mathcal{R}(7)$ falsch sind,
(ii) $\mathcal{S}(1, 7)$ wahr und $\mathcal{S}(3, 5)$ falsch sind,
(iii) $\mathcal{T}(1, 3, 12)$ wahr und $\mathcal{T}(3, 1, -1)$ falsch sind.

Die folgenden Aufgaben enthalten Texte aus T. Zoglauer: *Einführung in die formale Logik für Philosophen,* Seite 16 bzw. Abschnitt 1.2 (2008).

Aufgabe 1.4 Welche drei Fehler sind in folgendem Satz gemeint?

> Dieser Sats enthält drei Feler.

Aufgabe 1.5 Was könnte in der folgenden kleinen Geschichte die Kannibalen in Verwirrung gebracht haben?

> Ein Reisender gerät unter Kannibalen, die ihn gefangen nehmen und anschließend zur Bereicherung ihres Speiseplanes essen wollen. Die Kannibalen sind sich nur noch nicht einig, wie sie ihn zubereiten sollen. Sie bieten ihm an, er könne irgendeine Aussage machen. Wenn die Aussage wahr ist, werde er gekocht, und wenn sie falsch ist, werde er geröstet ... Seine Aussage lautet: „Das, was ich jetzt sage, ist falsch.“ Dieser Satz stürzte die Kannibalen in große Verwirrung.

1.2 Verknüpfungen von Aussagen

Mathematische Aussagen bezeichnen wir mit kleinen Buchstaben a, b, c usw. Wir ordnen ihnen genau einen der beiden *Wahrheitswerte* zu

entweder 1 (wahr) oder 0 (falsch).

Aussagen setzen wir durch folgende *Junktoren* miteinander in Beziehung

$$\neg, \quad \wedge, \quad \vee, \quad \rightarrow, \quad \leftrightarrow .$$

In dieser Reihenfolge bedeuten sie: *nicht, und, oder, folgt* (impliziert), *äquivalent.*

Die Bedeutungen dieser Verknüpfungen definieren wir wie folgt anhand einer *Wahrheitstabelle:*

a	b	$\neg a$	$\neg b$	$a \wedge b$	$a \vee b$	$a \rightarrow b$	$b \rightarrow a$	$a \leftrightarrow b$
0	0	1	1	0	0	1	1	1
0	1	1	0	0	1	1	0	0
1	0	0	1	0	1	0	1	0
1	1	0	0	1	1	1	1	1

Beispiel. Es besitzen $a \rightarrow b$ und $\neg a \vee b$ dieselben Wahrheitstabellen:

a	b	$a \rightarrow b$	$\neg a$	$\neg a \vee b$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

Sie heißen daher im *aussagenlogischen Sinne äquivalent,* in Zeichen

$$(a \rightarrow b) \equiv (\neg a \vee b).$$

Die runden Klammern geben dabei an, in welcher Reihenfolge die Verknüpfungen auszuführen sind. Wir vereinbaren: Von der höchsten zur niedrigsten Priorität sind der Reihe nach auszuführen $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.

Statt $\rightarrow$ benutzen wir später auch oft einen Doppelpfeil: $\Rightarrow$

Aufgaben

Aufgabe 1.6 Beweisen Sie die aussagenlogische Äquivalenz vermittels einer Wahrheitstabelle

$$\neg\neg a \equiv a.$$

Aufgabe 1.7 Beweisen Sie die folgenden aussagenlogischen Äquivalenzen vermittels Wahrheitstabellen:

(i) $a \to b \equiv \neg a \vee b$
(ii) $a \to b \equiv \neg b \to \neg a$
(iii) $a \leftrightarrow b \equiv (a \vee \neg b) \wedge (\neg a \vee b)$

Aufgabe 1.8 Beweisen Sie die folgenden aussagenlogischen Äquivalenzen vermittels Wahrheitstabellen:

(i) $a \vee b \equiv b \vee a$
(ii) $a \wedge b \equiv b \wedge a$

Aufgabe 1.9 Beweisen Sie die folgenden aussagenlogischen Äquivalenzen vermittels Wahrheitstabellen:

(i) $a \wedge (b \vee c) \equiv (a \wedge b) \vee (a \wedge c)$
(ii) $a \vee (b \wedge c) \equiv (a \vee b) \wedge (a \vee c)$

Aufgabe 1.10 Beweisen Sie die folgenden aussagenlogischen Äquivalenzen vermittels Wahrheitstabellen:

(i) $a \equiv a \wedge (a \vee b)$
(ii) $a \equiv a \vee (a \wedge b)$

Man bezeichnet $a \vee b$ auch als Disjunktion und $a \wedge b$ als Konjunktion.

Aufgabe 1.11 Beweisen Sie die folgenden aussagenlogischen Äquivalenzen vermittels Wahrheitstabellen:

(i) $\neg(a \wedge b) \equiv \neg a \vee \neg b$
(ii) $\neg(a \vee b) \equiv \neg a \wedge \neg b$

1.3 Aussagenlogische Beweisprinzipien

Grundlegend für die gesamte Mathematik ist der Begriff der Tautologie.

Unter einer *Tautologie* verstehen wir eine Aussage, die unabhängig von der Belegung ihrer Variablen durch die Wahrheitswerte 0 oder 1 *stets wahr* ist.

Beispiele solcher Tautologien, die auch gleichzeitig grundlegende mathematische Beweisprinzipien darstellen, beinhaltet der in den Übungen zu beweisende

Satz 1.1: Die folgenden Aussagen sind Tautologien:

(i)	Satz vom ausgeschlossenen Dritten	$a \vee \neg a$
(ii)	Satz vom Widerspruch	$\neg(a \wedge \neg a)$
(iii)	Satz von der doppelten Verneinung	$\neg(\neg a) \to a$
(iv)	Satz von der Kontraposition	$(a \to b) \to (\neg b \to \neg a)$
(v)	Satz zum modus ponens	$(a \to b) \wedge a \to b$
(vi)	Satz zum modus tollens	$(a \to b) \wedge \neg b \to \neg a$
(vii)	Satz zum modus barbara	$(a \to b) \wedge (b \to c) \to (a \to c)$

Wir möchten aus dieser Liste vier, in unseren Vorlesungen stets wiederkehrende und daher besonders wichtige Beweisprinzipien herausgreifen und in Worten formulieren.

- *Satz vom ausgeschlossenen Dritten*

  → Entweder es gilt a, oder es gilt nicht a. Ein Drittes gibt es nicht.

- *Satz vom Widerspruch*

  → Eine Aussage a und ihre Negation $\neg a$ sind nie gleichzeitig wahr.

- *Satz zum modus ponens (direkter Beweis)*

  → Gilt a, und folgt b aus a, so gilt auch b.

- *Satz zum modus tollens (indirekter Beweis)*

  → Gilt $\neg b$, und kann b aus a abgeleitet werden, so gilt nicht a.

Bemerkung. Ohne Beweis bemerken wir, dass aus einer falschen Aussage alles geschlossen werden kann. Das ist der Grund, warum wir in der Mathematik besonders viel Wert auf saubere Beweise legen.

Aufgaben

Aufgabe 1.12 Beweisen Sie die folgenden aussagenlogischen Tautologien vermittels Wahrheitstabellen:

(i) Satz vom ausgeschlossenen Dritten $a \vee \neg a$
(ii) Satz vom Widerspruch $\neg(a \wedge \neg a)$
(iii) Satz von der doppelten Verneinung $\neg(\neg a) \to a$
(iv) Satz von der Kontraposition $(a \to b) \to (\neg b \to \neg a)$

Aufgabe 1.13 Beweisen Sie die folgenden aussagenlogischen Tautologien vermittels Wahrheitstabellen:

(i) Satz zum modus ponens $(a \to b) \wedge a \to b$
(ii) Satz zum modus tollens $(a \to b) \wedge \neg b \to \neg a$
(iii) Satz zum modus barbara $(a \to b) \wedge (b \to c) \to (a \to c)$
iv Satz von der Kontraposition: $(a \to b) \to (\neg b \to \neg a)$

Aufgabe 1.14 Beweisen Sie vermittels Wahrheitstabellen die Distributivgesetze der Aussagenlogik:

1. $a \wedge (b \vee c) \equiv (a \wedge b) \vee (a \wedge c)$.
2. $a \vee (b \wedge c) \equiv (a \vee b) \wedge (a \vee c)$.

Aufgabe 1.15 Beweisen Sie die folgenden aussagenlogischen Tautologien vermittels Wahrheitstabellen:

(i) Kompressionsregel $a \vee a \to a$
(ii) Expansionsregel $a \to a \vee b$

Aufgabe 1.16 Es seien a und $\neg a$ gleichzeitig wahr, und es sei b eine beliebige andere Aussage. Beweisen Sie (ohne Wahrheitstabelle), dass dann auch b wahr ist. Vervollständigen Sie dazu folgendes abstrakte Schema:

(1) es gilt a
(2) es gilt $\neg a$
(3) die Expansionsregel, angewandt auf (2) und auf b, ergibt .....
(4) unter Verwendung der Implikation $\to$ schreibt sich (3) in der Form .....
(5) der Satz zum modus ponens, angewandt auf (4) und (1), ergibt .....

1.4 Aussagenlogik in SageMath

Aussagenlogische Formeln lassen sich leicht in SageMath übergeben und auswerten. Wir wollen davon am Beispiel der Ermittlung von Wahrheitstabellen einfacher Beispielformeln überzeugen. Dabei gehen wir nach

https://doc.sagemath.org/pdf/en/reference/logic/logic.pdf

vor, wo sich viele weitere Möglichkeiten, Aussagenlogik unter Sagemath zu realisieren, finden.

Aussagenlogische Variablen werden als gewöhnliche Buchstaben geschrieben, eventuell mit Unterstrich, und die Junktoren werden wie folgt realisiert:

Unsere Symbolik	$\neg$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$
SageMath	`~`	`&`	`|`	`->`	`<->`

Dazu ein Beispiel.

Den Satz zum modus ponens übergeben wir SageMath wie folgt:

```
f = propcalc.formula("((a->b)&a)->b")
```

Um die Formel f als Tautologie zu verifizieren, ermitteln wir ihre Wahrheitstabelle. Die Wahrheitswerte werden als `False` für 0 bzw. `True` für 1 ausgeben.

Hierzu gehen wir wie folgt vor:

```
f.truthtable()
```

SageMath gibt daraufhin aus

```
a      b      value
False  False  True
False  True   True
True   False  True
True   True   True
```

Wir können f auch für individuelle Argumente auswerten:

```
f.evaluate('a':True, 'b':False, 'c':False)
```

Aufgaben

Aufgabe 1.17 Verifizieren Sie unter Verwendung von SageMath, dass es sich bei folgenden Formeln um Tautologien handelt:

(i) $a \vee (b \wedge \neg b) \to a$
(ii) $a \wedge (b \vee \neg b) \to a$

Erläutern Sie diese Aussagen mit eigenen Worten.

Bemerkung. Die Aussage (i) bezeichnet man auch als *reductio ad absurdum.*

Aufgabe 1.18 Verifizieren Sie unter Verwendung von SageMath, dass es sich bei folgenden Formeln um Tautologien handelt:

(i) $a \to ((a \to b) \to b)$
(ii) $a \to (b \to (a \to b))$
(iii) $((a \to b) \to a) \to a$
(iv) $\neg(a \to b) \to \neg b$
(v) $\neg(a \to b) \to a$

Erläutern Sie diese Aussagen mit eigenen Worten.

Bemerkung. Aussage (iii) bezeichnet man auch *Gesetz von Peirce.*

Aufgabe 1.19 Verifizieren Sie unter Verwendung von SageMath, dass es sich bei folgenden, zum Teil bereits bekannten Formeln um Tautologien handelt:

(i) $a \vee a \to a$
(ii) $a \to a \vee b$
(iii) $(a \vee b) \wedge (\neg a \vee c) \to (b \vee c)$

Erläutern sie diese Aussagen mit eigenen Worten.

Bemerkung. Es heißt (iii) *Schnittregel.* Diese drei Regeln dienen in J. Shoenfields Axiomensystem der Aussagenlogik als Schlussregeln neben dem Satz vom ausgeschlossenen Dritten als einzigem Axiom, siehe Hodel [**?**].

Aufgabe 1.20 Ermitteln Sie unter Verwendung von SageMath die Wahrheitswerte der folgenden Formeln für die Argumente $a = 1$ und $b = 0$.

(i) $(a \vee \neg b) \wedge a \to a \wedge (b \vee \neg a)$
(ii) $(\neg a \wedge b) \vee (a \wedge\ b) \to a \vee (a \vee\ \neg a \vee\ \neg b) \wedge (a \vee\ \neg b)$

1.5 Quantoren

In der Mathematik haben wir es mit *Variablen* $x, y, \ldots$ als *Elementen von Mengen* X zu tun, in Zeichen

$$x, y, \ldots \in X.$$

Für ihre Beschreibung benötigen wir Quantoren.

Es sei p eine von einer Variablen $x \in X$ abhängige Aussageform. Der *Allquantor* $\forall$ und der *Existenzquantor* $\exists$ sind dann wie folgt definiert:

- $\forall x \in X \,:\, p(x)$
  sprich: für alle Elemente x aus X ist die Aussage $p(x)$ wahr
- $\exists x \in X \,:\, p(x)$
  sprich: es existiert ein Element x aus X, für welches die Aussage $p(x)$ wahr ist

Im zweiten Punkt bedeutet „es existiert“ die Existenz wenigstens eines Elementes $x \in X$. Ferner dient der Doppelpunkt hierin nur zur bessere Lesbarkeit und kann auch weggelassen werden.

Beispiel. Bedeutet $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ die Menge der natürlichen Zahlen (auf Zahlenbereiche kommen wir noch genauer zu sprechen), so gelten

$$\exists n \in \mathbb{N} \,:\, n = 2 \quad \text{und} \quad \forall n \in \mathbb{N} \,:\, n \geq 0.$$

Oft benötigen wir von mathematischen Aussagen die Negation. Dazu hilft uns die nächste Definition.

Der Allquantor $\forall$ und der Existenzquantor $\exists$ werden wie folgt *negiert*

$$\neg \forall x \, p(x) \equiv \exists x \, \neg p(x), \quad \neg \exists x \, p(x) \equiv \forall x \, \neg p(x).$$

Linksseitig wirkt der Negationsoperator jeweils auf die gesamten Ausdrücke $\forall x \, p(x)$ bzw. $\exists x \, p(x)$.

Beispiel. Wir ermitteln

$$\neg \forall x \, \exists y \, p(y) \equiv \exists x \, \neg \exists y \, p(y) \equiv \exists x \forall y \, \neg p(y).$$

Aufgaben

Aufgabe 1.21 Es bezeichne $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ die Menge der ganzen Zahlen. Schreiben Sie die folgenden Aussagen als prädikatenlogische Formeln. Welche Aussage ist wahr, welche ist falsch?

(i) Es existieren ein $x \in \mathbb{Z}$ und ein $y \in \mathbb{Z}$ mit $x + y = 0$.
(ii) Für alle $x \in \mathbb{Z}$ existiert ein $y \in \mathbb{Z}$ mit $x + y = 0$.
(iii) Es existiert ein $x \in \mathbb{Z}$, so dass für alle $y \in \mathbb{Z}$ gilt $x + y = 0$.
(iv) Für alle $x \in \mathbb{Z}$ und für alle $y \in \mathbb{Z}$ gilt $x + y = 0$.

Aufgabe 1.22 Es bezeichne $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ die Menge der natürlichen Zahlen. Formulieren Sie die folgenden prädikatenlogischen Formeln in Worten. Welche Aussage ist wahr, welche ist falsch? Negieren Sie die Aussagen. Sind die Negationen wahr? Begründen Sie jeweils anhand eines Beispiels bzw. Gegenbeispiels.

(i) $\exists m \in \mathbb{N}\, \forall n \in \mathbb{N}\, (m < n)$
(ii) $\exists m \in \mathbb{Z}\, \forall n \in \mathbb{N}\, (m < n)$
(iv) $\forall m \in \mathbb{N}\, \exists nin \mathbb{N}\, (n < m)$
(v) $\forall m \in \mathbb{N}\, \exists n \in \mathbb{Z}\, (n < m)$

Aufgabe 1.23 Es sei $f \colon \mathbb{R} \to \mathbb{R}$ eine reellwertige Funktion. Negieren Sie die folgende Formel der Stetigkeit dieser Funktion in einem Punkt $x_0 \in \mathbb{R}$, d.h.

$$\forall \varepsilon > 0\, \exists \delta > 0\, \forall x \in \Omega\, (|x - x_0| < \delta \to |f(x) - f(x_0)| < \varepsilon)$$

mit dem Ergebnis

$$\exists \varepsilon > 0\, \forall \delta > 0\, \exists x \in \Omega\, (|x - x_0| < \delta \wedge |f(x) - f(x_0)| \geq \varepsilon).$$

Formulieren Sie die Formel auch mit eigenen Worten.

Neben dieser „ε-δ-Definition“ der Stetigkeit werden wir hauptsächlich die sogenannte *Folgenstetigkeit* diskutieren.

Damit schließen wir unsere Einführung in die mathematische Logik ab.

Kapitel 2

Mengenlehre

2.1 Charakterisierung von Mengen

Georg Cantor definierte 1895 eine Menge wie folgt:

> Unter einer ‚Menge' verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objecten m unserer Anschauung oder unseres Denkens (welche die ‚Elemente' von M genannt werden) zu einem Ganzen.

Da diese wie auch spätere Definitionen des Mengenbegriffs nicht widerspruchsfrei waren, schlug E. Zermelo vor, Mengen besser durch ihre Eigenschaften axiomatisch zu *charakterisieren* und nicht zu definieren.

Wir gehen im Folgenden einen nichtaxiomatisch Weg.

Eine Menge M lässt sich auf zwei Arten charakterisieren, nämlich:

- durch Angabe ihrer Elemente m_1, m_2, m_3 usw., in Zeichen

  $$M = \{m_1, m_2, m_3, \ldots\},$$

  wobei die Reihenfolge der Elemente nicht wichtig ist, aber Elemente werden nicht mehrfach angegeben werden;
- durch Angabe einer definierenden Eigenschaft, z.B.

  $$M = \{x \in X : p(x)\},$$

  d.h. es besteht M aus allen $x \in X$ mit der Eigenschaft $p(x)$.

Beispiel.

(i) Die Menge $M = \{1\}$ besitzt 1 als einziges Element.
(ii) Die Menge $M = \{1, \{1\}\}$ besteht aus den beiden Elementen 1 und $\{1\}$.
(iii) Es ist $\{x \in \mathbb{R} : x^2 = 2\} = \{\sqrt{2}, -\sqrt{2}\}$.
(iv) Es ist $\{n \in \mathbb{N} : 2^n < n^2\} = \{3\}$.

Nach der axiomatischen Mengenlehre von Zermelo und Fraenkel existiert genau eine *leere Menge* $\emptyset$, welche kein Element enthält. Sie ist *Teilmenge jeder Menge* (siehe unten für den Teilmengenbegriff). Es ist insbesondere

$$\{x \in X : p(x)\}$$

gleich der leeren Menge, falls die Aussage $p(x)$ für kein $x \in X$ wahr ist. Jede andere Menge besitzt wenigstens ein Element.

Aufgaben

Aufgabe 2.1 Welche Elemente besitzen die folgenden Mengen?

(i) $M = \{x \in \mathbb{N} : 1 \leq x \leq 34 \text{ und } x \text{ ist Primzahl}\}$
(ii) $M = \{x \in \mathbb{N} : x \text{ ist ohne Rest durch 2 teilbar}\}$

Aufgabe 2.2 Finden Sie für folgende Mengen jeweils eine charakterisierende Eigenschaft.

(i) $M = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$
(ii) $M = \{2, 4, 8, 16, 32, 64, \ldots\}$
(iii) $M = \{0.1, 0.01, 0.001, 0.0001, 0.00001, \ldots\}$

Historisches

In seiner Autobiographie *Lebenskreise* (1967) belegt A. Fraenkel die seinerzeit oft anzutreffenden Ressentiments gegenüber der Cantorschen Mengenlehre am Beispiel eines von H.A. Schwarz geleiteten Seminars an der Universität Berlin, welchem Fraenkel als Student beiwohnte:

> Am bequemsten machte es sich Schwarz. Er ließ den Studenten, die dazu Lust hatten, völlige Freiheit, in den Seminarstunden über beliebige Themen vorzutragen. Ich wählte mir, künftige Entwicklungen unbewußt antizipierend, als Thema die Elemente der in Berlin fast unbekannten Mengenlehre und erregte mit meinem zweistündigen Vortrag bei den Studenten lebhaftes Interesse. Der Professor verkündete indes in seinem Nachwort: Auch er habe von diesen bedenklichen Theorien Georg Cantors gehört, müsse aber die studierende Jugend ernstlich vor ihnen warnen.

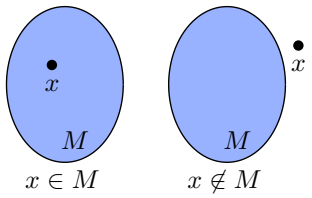


Abbildung 2.1: Enthält M das Element x, so schreibt man $x \in M$. Enthält M das Element x nicht, so schreibt man $x \notin M$. Zur Veranschaulichung benutzt man oft sogenannte *Venn-Diagramme,* wie in der dieser Abbildung.

2.2 Mengenrelationen und Mengenoperationen

Um mit Mengen rechnen zu können, benötigen wir verschiedene Relationen und Operationen zwischen ihnen, die wir nun einführen wollen. Beachten Sie, wie diese Relationen und Operationen auf den aussagenlogischen Junktoren und Operationen aufbauen.

Die Mengenrelationen $A = B$, $A \subset B$ und $A \subsetneq B$ zwischen zwei beliebigen Mengen A und B erklären wir wie folgt:

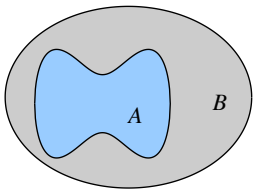
$A = B$	A ist gleich B	$x \in A \longleftrightarrow x \in B$
$A \subset B$	A ist Teilmenge von B	$x \in A \longrightarrow x \in B$
$A \subsetneq B$	A ist echte Teilmenge von B	$A \subset B \wedge A \neq B$

Hierin bedeutet $A \neq B$ die Aussage $\neg(A = B)$.

Die *Mengengleichheit* $A = B$ können wir auch so auffassen:

$$A = B \quad \text{genau dann, wenn} \quad A \subset B \text{ und } B \subset A,$$

und auf diese Weise werden auch Beweise zur Mengengleichheit $A = B$ geführt: erst $A \subset B$, dann $B \subset A$ zeigen.



Venn-Diagramm zu Teilmengenrelation $A \subsetneq B$

Die Mengenoperationen *Vereinigung* $A \cup B$, *Durchschnitt* $A \cap B$ und *Differenz* $A \setminus B$ zwischen beliebigen Mengen A und B erklären wir wie folgt:

$A \cup B$	A vereinigt B	$\{x : x \in A \vee x \in B\}$
$A \cap B$	A geschnitten B	$\{x : x \in A \wedge x \in B\}$
$A \setminus B$	A weniger B	$\{x : x \in A \wedge x \notin B\}$

Ferner vereinbaren wir ihr *kartesisches Produkt* $A \times B$ als die Menge folgender Zahlenpaare

$$A \times B := \{(x, y) : x \in A \wedge y \in B\}.$$

Schließlich benötigen wir noch das *Komplement* einer Menge A.

Es seien eine Menge X und eine Menge $A \subset X$ vorgelegt. Unter dem *Komplement* A^c von A in X verstehen wir

$$A^c := \{x \in X : x \notin A\}.$$

Aufgaben

Aufgabe 2.3 (Rechenübung zu den Mengenoperationen)
Gegeben seien eine Grundmenge $\Omega = \{0, 1, 2, 3, 4, 5, 6\}$ sowie die beiden Teilmengen $A = \{1, 2, 3\}$ und $B = \{2, 3, 4\}$. Ermitteln Sie

$$\Omega \setminus A, \quad \Omega \setminus B, \quad A \cup B, \quad A \cap B, \quad A \setminus B, \quad B \setminus A.$$

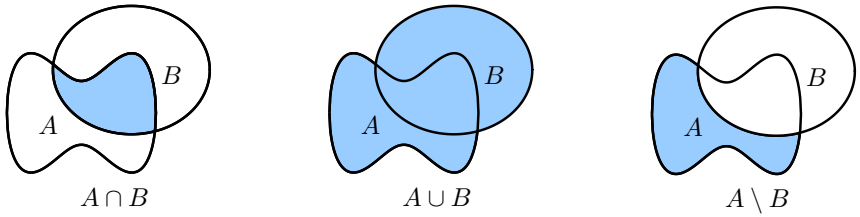


Abbildung 2.2: Venn-Diagramm zu den Mengenoperationen

Aufgabe 2.4 (Operationen mit der leeren Menge)
Es sei A eine beliebige Menge. Beweisen Sie:

a) $A \cup \emptyset = A$ b) $A \cap \emptyset = \emptyset$
c) $A \setminus A = \emptyset$ d) $A \setminus \emptyset = A$

Aufgabe 2.5 (Regeln zur Komplementbildung)
Es sei A eine Teilmenge einer Obermenge X, so dass insbesondere $A, A^c \subset X$ gelten. Beweisen Sie

a) $A \cap A^c = \emptyset$ b) $A \cup A^c = X$ c) $(A^c)^c = A$

Aufgabe 2.6 Betrachte die nachfolgenden:

$$L = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}.$$

Für alle $A, B \in L$ bestimme ob $A \in B$ und ob $A \subset B$.

Aufgabe 2.7 (Kartesisches Produkt von Mengen)
Ermitteln Sie das kartesische Produkt $M \times N$ der folgenden Mengen:

(i) $M = \{1, 2, 3, 4\}$ und $N = \{a, b\}$
(ii) $M = \{1, 2, 3, 4, \ldots\}$ und $N = \{1, 2, 3, 4, \ldots\}$
(iii) $M = \{x \in \mathbb{N} : 2 \leq x \leq 3\}$ und $N = \{x \in \mathbb{N} : 6 \leq x < 9\}$

2.3 Rechenregeln für Mengen

In Verallgemeinerung der aussagenlogischen Formeln

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c), \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

beweisen wir den

Satz 2.1: Für drei beliebige Mengen A, B und C gelten die folgenden Distributivgesetze:

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Beweis. Wir zeigen nur die erste Behauptung. Wählen ein $x \in A \cap (B \cup C)$ beliebig.Wir wenden den aussagenlogischen Distributivgesetz für $\wedge$ und $\vee$ in der dritten Zeile auf die Aussagen $x \in A$ usw. an:

$$\begin{aligned} x \in A \cap (B \cup C) &\iff (x \in A) \wedge (x \in B \cup C) \\ &\iff (x \in A) \wedge (x \in B \vee x \in C) \\ &\iff (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\ &\iff (x \in A \cap B) \vee (x \in A \cap C) \\ &\iff x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Es ist also $x \in (A \cap B) \cup (A \cap C)$, genau dann, wenn $x \in A \cap (B \cup C)$, Da x beliebig gewählt wurde, folgt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. ∎

Satz 2.2: Sind A und B zwei beliebige Teilmengen einer Obermenge X, so gelten die folgende de Morganschen Regeln:

1. $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$
2. $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$

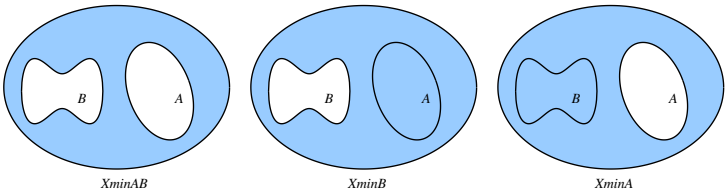


Abbildung 2.3: Zur ersten de Morganschen Regel - beschriften Sie die Skizzen!

Aufgaben

Aufgabe 2.8 Es seien A, B und C drei beliebige Mengen. Beweisen Sie:

(i) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(ii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Aufgabe 2.9 Es seien A und B zwei beliebige Teilmengen einer nichtleeren Obermenge X. Beweisen Sie:

(i) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$
(ii) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$

Aufgabe 2.10 Es seien A, B, C, D beliebige Mengen. Welche der folgenden Behauptungen ist richtig, welche falsch? Beweisen Sie bzw. begründen Sie gegebenenfalls durch ein Gegenbeispiel.

(i) $(A \cap C) \cup (B \cap D) \subset (A \cup B) \cap (C \cup D)$
(ii) $(A \cap C) \cup (B \cap D) = (A \cup B) \cap (C \cup D)$

Aufgabe 2.11 Es seien A, B und C drei beliebige Mengen. Beweisen Sie:

a) $(A \setminus B) \setminus C = A \setminus (B \cup C)$ b) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \setminus C)$

Aufgabe 2.12 Seien A, B Teilmengen einer Menge X, d.h. $A, B, A^c, B^c \subset X$. Beweisen Sie:

a) $A \setminus B = A \cap B^c$ b) $(A \setminus B)^c = A^c \cup B$

Aufgabe 2.13 Die de Morganschen Regeln sind nicht nur für zwei Teilmengen $A, B \subset X$ einer Obermenge X richtig, sondern auch für Teilmengen $A_i \subset X$ mit $i \in I$ aus einer einer *beliebigen* Indexfamilie I. Zeigen Sie dafür:

a) $\left(\bigcup_{i \in I} A_i \right)^c = \bigcap_{i \in I} A_i^c$ b) $\left(\bigcap_{i \in I} A_i \right)^c = \bigcup_{i \in I} A_i^c$

mit den Setzungen

$$\bigcup_{i \in I} A_i := \{x \,:\, x \in A_i \text{ für ein } i \in I\},$$
$$\bigcap_{i \in I} A_i := \{x \,:\, x \in A_i \text{ für alle } i \in I\}.$$

2.4 Rechnen mit Mengen in SageMath

Die elementaren Rechenoperationen lassen sich leicht in SageMath realisieren. Wir wollen das ein einfachen Beispielen endlicher Mengen demonstrieren und gehen dabei nach

https://doc.sagemath.org/pdf/en/reference/sets/sets.pdf

vor. Zunächst übergeben wir die beiden endlichen Menge $A = \{1, 2, 3, 4, 5, 6, 7\}$ und $B = \{3, 4, 5, 7\}$:

```
a = [1, 2, 3, 4, 5, 6, 7]; A = Set(a)
b = [3, 4, 5, 7]; B = Set(b)
```

Auf folgende Weise verifiziert man die gegenseitigen Teilmengenrelationen:

```
A.issubset(B)
B.issubset(A)
```

SageMath gibt die Resultate `False` bzw. `True` zurück. Vereinigung, Durchschnitt und Differenz lassen sich schließlich wie folgt ermitteln:

```
A.union(B)
A.intersection(B)
A.difference(B)
```

Das Hinzufügen und Streichen einzelner Elemente zu bzw. aus Mengen

```
A.add(8)
B.discard(7)
```

mit den Resultaten `{1, 2, 3, 4, 5, 6, 7, 8}` für A und `{3, 4, 5, 6}` für B. Dass 8 jetzt tatsächlich Element von A ist, prüfen wir schließlich mit

```
8 in A
```

mit der Ausgabe `True`.

Aufgaben

Aufgabe 2.14 Vorgelegt seien die beiden Mengen

$$A = \{1, 2, 3, 4, 5, 6, 7\}, \quad B = \{3, 4, 5, 7\}.$$

Ermitteln Sie unter Verwendung von SageMath

$$A \cup B, \quad A \cap B, \quad A \setminus B, \quad B \setminus A.$$

Die Differenz $B \setminus A$ ist natürlich gleich der leeren Menge $\emptyset$, was SageMath wie folgt verifiziert:

```
B.difference(A).is_empty()
```

Aufgabe 2.15 Es sei wieder $A = \{1, 2, 3, 4, 5, 6, 7\}$. Ermitteln Sie unter Verwendung von SageMath

a) $A \cup \emptyset = A$ b) $A \cap \emptyset = \emptyset$ c) $A \setminus A = \emptyset$ d) $A \setminus \emptyset = A$

Aufgabe 2.16 Wir betrachten die drei Mengen

$$A = \{1, 2, 3, 5, 8\}, \quad B = \{2, 4, 6, 8, 10\}, \quad C = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

Werten Sie jeweils mit einem einzigen Befehl unter SageMath aus:

(i) $C \setminus (A \cup B)$ und $(C \setminus A) \cap (C \setminus B)$
(ii) $C \setminus (A \cap B)$ und $(C \setminus A) \cup (C \setminus B)$
(iii) $(A \setminus B) \setminus C$ und $A \setminus (B \cup C)$
(iv) $A \setminus (B \setminus C)$ und $(A \setminus B) \cup (A \setminus C)$

Welche bekannten Rechenregeln erkennen Sie wieder?

Aufgabe 2.17 Wir betrachten die zwei Mengen

$$A = \{1, 2, 3, 5, 8\}, \quad B = \{2, 4, 6, 8, 10, 18, 93\}$$

sowie die A und B enthaltene Obermenge

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 18, 27, 93, 132\}.$$

Verifizieren Sie anhand dieser Mengen folgenden Rechenregeln:

a) $(A \cup B)^c = A^c \cap B^c$ b) $(A \cap B)^c = A^c \cup B^c$
c) $A \setminus B = A \cap B^c$ d) $(A \setminus B)^c = A^c \cup B$

2.5 Abbildungen zwischen Mengen

Der Begriff der Abbildung ist grundlegend für die gesamte Mathematik.

Unter einer *Abbildung* (auch Funktion genannt) zwischen zwei Mengen A und B, in Zeichen

$$f\colon A \longrightarrow B,$$

verstehen wir eine Vorschrift, die jedem $a \in A$ genau $b \in B$ zuordnet.

Hierin heißen A die *Urbildmenge* und B der *Wertebereich.* Ferner heißt $b \in B$ das *Bild von a unter f*, falls $f(a) = b$.

Beachten Sie: Eine Abbildung $f\colon A \to B$, oder wie wir auch sagen: *Funktion,* ist stets in allen Punkten $a \in A$ definiert, aber nicht jedes $b \in B$ muss Bild eines *Urbildes* $a \in A$ sein.

Beispiel. Folgende Definition einer Funktion $f(x)$ ist nicht möglich - warum?

$$f(x) := \frac{1}{x}, \quad x \in \mathbb{R}.$$

Funktionen sind natürlich auch in der Informatik von Bedeutung. Ein Computerprogramm ist tatsächlich eine Funktion mit einer Eingabe x und einer Ausgabe $f(x)$.

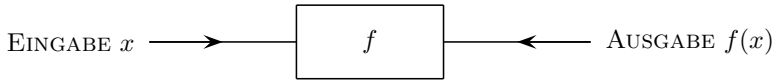


Abbildung 2.4: Ein Computerprogramm ist eine Funktion

Wie eine Funktion nun beschrieben wird, hängt ganz von den Umständen ab.

- In unseren Vorlesungen beschreiben wir Funktionen in der Regel durch *Funktionsvorschriften,* wie beispielsweise

$$f\colon \mathbb{R} \longrightarrow \mathbb{R} \quad \text{vermöge} \quad f(x) = x^2 + 3x - 4.$$

- Ist der Definitionsbereich endlich, so können wir $f(x)$ für alle Elemente x auch einfach *auflisten,* beispielsweise durch Aufzählen in der Form

$$\{(0, f(0)), (1, f(1)), (2, f(2)), (3, f(3), (4, f(4))\}$$

oder tabellarisch gemäß

i	0	1	2	3	4
$f(i)$	$f(0)$	$f(1)$	$f(2)$	$f(3)$	$f(4)$

Beispiele

1. Seien A die Menge aller Dreiecke in der Ebene und B die Menge aller Punkte der Ebene. Wir können eine Abbildung von A nach B konstruieren, indem wir jedem Dreieck aus A seinen Schwerpunkt in B zuordnen. Es sei A die Menge der Studierenden, welche über ein Handy verfügen. Wir können dann eine Abbildung von A in die Menge der ganzen Zahlen konstruieren, indem wir jedem Studierenden $a \in A$ seine Telefonnummer zuordnen.
2. Die identitätsabbildung id_A ist definiert durch $\mathrm{id}_A(a) = a$ für alle $a \in A$.
3. Ist $f\colon A \to B$ und $g\colon B \to C$, so ist die Verkettung $g \circ f\colon A \to C$ definiert durch $g \circ f(a) := g(f(a))$ für alle $a \in A$.

Unter dem *Graphen* $\Gamma(f)$ einer Funktion $f\colon A \to B$ verstehen wir die Menge

$$\Gamma(f) := \{(x, f(x)) \,:\, x \in A\} \subset A \times B.$$

Eine Funktion ist durch ihren Graphen bestimmt und umgekehrt.

Aufgaben

Aufgabe 2.18 In welchen der nachfoglenden Fällen liegt eine Abbildung vor?

1. $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(k) = 2k$ für alle $k \in \mathbb{N}$.
2. $f\colon \mathbb{N} \to \mathbb{Z}$ mit $f(k) = 2k$ für alle $k \in \mathbb{N}$.
3. $f\colon \mathbb{N} \setminus \{0\} \to \mathbb{Z}$ mit $f(k) = 2k$ für alle k
4. $f\colon \mathbb{N} \to \mathbb{N} \setminus \{0\}$ mit $f(k) = 2k$ für alle k
5. $f\colon \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ mit $f(k) = 2k$ für alle k
6. $f\colon \mathbb{N} \to \mathbb{Q}$ mit $f(n) = 1/n$ für alle $n \in \mathbb{N}$.
7. $f\colon \mathbb{N} \setminus \{0\} \to \mathbb{Q}$ mit $f(n) = 1/n$ für alle $n \in \mathbb{N}$.
8. $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = n/2$ für alle $n \in \mathbb{N}$.
9. $f\colon 2\mathbb{N} \to \mathbb{N}$ mit $f(n) = n/2$ für alle $n \in \mathbb{N}$ wobei $2\mathbb{N} = \{2n\colon n \in \mathbb{N}\}$.
10. $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = 2n \forall n$ und $f(0) = 0$.
11. $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = 2n \forall n$ und $f(0) = 2$.
12. $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = 2n \forall n$ mit $n \neq 0$ und und $f(0) = 2$. $f\colon \mathbb{N} \setminus \{0\} \to \mathbb{N}$ mit $f(n) = 2n \forall n$ mit $n \neq 0$ und und $f(0) = 2$.
13. $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = 2n \forall n$ mit $n \neq 0$.

2.6 Surjektiv, injektiv und bijektiv

Eine Abbildung $f\colon A \to B$ zwischen zwei Mengen A und B heißt

1. *surjektiv,* wenn für jedes $b \in B$ ein $a \in A$ existiert mit $f(a) = b$;
2. *injektiv,* wenn die Gleichung $f(a) = b$ für gegebenes $b \in B$ höchstens eine Lösung $a \in A$ besitzt, d.h.

   sind $a_1, a_2 \in A$ mit $a_1 \neq a_2$, so gilt $f(a_1) \neq f(a_2)$ bzw.
   sind $a_1, a_2 \in A$ mit $f(a_1) = f(a_2)$, so gilt $a_1 = a_2$;
3. *bijektiv,* wenn f surjektiv und injektiv ist.

Es sei $f\colon A \to B$:

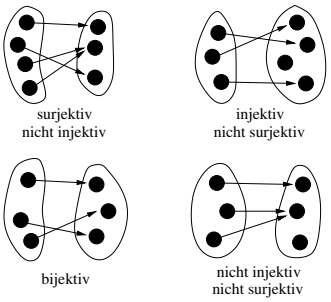
1. Für $X \subset A$ definieren wir $f(X) = \{f(x)\colon x \in A\}$: das Bild von X.
2. Für $Y \subset B$ definieren wir $f^{-1}(Y) = \{a \in A\colon f(a) \in Y\}$; das totale Urbild von Y.

Insbesondere ist eine Abbildung $f\colon A \to B$

- nicht surjektiv, wenn ein $b \in B$ gibt, welches nicht in der *Bildmenge*

  $$f(A) := \{b \in B \,:\, \text{es existiert ein } a \in A \text{ mit } f(a) = b\}$$

  von f liegt,
- surjektiv genau dann, wenn $f(A) = B$.
- nicht injektiv, wenn es $a_1 \neq a_2$ aus A gibt mit $f(a_1) = f(a_2)$.



Eine bijektive Abbildung $f\colon A \to B$ ordnet jedem $a \in A$ genau ein $b \in B$ zu, und umgekehrt wird jedem $b \in B$ genau ein $a \in A$ zugeordnet. Diese letztere Zuordnung heißt *inverse Abbildung* oder *Umkehrfunktion* von f, in Zeichen

$$f^{-1}\colon B \longrightarrow A.$$

Sie genügt also den Eigenschaften

$$f^{-1}(f(a)) = a \quad \text{für alle } a \in A, \qquad f(f^{-1}(b)) = b \quad \text{für alle } b \in B.$$

Aufgaben

Aufgabe 2.19 Wir betrachten die Abbildung $f\colon A \to B$ vermöge $f(x) := x^2$. Verifizieren Sie

(i) Im Fall $A = [-1,1]$ und $B = [-1,1]$ ist f weder injektiv noch surjektiv.
(ii) Im Fall $A = [0,1]$ und $B = [-1,1]$ ist f injektiv, aber nicht surjektiv.
(iii) Im Fall $A = [-1,1]$ und $B = [0,1]$ ist f surjektiv, aber nicht injektiv,
(iv) Im Fall $A = [0,1]$ und $B = [0,1]$ ist f sowohl injektiv wie auch surjektiv.

Aufgabe 2.20 Es seien A und B zwei nichtleere Mengen und $f\colon A \to B$ und $g\colon B \to A$ zwei Abbildungen mit

$$g(f(a)) := g \circ f(a) = a \quad \text{für alle } a \in A.$$

Beweisen Sie, dass f injektiv und g surjektiv ist.

Aufgabe 2.21 Es seien $f\colon A \to B$ und $g\colon B \to C$ zwei Abbildungen zwischen den nichtleeren Mengen A, B und C. Beweisen Sie:

(i) Ist $g \circ f$ bijektiv, so sind f injektiv und g surjektiv.
(ii) Sind f injektiv und g surjektiv, so ist $g \circ f$ nicht notwendig bijektiv.
(iii) Sind f und g injektiv, so ist auch $g \circ f$ injektiv.
(iv) Sind f und g surjektiv, so ist auch $g \circ f$ surjektiv.

Aufgabe 2.22 Es sei $f\colon X \to Y$ eine Abbildung zwischen den nichtleeren Mengen X und Y. Beweisen Sie, dass für alle $A, B \subseteq X$ mit $A \cap B \neq \emptyset$ gelten:

(i) $f(A \cup B) = f(A) \cup f(B)$
(ii) $f(A \cap B) \subset f(A) \cap f(B)$ mit Gleichheit, falls wenn f injektiv
(iii) $f(A \setminus B) \subset f(A)$

Aufgabe 2.23 Es sei $f\colon A \to B$ eine Abbildung zwischen den nichtleeren Mengen A und B. Ferner seien $\Omega, \Theta \subset B$ zwei echte Teilmengen. Beweisen Sie:

(i) $f^{-1}(\Omega \cup \Theta) = f^{-1}(\Omega) \cup f^{-1}(\Theta)$
(ii) $f^{-1}(\Omega \cap \Theta) = f^{-1}(\Omega) \cap f^{-1}(\Theta)$
(iii) $f^{-1}(\Omega \setminus \Theta) = f^{-1}(\Omega) \setminus f^{-1}(\Theta)$

Aufgabe 2.24

1. Es sei $g\colon X \to Y$ und $g\colon Y \to X$ mit $g \circ f = \mathrm{id}_X$. (Man nennt g eine Linksinverse von f und f eine Rechtsinverse von g) Zeigen Sie, dass f injektiv ist genau dann, wenn f eine Linksinverse hat.

2. Es sei $f\colon X \to Y$ surjektiv und $h\colon X \to Z$.

   (a) Es existiert höchstens ein $g\colon Y \to Z$ mit $h = g \circ f$.

   (b) Ein solches g wie in a) existiert genau dann, wenn

$$\forall y \in Y \exists z \in Z \text{ sodass } \forall x \in f^{-1}(y) \text{ gilt } h(x) = z.$$

2.7 Mächtigkeit von Mengen

Unter der *Mächtigkeit einer Menge mit endlich vielen Elementen* $a_1, \ldots, a_n \in A$, verstehen wir die Anzahl $n \in \mathbb{N}$ ihrer Elemente, in Zeichen

$$|A| := n.$$

Im Fall unendlicher Mengen können wir aber nicht von einer solchen Anzahl sprechen. Daher machen wir mit G. Cantor folgende Definition:

Zwei Mengen A und B heißen *gleichmächtig,* wenn es eine bijektive Abbildung $f\colon A \to B$ gibt.

Für eine beliebige Menge A bezeichnen wir nun mit $\mathcal{P}(A)$ ihre *Potenzmenge,* d.h. die Menge, deren Elemente genau sämtliche Teilmengen von A sind.

Beispiel. Es ist (beachte, dass die leere Menge $\emptyset$ Teilmenge jeder Menge ist)

$$\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\},$$

denn $\emptyset$, $\{1\}$, $\{2\}$ und $\{1,2\}$ sind genau die vier möglichen Teilmengen von $\{1,2\}$.

Satz 2.3: Es sei A eine beliebige Menge. Dann existiert keine surjektive und damit auch keine bijektive Abbildung $f\colon A \to \mathcal{P}(A)$.

Beweis. Für jedes $a \in A$ ist $f(a) \in \mathcal{P}(A)$ eine Menge. Wir zeigen, dass

$$M := \{a \in A \,:\, a \notin f(a)\} \in \mathcal{P}(A)$$

nicht zum Bild $f(A) \subset \mathcal{P}(A)$ gehört. Wäre nämlich $M = f(a^*)$ für ein $a^* \in A$, so gilt nach Definition von M

$$a^* \in f(a^*) = M \quad \text{genau dann, wenn} \quad a^* \notin f(a^*).$$

Das ist aber ein Widerspruch, d.h. ein solches $a^* \in A$ existiert nicht. ———

Wir schreiben $|A| \leq |B|$ und sagen, B *ist mächtiger als* A, wenn eine *injektive* Abbildung $f\colon A \to B$ existiert.

Beispiel. Es ist $\mathcal{P}(A)$ stets mächtiger als A.

Da die Verkettung injektiver Abbildungen wieder injektiv ist, gilt

$$|A| \leq |B| \text{ und } |B| \leq |C|, \quad \text{dann} \quad |A| \leq |C|.$$

Im Fall $|A| \leq |B|$ und $|B| \leq |A|$ gibt uns der folgende *Satz von Cantor-Schröder-Bernstein* Auskunft, für dessen Beweis wir auf die Literatur verweisen.

Satz 2.4: Es seien A und B zwei beliebige Mengen mit der Eigenschaft $|A| \leq |B|$ und $|B| \leq |A|$. Dann gilt

$$|A| = |B|.$$

Existieren also injektive Abbildungen $f\colon A \to B$ und $g\colon B \to A$, so existiert auch eine Bijektion $h\colon A \to B$.

Aufgaben

Aufgabe 2.25 Bestimmen Sie die Potenzmengen folgender Mengen:

a) $M = \emptyset$ b) $M = \{a\}$
c) $M = \{a, b\}$ d) $M = \{a, b, c\}$
e) $M = \mathcal{P}(\emptyset)$ f) $M = \mathcal{P}(\{a\})$

Aufgabe 2.26 Es seien A und B zwei beliebige Mengen.

(i) Zeigen Sie durch Angabe eines Gegenbeispiels, dass nicht gilt

$$\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B).$$

(ii) Beweisen Sie die Richtigkeit der Aussage

$$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B).$$

Aufgabe 2.27 Es seien A und B zwei endliche Mengen. Beweisen Sie:

(i) $|A \cup B| + |A \cap B| = |A| + |B|$
(ii) $|A \cup B| = |A| + |B|$ genau dann, wenn $A \cap B = \emptyset$
(iii) $|A \setminus B| = |A| - |B|$, falls $B \subset A$

Damit schließen wir unsere Einführung in Mengenlehre und unser erstes Kapitel über die Grundlagen der Mathematik ab.

2.8 Mächtigkeiten in SageMath

Bedeutet A eine endliche Menge, so lässt sich leicht deren Mächtigkeit mit Hilfe von SageMath bestimmen:

```
A.cardinality()
```

Beispielsweise haben wir

```
A = Set([1,2,3,4])
A.cardinality()
```

mit der Ausgabe 4. Die Potenzmenge $\mathcal{P}(A)$ dieser Menge besitzt 8 Elemente. Hierzu bestimmen wir zunächst alle Teilmengen A und dann deren Anzahl:

```
P = Set(A.subsets())
P.cardinality()
```

Die Teilmengen von A lassen sich auch direkt ausgeben:

```
list(A.subsets())
```

Aufgaben

Aufgabe 2.28 Bestimmen Sie die Mächtigkeiten der folgenden Mengen und deren Potenzmengen unter Verwendung von SageMath.

a) $A = \emptyset$ b) $B = \{1\}$
c) $C = \{1, 2, 3\}$ d) $D = \{1, 2, a, b, c\}$

Gehen Sie in (iv) dabei wie folgt vor:

```
D = Set([1,2,'a','b','c'])
```

Kapitel 3

Elementare Zahlenbereiche

3.1 Die natürlichen Zahlen

Die *Menge der natürlichen Zahlen*

$$\mathbb{N} := \{0, 1, 2, 3, 4, 5, 6, \ldots\}$$

fasst die beim Zählen verwendeten Zahlen zusammen. Wir vereinbaren auch

$$\mathbb{N}_+ := \mathbb{N} \setminus \{0\} = \{1, 2, 3, 4, 5, 6, \ldots\}$$

für die Menge der *positiven* natürlichen Zahlen.

Innerhalb der natürlichen Zahlen lassen sich *Addition* $+$ und *Multiplikation* $\cdot$ uneingeschränkt ausführen, d.h. für alle $m, n \in \mathbb{N}$ sind $m + n \in \mathbb{N}$ und $m \cdot n \in \mathbb{N}$. Addition und Multiplikation genügen dabei den folgenden Rechenregeln.

Für alle $\ell, m, n \in \mathbb{N}$ gelten

- Kommutativität und Assoziativität bez. der Addition

  $$m + n = n + m, \ \ell + (m + n) = (\ell + m) + n$$

- Neutrales Element der Addition

  $m + 0 = m$
  und außer 0 gibt es keine weitere Zahl mit dieser Eigenschaft

- Kommutativität und Assoziativität bez der Multiplikation

  $$m \cdot n = n \cdot m, \ \ell \cdot (m \cdot n) = (\ell \cdot m) \cdot n$$

- Neutrales Element der Multiplikation

  $m \cdot 1 = m$
  und außer 1 gibt es keine weitere Zahl mit dieser Eigenschaft

- Distributivität

  $$\ell \cdot (m + n) = \ell \cdot m + \ell \cdot n$$

Ferner seien für alle $\ell, m, n \in \mathbb{N}$ folgende Kürzungsregeln richtig

aus $m + \ell = n + \ell$ folgt $m = n$,
aus $\ell \cdot m = \ell \cdot n$ und $\ell \neq 0$ folgt $m = n$.

Wir schreiben

$m \leq n$ genau dann, wenn es ein $k \in \mathbb{N}$ gibt mit $m + k = n$,
$m < n$ genau dann, wenn $m \leq n$ und $m \neq n$.

Als Übung zeigen wir die Eindeutigkeit dieser Zahl k. Ferner gilt

$$m \leq n, \quad \text{dann,} \quad m + k \leq n + k \quad \text{für alle } k \in \mathbb{N}.$$

Wir schreiben $n \geq m$ bzw. $n > m$, wenn $m \leq n$ bzw. $m < n$.

Es stellt $\leq$ eine *Ordnungsrelation* auf $\mathbb{N}$ dar, charakterisiert durch die folgenden Eigenschaften:

- es gilt $m \leq m$ für alle $m \in \mathbb{N}$ (Reflexivität)
- falls $m \leq n$ und $n \leq m$, dann $m = n$ (Antisymmetrie)
- falls $k \leq m$ und $m \leq n$, dann $k \leq n$ (Transitivität)
- entweder $m \leq n$ oder $n \leq m$ (Totalität)

Man spricht auch von einer *totalen Ordnung* oder *Totalordnung.*

Aufgaben

Aufgabe 3.1 Die Summe von 9 aufeinander folgenden natürlichen Zahlen beträgt 396. Wie lauten diese Zahlen?

Folgende Definition der Begriffe *unendlich* und *endlich* geht auf R. Dedekind: *Was sind und was sollen Zahlen?* (1888) zurück:

> Ein System S heißt UNENDLICH, wenn es einem echten Teile seiner selbst ähnlich ist ...; im entgegengesetzten Falle heißt S ein ENDLICHES System.

Wir benutzen heute für diese Definition den Begriff der bijektiven Abbildung, kurz: den einer Bijektionen. Eine Menge M heißt

- *endlich,* wenn es eine Bijektion zwischen M und der Menge $\{1, \ldots, n\}$ mit $n \in \mathbb{N}_+$ geeignet gibt,
- *unendlich,* wenn es eine Bijektion zwischen M und einer echten Teilmenge von M gibt.

Aufgabe 3.2 Einerseits gibt es weniger Quadratzahlen, also natürliche Zahlen der Form n^2 mit $n \in \mathbb{N}$, als natürliche Zahlen selbst, da alle Quadratzahlen natürlich sind, aber z.B. die Zahl 3 keine Quadratzahl ist. Andererseits, so argumentierte Galilei, gibt es „genauso viele“ Quadratzahlen wie natürliche Zahlen. Wie könnte er argumentiert haben? Gibt es einen Widerspruch? Erläutern Sie.

Aufgabe 3.3 Beweisen Sie: Falls $m \leq n$, so existiert genau ein $k \in \mathbb{N}$ mit $m+k = n$.

Aufgabe 3.4 Beweisen Sie, dass $\leq$ eine Ordnungsrelation auf $\mathbb{N}$ darstellt.

3.2 Das Prinzip der schwachen Induktion

Aus dem Peanoschen Axiomensystem lässt sich das folgende *Prinzip der vollständigen* oder auch *schwachen Induktion* ableiten.

Für jedes $k \in \mathbb{N}$ sei eine Aussage A_k derart gegeben, dass gelten:

(i) die Aussage A_0 sei richtig,

(ii) für alle $n \in \mathbb{N}$ folgt aus der Richtigkeit der Aussage A_n die Richtigkeit von A_{n+1}.

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

Oder anders ausgedrückt:

$$[A_0 \wedge (\forall n \in \mathbb{N} : A_n \to A_{n+1})] \longrightarrow \forall n \in \mathbb{N} : A_n \,.$$

Es heißt (i) der *Induktionsanfang,* und (ii) beinhaltet mit der Annahme der Richtigkeit von A_n die *Induktionsvoraussetzung* und mit dem Schluss von A_n auf A_{n+1} den *Induktionsschritt.*

Beispiel. Vermittels vollständiger Induktion beweisen wir, dass für alle $n \in \mathbb{N}_+$ die *Gaußsche Summenformel* richtig ist

$$A_n : \quad S_1(n) := \sum_{k=1}^{n} k \equiv 1 + 2 + \ldots + (n-1) + n = \frac{n(n+1)}{2} \,.$$

(i) Es ist A_1 richtig, denn es gelten

$$\sum_{k=1}^{1} k = 1 \quad \text{und} \quad \frac{n(n+1)}{2}\Big|_{n=1} = \frac{1 \cdot (1+1)}{2} = 1.$$

(ii) Für ein $n \in \mathbb{N}_+$ sei A_n richtig. Dann berechnen wir mit (i)

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

Das ist die Aussage A_{n+1}.

Nach dem Prinzip der vollständigen Induktion ist A_n für alle $n \in \mathbb{N}_+$ bewiesen.

Unabhängig vom Beweisaufbau müssen deutlich werden, dass ein Induktionsbeweis vorliegt, und an welchen Stellen Induktionsvoraussetzung, Induktionsannahme und Induktionsschluss eingehen.

Aufgaben

Aufgabe 3.5 (Beweisen Sie vermittels vollständiger Induktion

$$S_2(n) := \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \quad \text{für alle } n \in \mathbb{N}_+ .$$

Aufgabe 3.6 Beweisen Sie vermittels vollständiger Induktion

$$\sum_{k=1}^{n} (2k-1)^2 = \frac{n(2n-1)(2n+1)}{3} \quad \text{für alle } n \in \mathbb{N}_+ .$$

Schließen Sie nun auf eine Darstellung für die Summe der ersten n geraden Quadratzahlen.

Aufgabe 3.7 (i) Es seien $m, n \in \mathbb{N}$. Ermitteln Sie $(m+n)^k$ für $k = 1, 2, 3$.

(ii) Bestimmen Sie nun eine explizite Darstellung für $S_2(n)$ aus Aufgabe 2.2.1. Berechnen Sie dazu $(k+1)^3 - k^3$ nacheinander für $k = 1, \ldots, n$, und ermitteln Sie dann durch geschicktes Summieren

$$(n+1)^3 - (n+1) = 3 \cdot (1^2 + 2^2 + \ldots + n^2) + 3 \cdot (1 + 2 + \ldots + n).$$

Aufgabe 3.8 Beweisen Sie vermittels vollständiger Induktion

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4} \quad \text{für alle } n \in \mathbb{N}_+ .$$

Erkennen Sie einen Zusammenhang zur Gaußschen Summenformel?

Aufgabe 3.9 Beweisen Sie vermittels vollständiger Induktion, dass für alle $n \in \mathbb{N}_+$ gelten:

a) $\displaystyle\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$ b) $\displaystyle\sum_{k=0}^{n} 3^k = \frac{1}{2}\left(3^{n+1} - 1\right)$

Aufgabe 3.10 Beweisen Sie vermittels vollständiger Induktion:

(i) Für alle $n \in \mathbb{N}_+$ ist $n^3 + 5n + 3$ ohne Rest durch 3 teilbar.

(ii) Für alle $n \in \mathbb{N}_+$ ist $5^n + 7$ ohne Rest durch 4 teilbar.

(iii) Für alle $n \in \mathbb{N}_+$ ist $2^{7n+3} + 3^{2n+1} \cdot 5^{4n+1}$ ohne Rest durch 23 teilbar.

3.3 Endliche Summen in SageMath

Wir folgen nun

https://doc.sagemath.org/pdf/en/tutorial/SageTutorial.pdf
https://doc.sagemath.org/pdf/en/reference/calculus/calculus.pdf

Endliche Summen lassen sich in SageMath mit Hilfe von `sum` ermitteln. Beispielsweise wissen wir

$$\sum_{k=1}^{100} k = 5050,$$

was wir vermittels SageMath wie folgt verifizieren:

```
s = sum(k for k in [1..100])
```

mit dem Resultat `5050`, und ebenso für $S_2(100) = \sum_{k=1}^{100} k^2$:

```
s = sum(k^2 for k in [1..100])
```

mit dem Resultat `338350`. Mit einer `for`-Schleife lässt sich diese Summe auch „händisch“ berechnen:

```
s = 0
for k in range(1,101):
    s = s+k^2
```

mit dem Resultat `338350` nach Eingabe von `s`. Beachte hierbei die anfängliche Setzung `s = 0` sowie die obere Summationsgrenze `101`. Eine weitere Möglichkeit ist die Verwendung einer `while`-Schleife:

```
s = 0; k = 0
while k < 101:
    s = s+k
    k += 1
```

Hierin bedeutet `k += 1` einfach `k = k+1`. Die Eingabe `s` ergibt wieder `5050`.

Aufgaben

Aufgabe 3.11 (Noch einmal die Gaußsche Summe)
Betrachten Sie die folgende Tabelle:

	1	2	3	$\cdots$	99	100
+	100	99	98	$\cdots$	2	1
=	101	101	101	101	101	101

(i) Erläutern Sie, wie C.F. Gauß hiermit auf $S_1(100) = 5050$ schloss.

(ii) Schreiben Sie unter SageMath eine `for`-Routine zur Berechnung von $S_1(20)$, $S_1(200)$ und

Aufgabe 3.12 (Noch einmal die Summe der ersten Quadratzahlen)
Wir betrachten erneut den Ausdruck

$$S_2(n) = \sum_{k=1}^{n} k^2 = 1 + 2^2 + 3^2 + \ldots + n^2 \,.$$

(i) Verifizieren Sie zunächst

$$S_2(n) = 1 + (2 + 2) + (3 + 3 + 3) + \ldots + (n + \ldots + n).$$

(ii) Folgern Sie hieraus

$$S_2(n) = \sum_{k=1}^{n} k + \sum_{k=2}^{n} k + \sum_{k=3}^{n} k + \ldots + \sum_{k=n}^{n} k \quad \text{und damit}$$
$$S_2(n) = nS_1(n) - \sum_{k=1}^{n-1} S_1(k)$$

mit dem Summenausdruck $S_1(n) = \sum_{k=1}^{n} k$.

(iii) Schließen Sie nun unter Verwendung der bekannten Darstellungsformel für die Gaußsche Summe $S_1(n)$ auf

$$S_2(n) = \frac{n(2n+1)(n+1)}{6} \,.$$

(iv) Schreiben Sie unter SageMath eine `while`-Routine zur Berechnung von $S_2(10)$, $S_2(100)$ und $S_2(1000)$.

3.4 Das Prinzip der starken Induktion

Neben dem Prinzip der schwachen Induktion gilt das der *starken Induktion.*

Für jedes $k \in \mathbb{N}$ sei eine Aussage A_k derart gegeben, so dass gilt:

A_0 sei richtig und für jedes $n \in \mathbb{N}$ folgt aus der Richtigkeit jeder der Aussagen $A_0, \ldots, A_n$ die Richtigkeit der Aussage A_{n+1}.

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

Oder anders ausgedrückt:

$$A_0 \wedge (\forall n \in \mathbb{N}\colon A_0 \wedge \ldots \wedge A_n \to A_{n+1}) \longrightarrow \forall n \in \mathbb{N}\colon A_n\,.$$

Satz 3.1: Beide Prinzipien sind äquivalent im folgenden Sinne:

1. Kann eine Aussage über die natürlichen Zahlen mit dem Prinzip der schwachen Induktion bewiesen werden, so auch mit dem Prinzip der starken Induktion.
2. Kann eine Aussage über die natürlichen Zahlen mit dem Prinzip der starken Induktion bewiesen werden, so auch mit dem Prinzip der schwachen Induktion.

Beweis. Wir müssen zwei Behauptungen beweisen, die wir jeweils in mehrere aussagenlogische Einzelschritte zerlegen.

1. Angenommen, das Prinzip der starken Induktion ist gültig. Dann müssen wir auch das Prinzip der schwachen Induktion zeigen.

   (i) es gilt A_0 nach Induktionsanfang
   (ii) es gilt $A_n \to A_{n+1}$ für alle $n \in \mathbb{N}$ wegen schwacher Induktionsvoraussetzung
   (iii) es gilt $A_0 \wedge \ldots \wedge A_n \to A_n$ für alle $n \in \mathbb{N}$
   (iv) es gilt $A_0 \wedge \ldots \wedge A_n \to A_{n+1}$ für alle $n \in \mathbb{N}$ nach (ii) und (iii)

2. Angenommen, das Prinzip der schwachen Induktion ist gültig. Dann müssen wir auch das Prinzip der starken Induktion zeigen.

   (i) es gilt A_0
   (ii) Sei $\varphi(n) := \forall_{k \leq n} A_k$.
   (iii) $\varphi(0)$ ist wahr.
   (iv) Es gilt $(A_0 \wedge \cdots \wedge A_n) \to A_{n+1}$ wegen starker Induktionsannahmen.
   (v) $\varphi(n) \to A_{n+1}$ wegen (iii) und (iv).
   (vi) $\varphi(n) \to \forall_{k \leq n+1} A_k$ wegen (ii) und (v).

(vi) $\varphi(n) \to \varphi(n+1)$ wegen (vi).
(vii) $\forall_n \varphi(n)$ wegen (i) und (vi) und schwacher Induktion, also A_k for all $k \in N$.

Damit ist der Satz bewiesen. ∎

Aufgaben

Aufgabe 3.13 (Rekursive Zuordnungsvorschriften I)
Vorgelegt seien natürliche Zahlen $a_0, a_1, a_2, \ldots \in \mathbb{N}$ mit den Eigenschaften

$$a_0 = 1, \quad a_1 = 3, \quad a_n = 2a_{n-1} - a_{n-2} \quad \text{für alle } n = 2, 3, \ldots$$

Beweisen Sie vermittels des Prinzips der starken Induktion, dass gilt

$$a_n = 2n + 1 \quad \text{für alle } n = 0, 1, 2, 3, \ldots$$

Aufgabe 3.14 (Rekursive Zuordnungsvorschriften II)
Vorgelegt seien natürliche Zahlen $a_0, a_1, a_2, \ldots \in \mathbb{N}$ mit den Eigenschaften

$$a_0 = 2, \quad a_1 = 5, \quad a_n = 2a_{n-1} - a_{n-2} \quad \text{für alle } n = 2, 3, \ldots$$

Beweisen Sie vermittels des Prinzips der starken Induktion, dass gilt

$$a_n = 3n + 2 \quad \text{für alle } n = 0, 1, 2, 3, \ldots$$

Aufgabe 3.15 (Rekursive Zuordnungsvorschriften III)
Vorgelegt seien natürliche Zahlen $a_0, a_1, a_2, \ldots \in \mathbb{N}$ mit den Eigenschaften

$$a_0 = 0, \quad a_1 = 1, \quad a_n = 3a_{n-1} - 2a_{n-2} \quad \text{für alle } n = 2, 3, \ldots$$

Beweisen Sie vermittels des Prinzips der starken Induktion, dass gilt

$$a_n = 2^n - 1 \quad \text{für alle } n = 0, 1, 2, 3, \ldots$$

mit den n-fachen Produkt $2^n := 2 \cdot \ldots \cdot 2$.

Aufgabe 3.16 (Summendarstellung natürlicher Zahlen I)
Beweisen Sie vermittels des Prinzips der starken Induktion: Für jede natürliche Zahl $n \in \{8, 9, 10, \ldots\}$ existieren $a, b \in \mathbb{N}$, so dass gilt

$$s = 3a + 5b.$$

Aufgabe 3.17 (Summendarstellung natürlicher Zahlen II)
Beweisen Sie vermittels des Prinzips der starken Induktion: Für jede natürliche Zahl $n \in \{12, 13, 14, \ldots\}$ existieren $a, b \in \mathbb{N}$, so dass gilt

$$s = 4a + 5b.$$

Aufgabe 3.18 Ist A eine Menge der Mächtigkeit $|A| = n$, so zeigen Sie, dass $|\mathcal{P}(A)| = 2^n$.

3.5 Binärdarstellung natürlicher Zahlen

Im alltäglichen Leben schreiben wir natürliche Zahlen in Dezimalschreibweise, d.h. in Potenzen zur Basis 10, wie etwa

$$123 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0 \,.$$

Im heutigen Computerzeitalter ist aber auch die *binäre Schreibweise* von großer Bedeutung. Statt den Ziffern $0, 1, \ldots, 9$ und der Basis 10 benutzen wir dazu die Bits 0 und 1 als Ziffern und die Basis 2, in unserem Beispiel

$$123 = 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 \,,$$

d.h. 123 dezimal, i.Z. 123_{10}, entspricht 1111011 binär, i.Z. 1111011_2.

Satz 3.2: Für jedes $n \in \mathbb{N}_+$ existieren ein eindeutig bestimmtes $k \in \mathbb{N}$ sowie eindeutig bestimmte Bits $a_0, \ldots, a_k \in \{0, 1\}$, so dass

$$n = a_k 2^k + a_{k-1} \cdot 2^{k-1} + \ldots + a_1 \cdot 2^1 + a_0 \cdot 2^0 \quad \text{und} \quad a_k \neq 0.$$

Beweis. Im Fall $n = 1$ wählen wir $k = 0$ und $a_0 = 1$. Die Darstellung $1 = 1 \cdot 2^0$ ist eindeutig. Angenommen, die Behauptung ist für alle $1 \leq m < n$ mit einem $n \geq 2$ richtig. Wir setzen

$$a_0 := \begin{cases} 0, & \text{falls } n \text{ gerade} \\ 1, & \text{falls } n \text{ ungerade} \end{cases} \,, \quad \text{so dass} \quad \frac{n - a_0}{2} \in \mathbb{N}.$$

Nach Voraussetzung existieren genau ein $k \in \mathbb{N}$ und eindeutig bestimmte Bits $b_0, \ldots, b_k \in \{0, 1\}$, wobei $b_k = 1$, mit

$$\frac{n - a_0}{2} = b_k 2^k + b_{k-1} \cdot 2^k + \ldots + b_1 \cdot 2^1 + b_0 \cdot 2^0 \,.$$

Umstellen liefert

$$n = b_k 2^{k+1} + b_{k-1} \cdot 2^k + \ldots + b_0 \cdot 2^1 + a_0 \,.$$

Mit $a_{k+1} := b_k$ folgt die Behauptung. ∎

Bemerkung. In diesem Satz wählen wir genauer

$$k := \max\{m \in \mathbb{N} \,:\, 2^k \leq n\} \,.$$

Unter Vorgriff auf die Eigenschaften der Potenz 2^k zeigt sich, dass die Wahl einer kleineren bzw. einer größeren Potenz $k \in \mathbb{N}$ der gesuchten Binärdarstellung widerspricht.

Beispiel. Wir schreiben $n = 729$ binär. Nach dem Beweis ist $a_0 = 1$, da 729 ungerade ist. Jetzt betrachte $\frac{n-1}{2} = 364$, eine gerade Zahl, also $a_1 = 0$. Fortfahren führt auf $a_2 = 0$, $a_3 = 1$ usw., und wir erhalten die Binärdarstellung

$$729_{10} = 1011\,0110\,01_2\,.$$

Nun schreiben wir umgekehrt $1011\,0110\,01_2$ dezimal. Wir fangen mit dem linken Bit 1 an und schreiben es als erste Ziffer in die obere Zeile. Wir multiplizieren mit 2 und addieren 0, das zweite Bit von links. Wir multiplizieren erneut mit 2 und addieren 1, das dritte Bit von links usw. Die obere Zeile endet so auf 729 :

1	2	5	11	22	45	91	182	354	729
1	0	1	1	0	1	1	0	0	1

Aufgaben

Aufgabe 3.19 Schreiben Sie die nachfolgenden Dezimalzahlen in Binärschreibweise.

a) 16 b) 27 c) 132 d) 2001

Aufgabe 3.20 Schreiben Sie die nachfolgenden Binärzahlen in Dezimalschreibweise.

a) 111 b) 1011 c) 100101 d) 1010011

Aufgabe 3.21 Zur Addition und Multiplikation zweier Binärzahlen gehen Sie vor wie bei der Addition bzw. Multiplikation von Dezimalzahlen, beachten aber

$$0+0=0,\quad 0+1=1,\quad 1+0=1,\quad 1+1=0,$$
$$0\cdot 0=0,\quad 0\cdot 1=0,\quad 1\cdot 0=0,\quad 1\cdot 1=1,$$

Beispiel (beachten Sie den Übertrag beim Addieren)

$$\begin{array}{rrrr} & 1 & 0 & 1 \\ + & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 \end{array} \qquad \begin{array}{rrrrrrr} 1 & 0 & 1 & \cdot & 1 & 1 & 0 \\ \hline & & 1 & 0 & 1 & & \\ & & & 1 & 0 & 1 & \\ & & & & 0 & 0 & 0 \\ \hline & & 1 & 1 & 1 & 1 & 0 \end{array}$$

Berechnen Sie Summe $a + b$ und Produkt $a \cdot b$ der folgenden Binärzahlen.

a) $a = 110$, $b = 101$ b) $a = 110$, $b = 1101$

Verifizieren Sie Ihre Ergebnisse im Dezimalsystem.

Aufgabe 3.22 Benutzen Sie die Binärentwickung natürlichen Zahlen um eine Bijektion $f\colon \{0, 1, 2, \ldots, 2^n - 1\} \to \mathcal{P}(\{0, 1, 2, \ldots, n-1\})$ hinzuschreiben.

3.6 Zahlenumwandlung in SageMath

Die naturliche Zahl $n = 25$ in Dezimaldarstellung lässt sich über

```
n = 25
z = n.binary()
```

in einen String umwandeln, der die Binärdarstellung 11001_2 von 25 kodiert. Dass es sich tatsächlich um einen String handelt, verifizieren wir vermittels `type(z)` mit dem Resultat `'str'`.

Wir wollen eine eigene Routine `binary()` angeben. Dazu benötigen wir neben einigen Stringoperationen folgende Operationen `//` und % zur Division, hier an einem Beispiel:

```
14//5   # gibt den ganzzahligen Anteil nach Division
14%5    # gibt den Rest nach Division
```

Als Resultate bekommen wir `2` und `4`. Die Eingabe

```
(14//5)*5+(14%5)
```

liefert zur Kontrolle natürlich wieder `14`. Nun zur angekündigten Routine:

```
def binary(a):               # definiere Funktion binary
    if a == 0: stri = '0'    # wann besteht String aus 0?
    else: stri = ''          # sonst starte mit leerem String
    while a!=0:              # solange a ungleich Null
      stri = str(a%2)+stri   # ergänze String um Rest
      a = a//2
    return(stri)
```

Beispielsweise liefert die Eingabe

```
binary(25)
```

das Ergebnis den String `'11001'` zurück.

Aufgaben

Aufgabe 3.23 (Binärformbestimmung in SageMath)
Bestimmen Sie mit Hilfe der Funktion `binary()` die Binärdarstellungen als String folgender Dezimalzahlen:

a) 16 b) 27 c) 132 d) 2001

Aufgabe 3.24 (Schreiben einer Funktion zur Dezimalzahlbestimmung)
Schreiben Sie eine SAGEMATH-Routine `dec(a)`, welche aus einem binären String a die zugehörige natürliche Zahl in Dezimaldarstellung berechnet.

Hinweis: Die Länge des Strings a kann durch `len(a)` bestimmt werden. Die einzelnen Einträge von a erhält man vermittels $a[k]$.

Aufgabe 3.25 (Dezimalzahlbestimmung in SageMath)
Unter Benutzung Ihrer Funktion `dec(a)` zur Dezimalzahlbestimmung aus voriger Aufgabe sind folgende Binärzahlen in Dezimalform umzurechnen.

a) 111 b) 1011 c) 100101 d) 1010011

Unter SageMath lassen sich auch leicht Dezimalzahlen in Darstellungen bez. anderer Basen umrechnen. So liefert

```
n = 123
z_3 = n.str(base=3)
z_16 = n.str(base=16)
```

Strings z_2 und z_{16}, die die Dezimalzahl 123 bez. den Basen 3 (Ternärdarstellung), nämlich `'221'`, bzw. $7b$ (Hexadezimaldarstellung), nämlich `'19'`, repräsentieren, denn es ist beispielsweise

$$123_{10} = 11120_3\,, \quad \text{denn} \quad 1\cdot 3^4 + 1\cdot 3^3 + 1\cdot 3^2 + 2\cdot 3^1 + 0\cdot 3^0 = 123.$$

Aufgabe 3.26 (Ternär- und Hexadezimaldarstellungen in SageMath)
Bestimmen Sie unter Verwendung von SageMath die Ternärdarstellungen und die Hexadezimaldarstellungen folgender Dezimalzahlen als Strings:

a) 16 b) 27 c) 132 d) 2001

3.7 Die ganzen Zahlen

Jeder Zahl $n \in \mathbb{N}_+$ ordnen wir genau ein *negatives Element* $-n$ zu und jedem solcher $-n$ eindeutig das ursprüngliche $n \in \mathbb{N}$. Damit stehen die Mengen

$$\mathbb{N}_+ = \{1, 2, 3, 4, \ldots\} \quad \text{und} \quad \mathbb{N}_- := \{\ldots, -4, -3, -2, -1\}$$

in Bijektion zueinander. Als die *Menge der ganzen Zahlen* definieren wir

$$\mathbb{Z} := \mathbb{N}_- \cup \{0\} \cup \mathbb{N}_+ = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

Außerdem vereinbaren wir $-0 := 0$. Wir bezeichnen $\mathbb{N}_+$ als die *positiven,* $\mathbb{N}$ als die *nichtnegativen* und $\mathbb{N}_-$ als die *negativen ganzen Zahlen.*

Addition und Multiplikation ganzer Zahlen

Um eine *Addition* $+_\mathbb{Z} \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ und einer *Multiplikation* $\cdot_\mathbb{Z} \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ zwischen ganzen Zahlen einzuführen, wiederholen wir: Sind $m, n \in \mathbb{N}$ mit $m \geq n$, so existiert genau ein $k \in \mathbb{N}$ mit $m = n + k$, in Zeichen $k = m - n$.

Es seien $m, n \in \mathbb{N}$. Dann definieren $+_\mathbb{Z} \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ vermöge

$$m +_\mathbb{Z} n := m + n, \quad (-m) +_\mathbb{Z} (-n) := -(m + n),$$
$$m +_\mathbb{Z} (-n) := (-n) +_\mathbb{Z} m := \begin{cases} m - n, & \text{falls } m \geq n \\ -(n - m), & \text{falls } n \geq m \end{cases}$$

sowie $\cdot_\mathbb{Z} \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ vermöge

$$m \cdot_\mathbb{Z} n := m \cdot n, \quad (-m) \cdot_\mathbb{Z} (-n) := m \cdot n$$
$$(-m) \cdot_\mathbb{Z} n = -(m \cdot n), \quad m \cdot_\mathbb{Z} (-n) := -(m \cdot n).$$

Es zeigt sich, dass $+_\mathbb{Z}$ und $\cdot_\mathbb{Z}$ kommutativ und assoziativ sind, d.h. es gelten

$$m +_\mathbb{Z} n = n +_\mathbb{Z} m, \quad k +_\mathbb{Z} (m +_\mathbb{Z} n) = (k +_\mathbb{Z} m) +_\mathbb{Z} n$$

für alle $k, m, n \in \mathbb{Z}$, und es ist das Distributivgesetz erfüllt, d.h.

$$k \cdot_\mathbb{Z} (m +_\mathbb{Z} n) = k \cdot_\mathbb{Z} m +_\mathbb{Z} k \cdot_\mathbb{Z} n \quad \text{für alle } k, m, n \in \mathbb{Z}.$$

Insbesondere folgt (ab jetzt schreiben wir einfach $+$ statt $+_\mathbb{Z}$ und $\cdot$ statt $\cdot_\mathbb{Z}$)

$$m + (-m) = 0 \quad \text{für alle } m \in \mathbb{N}.$$

Es heißt $-m$ auch das *additive Inverse* von m. Wegen $0 = m + (-m) = (-m) + m$ für alle $m \in \mathbb{N}$ ist aber ebenso m das additive Inverse von $-m$.

Es besitzt also jedes $z \in \mathbb{Z}$ ein additives Inverses, in Zeichen $-z$, genauer $-m$ im Fall $z = m \in \mathbb{N}$ und $-(-m) = m$ im Fall $z = -m \in \mathbb{N}_-$. Zukünftig schreiben wir daher $a - b$ anstatt $a + (-b)$ und $-a + b$ anstatt $(-a) + b$ für $a, b \in \mathbb{Z}$.

Ordnungsstruktur

Es seien $a, b \in \mathbb{Z}$. Wir schreiben

$$a \leq b \quad \text{genau dann, wenn es ein } k \in \mathbb{N} \text{ gibt mit } a + k = b.$$

Das k hierin ist eindeutig bestimmt. Entsprechend verstehen wir $<$, $\geq$ und $>$. Die Relation $\leq$ ist reflexiv, transitiv, antisymmetrisch und total.

Satz 3.3: Für alle $k, \ell, m, n \in \mathbb{Z}$ gelten

1. Aus $a \leq b$ und $c \leq d$ folgt $a + c \leq b + d$.
2. Aus $a \leq b$ und $0 \leq c$ folgt $a \cdot c \leq b \cdot c$.

Aufgaben

Aufgabe 3.27 (Additives Inverses in $\mathbb{Z}$)
Beweisen Sie $a + (-a) = 0$ für alle $a \in \mathbb{Z}$.

Aufgabe 3.28 (Kürzungsregeln in $\mathbb{Z}$)
Formulieren wie in Abschnitt 3.1 und beweisen Sie die Kürzungsregeln der Addition und Multiplikation in $\mathbb{Z}$.

Aufgabe 3.29 (Neutrales Element der Addition in $\mathbb{Z}$)
Beweisen Sie $a + 0 = a$ für alle $a \in \mathbb{Z}$, und außer 0 gibt es keine weitere ganze Zahl mit dieser Eigenschaft. Wie beweist man $a \cdot 0 = 0$ für alle $a \in \mathbb{Z}$?

Aufgabe 3.30 (Neutrales Element der Multiplikation in $\mathbb{Z}$)
Beweisen Sie $a \cdot 1 = a$ für alle $a \in \mathbb{Z}$, und außer 1 gibt es keine weitere ganze Zahl mit dieser Eigenschaft.

Aufgabe 3.31 (Monotonieeigenschaften der Kleiner-Relation)
Beweisen Sie obenstehenden Satz.

Aufgabe 3.32 (Spezialistenlager Junger Mathematiker 1966, Aufgabe W(9)94)
Es ist zu beweisen, dass die Gleichung $x^3 + px + q = 0$ keine ganzzahligen Lösungen besitzt, wenn p und q ungerade Zahlen sind.

Aufgabe 3.33 (Spezialistenlager Junger Mathematiker 1966, Aufgabe W(10)96)
Bei welchen Werten des Koeffizienten p hat die Gleichung $x^2 - px + 36 = 0$ Lösungen x_1, x_2, die die Bedingung $x_1^2 + x_2^2 = 153$ erfüllen?

3.8 Die rationalen Zahlen

Die natürlichen und die ganzen Zahlen lassen sich auf einer „*Zahlengeraden*“ veranschaulichen. Auf dieser wählen wir einen Ursprung 0 und tragen eine Strecke von 0 bis 1 ab. Äquidistant zu dieser „Längeneinheit“ tragen wir nun die positiven und die negativen ganzen Zahlen wie in der Skizze ab:

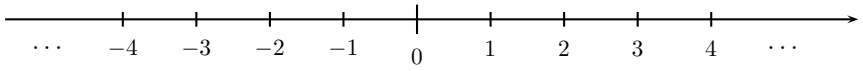


Abbildung 3.1: Zahlengerade zur Veranschaulichung von $\mathbb{Z}$

Wir erhalten Strecken der gemeinsamen Länge 1, die wir nun in $n \in \mathbb{N}_+$ äquidistante Teilstrecken unterteilen. Die neuen *rationalen* Teilungspunkte veranschaulichen die „*Brüche*“ bzw. *rationalen Zahlen*

$$\frac{m}{n} \quad \text{mit Zähler } m \in \mathbb{Z} \text{ und Nenner } n \in \mathbb{Z} \setminus \{0\},$$

zu denen wir auch die natürlichen und ganzen Zahlen mit Nenner $n = 1$ zählen, d.h. wir identifizieren $m \in \mathbb{N}$ bzw. $m \in \mathbb{Z}$ mit $\frac{m}{1}$. Die Menge der rationalen Zahlen bezeichnen wir mit $\mathbb{Q}$.

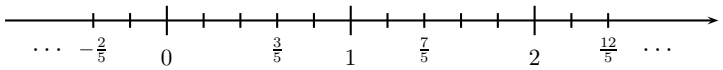


Abbildung 3.2: Zahlengerade zur Veranschaulichung von Brüchen

Zwei Brüche $\frac{k}{\ell}$ und $\frac{m}{n}$ betrachten wir als gleich, wenn $kn = \ell m$. Der Nenner darf also stets positiv gewählt werden. Im Fall $m, n \in \mathbb{N}_+$ heißt $\frac{m}{n}$ *positiv,* im Fall $m \in \mathbb{N}_-$, $n \in \mathbb{N}_+$ *negativ.* Sind $m \in \mathbb{N}$, $n \in \mathbb{N}_+$, so schreiben wir $\frac{m}{n} \geq 0$, entsprechend $\frac{m}{n} \leq 0$ usw. Schließlich vereinbaren wir $-\frac{m}{n} := \frac{-m}{n}$.

Addition und Multiplikation rationaler Zahlen

Es seien $k, \ell \in \mathbb{Z}$ und $m, n \in \mathbb{Z} \setminus \{0\}$. Dann definieren wir die Addition $+_{\mathbb{Q}} \colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ und die Multiplikation $\cdot_{\mathbb{Q}} \colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ vermöge

$$\frac{k}{\ell} +_{\mathbb{Q}} \frac{m}{n} = \frac{k \cdot n + \ell \cdot m}{\ell \cdot n}, \quad \frac{k}{\ell} \cdot_{\mathbb{Q}} \frac{m}{n} = \frac{k \cdot m}{\ell \cdot n}.$$

Es zeigt sich, dass $+_{\mathbb{Q}}$ und $\cdot_{\mathbb{Q}}$ kommutativ und assoziativ sind, und es gilt das Distributivgesetz. Ferner gelten, wie bereits für natürliche und ganze Zahlen formuliert, die Kürzungsregeln für die Addition und Multiplikation.

Zukünftig schreiben wir wieder $+$ statt $+_{\mathbb{Q}}$ und $\cdot$ statt $\cdot_{\mathbb{Q}}$.

Ordnungsstruktur

Es seien $p, q \in \mathbb{Q}$. Dann schreiben wir

$$p \leq q \quad \text{genau dann, es ein rationales } r \geq 0 \text{ gibt mit } p + r = q.$$

Das r hierin ist eindeutig bestimmt. Entsprechend verstehen wir $<, \geq, >$. Die Relation $\leq$ ist reflexiv, transitiv, antisymmetrisch und total. Sind insbesondere $k, \ell, m, n \in \mathbb{N}_+$, so folgt

$$\frac{k}{\ell} \leq \frac{m}{n} \quad \text{genau dann, wenn} \quad kn \leq \ell m.$$

Aufgabe

Aufgabe 3.34 (Positive Nenner)
Warum dürfen wir uns stets auf Brüche $\frac{m}{n}$ mit positivem Nenner $n > 0$ beschränken?

Aufgabe 3.35 (Eigenschaften der Addition und Multiplikation)
Beweisen Sie, dass die Addition $+_{\mathbb{Q}}$ und die Multiplikation $\cdot_{\mathbb{Q}}$ kommutativ und assoziativ sind, und dass das Distributivgesetz erfüllt ist.

Aufgabe 3.36 (Kürzungsregel der Division)
Beweisen Sie die Kürzungsregel

$$\frac{p \cdot r}{q \cdot r} = \frac{p}{q} \quad \text{für alle } p, q, r \in \mathbb{Z} \text{ mit } q, r \neq 0.$$

Aufgabe 3.37 (Eigenschaften der Kleiner-Relation)
Beweisen Sie, dass $\leq$ reflexiv, transitiv, antisymmetrisch und total ist.

Aufgabe 3.38 (Kleiner-Relation für Brüche)
Beweisen Sie: Sind $k, \ell, n, n \in \mathbb{N}_+$, so gilt

$$\frac{k}{\ell} \leq \frac{m}{n} \quad \text{genau dann, wenn } kn \leq \ell m.$$

Aufgabe 3.39 (Größer oder kleiner?)
Welche der folgenden Zahlen ist größer, welche ist kleiner?

a) $\frac{5}{8}$ und $\frac{4}{9}$ b) $\frac{3}{8}$ und $\frac{5}{6}$

c) $-\frac{1}{4}$ und $\frac{3}{25}$ d) $-\frac{10}{123}$ und $-\frac{312}{2513}$

3.9 $\mathbb{Q}$ als angeordneter Körper

Wir wollen die Menge der rationalen Zahlen in einen allgemeineren algebraischen Kontext stellen.

Eine Menge $\mathbb{K}$ heißt ein *Körper,* falls für alle Elemente $x, y \in \mathbb{K}$ eine Summe $x+y \in \mathbb{K}$ und ein Produkt $x \cdot y \in \mathbb{K}$ erklärt sind, so dass folgende *Körperaxiome* erfüllt sind:

(K1) *Axiome der Addition*

1. Die Addition ist kommutativ und assoziativ.
2. Es existiert ein $0 \in \mathbb{K}$ mit $x + 0 = x$ für alle $x \in \mathbb{K}$.
3. Zu jedem $x \in \mathbb{K}$ existiert ein $-x \in \mathbb{K}$ mit $x + (-x) = 0$.

(K2) *Axiome der Multiplikation*

1. Die Multiplikation ist kommutativ und assoziativ.
2. Es existiert ein $1 \in \mathbb{K}$ mit $x \cdot 1 = x$ für alle $x \in \mathbb{K}$.
3. Zu jedem $x \in \mathbb{K} \setminus \{0\}$ existiert ein $x^{-1} \in \mathbb{K}$ mit $x \cdot x^{-1} = 1$.

(K3) Es gilt das *Distributivgesetz.*

Die Menge $\mathbb{Q}$ mit der obigen Addition $+_{\mathbb{Q}}$ und Multiplikation $\cdot_{\mathbb{Q}}$ ist ein Körper. Das neutrale Element der Addition ist dabei die Zahl $0 \in \mathbb{N}$, das neutrale Element der Multiplikation die $1 \in \mathbb{N}_0$. Zu $\frac{m}{n} \in \mathbb{Q}$ ist ferner $\frac{-m}{n}$ additiv invers, zu $\frac{n}{m}$ mit $m \neq 0$ ist $\frac{n}{m}$ multiplikativ invers. Das erlaubt es uns auch, Brüche auf alle rationalen Zahlen zu erweitern:

$$\frac{\frac{k}{\ell}}{\frac{m}{n}} := \frac{k}{\ell} \cdot \left(\frac{n}{m}\right)^{-1} = \frac{k}{\ell} \cdot \frac{n}{m}, \quad k, m \in \mathbb{Z},\ \ell, n \in \mathbb{Z} \setminus \{0\}.$$

Ein Körper $\mathbb{K}$ heißt *angeordnet,* wenn mit einer Relationen $>$ folgende *Anordnungsaxiome* erfüllt sind:

(A1) Für jedes $x \in \mathbb{K}$ gilt genau eine der drei Bedingungen $x = 0$, $x > 0$ oder $-x > 0$.

(A2) Für alle $x \in \mathbb{K}$ mit $x > 0$ und $y > 0$ gelten $x + y > 0$ und $x \cdot y > 0$.

Es heißt $\mathbb{K}$ *archimedisch angeordnet,* wenn zu je zwei Elementen $x, y \in \mathbb{K}$ mit $0 < x < y$ stets ein $n \in \mathbb{N}_+$ existiert mit $y < n \cdot x$.

Mit der im vorigen Abschnitt eingeführten Relation $>$ ist $\mathbb{Q}$ ein archimedisch angeordneter Körper.

Aufgaben

Aufgabe 3.40 (Auflösungsaufgaben aus dem Papyrus Rhind I)
In den Aufgaben 21 bis 23 und 30 bis 34 des Papyrus Rhind ist jeweils - hier in moderner Notation - die Unbekannte x gesucht:

a) $\frac{2}{3}+\frac{1}{5}+x=1$ b) $\frac{2}{3}+\frac{1}{30}+x=1$

c) $\frac{1}{4}+\frac{1}{8}+\frac{1}{10}+\frac{1}{30}+\frac{1}{45}+x=\frac{2}{3}$ d) $\frac{2x}{3}+\frac{x}{10}=10$

Unter SageMath lassen sich diese Gleichungen wie folgt auflösen:

```
var = ('x')
eq = 2/3+1/5+x-1
solve([eq],x)
```

Aufgabe 3.41 (Auflösungsaufgaben unter SageMath)
Lösen Sie die Gleichungen aus Aufgabe 3.9.1 unter Verwendung von SageMath.

Aufgabe 3.42 (Eine weitere Aufgabe mit vollständiger Induktion)
Es sei $n \in \mathbb{N}_+$. Beweisen Sie vermittels vollständiger Induktion

$$\sum_{k=1}^{n} \frac{k}{2^k} = 2 - \frac{n+2}{2} \quad \text{mit} \quad 2^k := 2 \cdot 2 \cdot \ldots \cdot 2.$$

Aufgabe 3.43 (Verallgemeinerung der vorigen Aufgabe)
Es sei $n \in \mathbb{N}$. Wir setzen $S := \sum_{k=1}^{n} \frac{k^2}{2^k}$. Verifizieren Sie

$$2S = 1 - \frac{(n+1)^2}{2^n} + \sum_{k=1}^{n} \frac{(k+1)^2}{2^k},$$

und ermitteln Sie daraus einen expliziten Ausdruck für S.

Aufgabe 3.44 (Zum Nachweis der Anordnung)
Es seien $p, q \in \mathbb{Q}$ mit $p > 0$ und $q > 0$. Beweisen Sie $p + q > 0$ und $p \cdot q > 0$.

Aufgabe 3.45 ($\mathbb{Q}$ ist archimedisch angeordnet)
Beweisen Sie die folgenden Aussagen:

(i) Für jedes $p \in \mathbb{Q}$ existiert ein $n \in \mathbb{N}$ mit $p < n$.
(ii) Für jedes positive $p \in \mathbb{Q}$ existiert ein $n \in \mathbb{N}$ mit $n^{-1} < p$.
(iii) Für alle $p, q \in \mathbb{Q}$ mit $0 < p < q$ existiert ein $n \in \mathbb{N}$ mit $q < np$.

3.10 Abzählbarkeit der rationalen Zahlen

Wir schließen an unsere Diskussion über die Mächtigkeit von Mengen an.

Eine Menge M heißt *abzählbar unendlich,* falls sie gleichmächtig zur Menge $\mathbb{N}$ der natürlichen Zahlen ist, d.h. falls eine bjektive Abbildung $f\colon \mathbb{N} \to M$ existiert.

Eine solche Abzählung f heißt auch eine *Abzählung von* M. Insbesondere gilt

$$M = \{f(0), f(1), f(2), f(3), \ldots\}\,.$$

Satz 3.4: Die Menge $\mathbb{N} \times \mathbb{N}$ ist abzählbar unendlich.

Beweis. Wir geben nur eine Beweisidee und veranschaulichen eine mögliche Bijektion zwischen $\mathbb{N}$ und $\mathbb{N} \times \mathbb{N}$ durch folgendes Schema: Links ist die Menge $\mathbb{N} \times \mathbb{N}$ skizziert,

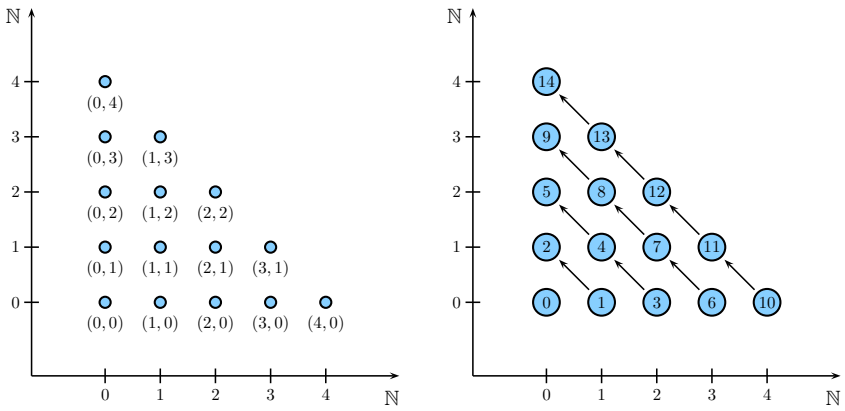


Abbildung 3.3: Abzählbarkeit der Menge $\mathbb{N} \times \mathbb{N}$

rechts eine mögliche Abzählung, beginnend bei $f(0) = (0,0) \in \mathbb{N} \times \mathbb{N}$ und fortfahrend mit

$$f(1) = (1,0), \quad f(2) = (0,1), \quad f(3) = (2,0) \quad \text{usw.}$$

Das veranschaulicht die Behauptung. ∎

Das hier verwendete Schema heißt *erstes Cantorsches Diagonalverfahren.* Im nächsten Abschnitt genauer wir hierauf genauer ein.

Hilfssatz 3.1: Es seien M eine nicht endliche Menge und $\sigma\colon \mathbb{N} \to M$ eine surjektive Abbildung. Dann ist M abzählbar unendlich.

Beweis. Es ist M nicht endlich. Wir konstruieren damit ein $f\colon \mathbb{N} \to M$ vermöge

$$\begin{aligned} &f(0) := \sigma(0), \\ &f(1) := \sigma(k_1) \text{ mit } k_1 > 0 \text{ minimal mit } \sigma(k_1) \neq f(0), \\ &f(2) := \sigma(k_2) \text{ mit } k_2 > 0 \text{ minimal mit } \sigma(k_2) \notin \{f(0), f(1)\} \quad \text{usw.} \end{aligned}$$

bzw. allgemein

$$f(n) := \sigma(k_n) \text{ mit } k_n > k_{n-1} \text{ minimal mit } \sigma(k_n) \notin \{f(0), \ldots, f(n-1)\}\,.$$

Als Übung zeige man, dass diese Abbildung bijektiv ist. ∎

Satz 3.5: Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar unendlich.

Beweis. Definiere zunächst eine Surjektion $g\colon \mathbb{N} \times \mathbb{N} \to \mathbb{Q}$ folgendermaßen:

(i) $g(m,0) = g(0,m) := 0$ für alle $m \in \mathbb{N}$,

(ii) $g(2m-1, n) := \frac{m}{n}$ für alle $m, n \in \mathbb{N}_+$,

(iii) $g(2m, n) := -\frac{m}{n}$ für alle $m, n \in \mathbb{N} +$.

Ist nun $f\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ eine Abzählung von $\mathbb{N} \times \mathbb{N}$, so stellt $\sigma := g \circ f\colon \mathbb{N} \to \mathbb{Q}$ wieder eine Surjektion dar. Die Aussage folgt aus vorigem Hilfssatz. ∎

Aufgaben

Aufgabe 3.46 (Kreuzprodukte abzählbarer Mengen sind abzählbar)
Es seien A und B zwei abzählbar unendliche Mengen. Beweisen Sie, dass das Mengenprodukt $A \times B$ abzählbar unendlich ist.

Aufgabe 3.47 (Zum Beweis des Hilfssatzes)
Beweisen Sie, dass die Abbildung f aus diesem Beweis tatsächlich bijektiv ist.

Aufgabe 3.48 (Zum Beweis der Abzählbarkeit von $\mathbb{Q}$)
Beweisen Sie, dass die Abbildung σ aus dem Beweis tatsächlich surjektiv ist.

3.11 Weiteres zur Abzählbarkeit

Das Abzählungsschema im rechten Bild 3.3 lässt sich als geschlossene Formel schreiben. Zu diesem Zweck wertet man sukzessive die einzelnen Spalten des Schemas aus. Die resultierende Abbildung

$$\pi\colon \mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{N},\quad (m,n)\mapsto\pi(m,n):=n+\sum_{k=0}^{m+n}k,$$

heißt *Cantorsche Paarungsfunktion.* Zur Ermittlung der Inversen $r=\pi^{-1}(m,n)$ dieser Abbildung setzen wir

$$f(r):=\max\{\ell\in\mathbb{N}\,:\,S_1(\ell)\le r\}$$

mit der Gaußschen Summe $S_1(r)=\frac{1}{2}r(r+1)$ und erhalten:

$$n(r)=r-S_1(f(r)),\quad m(r)=f(r)-n(r).$$

Beispiel. Es sind

$$\pi(1,2)=2+\sum_{k=0}^{1+2}k=2+\sum_{k=0}^{3}k=2+6=8$$

und umgekehrt $f(8)=3$,$n(8)=8-S_1(3)=8-6=2$, $m(8)=3-2=1$.

Historisches

Die Abzählbarkeit der Menge der rationalen Zahlen wurde ursprünglich von Cantor [**?**] im Jahre 1873 bewiesen, siehe auch Dauben [**?**] für eine historische Einordnung. Seine Beschreibung einer Bijektion zwischen $\mathbb{N}$ und $\mathbb{Q}$ führt auf ein Schema, ähnlich dem hier abgebildeten. Brüche, die auf Grund der Kürzungsregel bereits durchlaufen wurden, werden dabei ausgelassen. Führen Sie das Schema weiter!

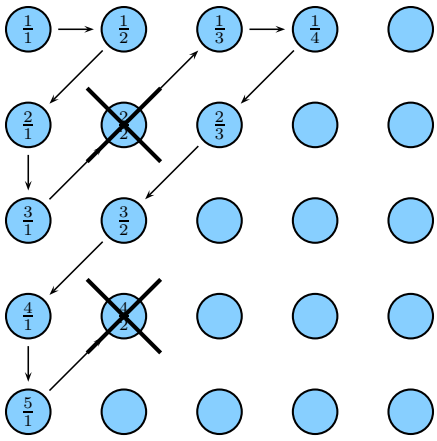


Abbildung 3.4: Zur Abzählung von $\mathbb{Q}$

Aufgaben

Aufgabe 3.49 (Cantorsche Paarungsfunktion und SageMath)
Schreiben Sie eine SageMath-Funktion `cantor(m,n)` zur Auswertung der Cantorsche Paarungsfunktion $\pi(m, n)$.

Aufgabe 3.50 (Zur Inversen der Cantorschen Paarungsfunktion)
Berechnen Sie $\pi^{-1}(k)$ für $k = 0, 1, 2, 3, 4, 5$.

Aufgabe 3.51 (Die Inverse der Paarungsfunktion und SageMath)
Schreiben Sie eine SageMath-Funktion `cantinv(r)` zur Berechnung der Werte $\pi^{-1}(r)$. Verifizieren Sie Ihre Ergebnisse aus der vorigen Aufgabe.

Aufgabe 3.52 (Beispiele abzählbarer Teilmengen)
Beweisen Sie, dass folgende Mengen M abzählbar unendlich sind.

(i) $M = \{n \in \mathbb{N} : \text{es gibt ein } k \in \mathbb{N} \text{ mit } n = 2k\}$
(ii) $M = \{0, 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, \ldots\}$

Aufgabe 3.53 (Abzählbarkeit der Menge der ganzen Zahlen)
Beweisen Sie durch ein geeignetes Schema, dass die Menge $\mathbb{Z}$ der ganzen Zahlen abzählbar unendlich ist.

Aufgabe 3.54 (Eigenes Schema zur Abzählung der rationalen Zahlen)
Fertigen Sie ein eigenes Schema an, um die Abzählung der Menge $\mathbb{Q}$ der rationalen zu veranschaulichen.

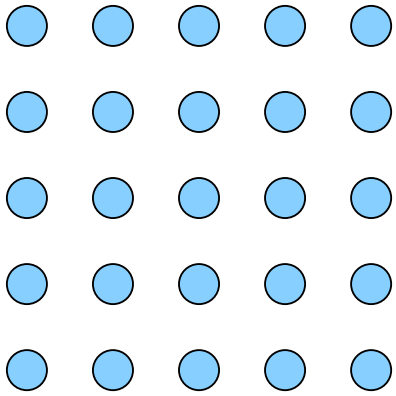


Abbildung 3.5: Eigenes Schema zur Abzählung von $\mathbb{Q}$

Kapitel 4

Kombinatorik

4.1 Binomialkoeffizienten

Ist A eine endliche Menge, so definieren wir

$$\binom{A}{k} := \{B \subset A : |B| = k\}$$

als die Menge aller Teilmengen von A mit $k \in \mathbb{N}$ Elementen. Ist insbesondere $|A| = n \in \mathbb{N}$, so setzen wir

$$\binom{n}{k} := \left|\binom{A}{k}\right|.$$

Die Größe $\binom{n}{k}$ mit $k, n \in \mathbb{N}$ heißt *Binomialkoeffizient.*

Die Menge $\binom{A}{k}$ beschreibt also alle Möglichkeiten, aus einer Menge A mit n Elementen k Elemente (ohne Zurücklegen, ohne Wiederholung) auszuwählen.

Satz 4.1: Es seien $k, n \in \mathbb{N}$. Dann gelten die nachfolgenden Identitäten.

a) $\binom{n}{0} = 1 = \binom{n}{n}$ b) $\binom{n}{k} = \binom{n}{n-k}$ für $k \leq n$

c) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ für $n \geq 2$ und $1 \leq k \leq n-1$

Beweis.

1. Es sei A eine endliche Menge mit $|A| = n$. Dann gelten $\binom{A}{0} = \{\emptyset\}$ sowie $\binom{A}{n} = \{A\}$ und daher $\binom{n}{0} = \binom{n}{n} = 1$.

2. Es sei A eine endliche Grundmenge mit $|A| = n$, siehe Abschnitt 2.2. Jeder Teilmenge $B \subset A$ mit $B \in \binom{A}{k}$ ordnen wir ihr Komplement $B^c \subset A$ mit

$$B \cup B^c = A \quad \text{und} \quad B \in \binom{A}{n-k}$$

zu. Diese Zuordnung ist wegen $(B^c)^c = B$ umkehrbar und eineindeutig, d.h. bijektiv, so dass die zweite Behauptung folgt.

3. Es sei A eine nichtleere Menge mit $|A| = n \geq 2$. Zu einem $a \in A$ betrachten wir die Abbildung

$$f\colon \binom{A}{k} \longrightarrow \binom{A \setminus \{a\}}{k} \cup \binom{A \setminus \{a\}}{k-1}, \quad 1 \leq k \leq n-1,$$

$$\text{vermöge} \quad f(B) := \begin{cases} B, & \text{falls } a \notin B \\ B \setminus \{a\}, & \text{falls } a \in B \end{cases}.$$

Diese Abbildung ist bijektiv mit der Umkehrabbildung

$$f^{-1}(B) = \begin{cases} B, & \text{falls } |B| = k \\ B \cup \{a\}, & \text{falls } |B| = k-1 \end{cases},$$

und wegen $\binom{A \setminus \{a\}}{k} \cap \binom{A \setminus \{a\}}{k-1} = \emptyset$ folgt

$$\left|\binom{A}{k}\right| = \left|\binom{A \setminus \{a\}}{k} \cup \binom{A \setminus \{a\}}{k-1}\right| = \left|\binom{A \setminus \{a\}}{k}\right| + \left|\binom{A \setminus \{a\}}{k-1}\right|.$$

Mit $|A \setminus \{a\}| = n-1$ ist auch die dritte Behauptung gezeigt.

Damit ist der Satz bewiesen. ∎

Unter SageMath lässt sich der Binomialkoeffizient $\binom{n}{k}$ wie folgt ermitteln:

```
binomial(n,k)
```

So liefert `binomial(120,7)` das Resultat `59487568920`.

Aufgabe

Aufgabe 4.1 (Bestimmen k-elementiger Teilmengen)
Es sei $A = \{a, b, c, d\}$. Bestimmen Sie die Mengen

$$\binom{A}{0}, \quad \binom{A}{1}, \quad \binom{A}{2}, \quad \binom{A}{3}, \quad \binom{A}{4}.$$

Aufgabe 4.2 (Beispiele zum Satz)
Verifizieren Sie anhand selbst gewählter Beispiele

(i) die zweite Aussage des Satzes,
(ii) die dritte Aussage des Satzes.

4.2 Die Fakultät

Eng verknüpft mit dem Begriff des Binomialkoeffizienten ist der der Fakultät.

Die *Fakultät* einer natürlichen Zahl $n \in \mathbb{N}$ ist definiert als

$$0! := 1, \quad n! := 1 \cdot 2 \cdot \ldots \cdot n \text{ für } n \geq 1.$$

Wir können auch *rekursiv* schreiben

$$n! = \begin{cases} 1, & \text{falls } n = 0 \\ n \cdot (n-1)!, & \text{falls } n \geq 1 \end{cases} .$$

Satz 4.2: Es seien $k, n \in \mathbb{N}$ mit $k \leq n$. Dann gilt

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} .$$

Beweis. Die Aussage ist richtig für $n = 0$ und $n = 1$. Sie sei nun ebenfalls richtig für ein $n - 1 \in \mathbb{N}$, genauer

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

Nun berechnen wir

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

Unter Beachtung der dritten Aussage des Satzes aus dem vorigen Abschnitt 4.1 folgt die Behauptung nach dem Prinzip der vollständigen Induktion. ∎

Diese hier zitierte dritte Aussage des Satzes 4.1 veranschaulichen wir anhand des folgenden *Pascalschen Dreiecks:*

$$\begin{array}{ccccccc} & & & \binom{0}{0} & & & \\ & & \binom{1}{0} & & \binom{1}{1} & & \\ & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\ \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \end{array} \quad \text{usw.}$$

Können Sie den Aufbau dieses Dreiecks im Detail erklären?

Aufgaben

Aufgabe 4.3 *(Berechnen von Fakultäten I)*
Berechnen Sie die folgenden Ausdrücke:

a) $\dfrac{3!}{1!}$ b) $\dfrac{4!}{2!}$ c) $\dfrac{2! \cdot 5!}{3!}$ d) $\dfrac{4! \cdot 7!}{2!}$ e) $\dfrac{5! \cdot 9!}{4!}$

Aufgabe 4.4 *(Berechnen von Fakultäten II)*
Berechnen Sie die folgenden Ausdrücke:

a) $\dfrac{173!}{171!}$ b) $\dfrac{429!}{426!}$ c) $\dfrac{1002!}{998!}$

Aufgabe 4.5 (Fakultät und Binomialkoeffizient in SageMath)
Schreiben Sie SageMath-Funktionen `facul(n)` und `binom(n,k)` zur Berechnung von $n!$ sowie $\binom{n}{k}$.

Aufgabe 4.6 (Die Fakultät als untere und obere Grenze)
Beweisen Sie, dass für jede natürliche Zahl $n \in \mathbb{N}_+$ ein $k \in \mathbb{N}$ existiert mit

$$k! \leq n \leq (k+1)!\,.$$

Aufgabe 4.7 (Noch einmal zum Binomialkoeffizienten)
Beweisen Sie, dass für alle $k, n \in \mathbb{N}$ mit $k \leq n$ gilt

$$\binom{n+1}{k+1} = \frac{n+1}{k+1} \cdot \binom{n}{k}.$$

Aufgabe 4.8 (Summen über Binomialkoeffizienten I)
Beweisen Sie vermittels vollständiger Induktion die folgenden Identitäten:

a) $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = 2^n$ für $n \in \mathbb{N}$ b) $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$ für $n \in \mathbb{N}_+$

Aufgabe 4.9 (Summen über Binomialkoeffizienten II)
Beweisen Sie ohne Induktion, dass für alle $k, n \in \mathbb{N}$ mit $k \leq n$ folgende Identitäten richtig sind:

a) $\displaystyle\sum_{k=0}^{n} k \binom{n}{k} = n \cdot 2^{n-1}$ b) $\displaystyle\sum_{k=0}^{n} k^2 \binom{n}{k} = n \binom{2n-1}{n-1}$

c) $\displaystyle\sum_{k=0}^{n} \frac{1}{k+1} \binom{n}{k} = \frac{2^{n+1}-1}{n+1}$

4.3 Multinomialkoeffizienten

Unser nächstes Resultat ist der folgende *binomische Lehrsatz.*

Satz 4.3: Sind a, b Zahlen und $n \in \mathbb{N}$, so gilt

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \,.$$

Beweis. Als Übung beweisen wir diese Identität vermittels vollständiger Induktion. An dieser Stelle wollen wir stattdessen folgendes Argument als Beweisidee anführen: Man mache sich klar, dass beim Ausklammern des Produktes

$$\underbrace{(a+b)\cdot(a+b)\cdot\ldots\cdot(a+b)}_{n}$$

nur Terme der Form $a^{n-k}b^k$ vorkommen. Wir erhalten einen solchen Term, wenn wir das k-fache Produkt von b aus den n Faktoren $a+b$ auswählen, und dafür gibt es genau $\binom{n}{k}$ Möglichkeiten. ∎

Allgemeiner suchen wir nun eine Darstellung für Produkte der Form

$$(x_1 + \ldots + x_k)^n \,.$$

Dazu benötigen wir die Multinomialkoeffizienten.

Ist $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{N}^k$ mit $|\alpha| := \alpha_1 + \ldots + \alpha_k = n$, so definieren wir den *Multinomialkoeffizienten* $\binom{n}{\alpha}$ durch

$$\binom{n}{\alpha} := \binom{n}{\alpha_1, \ldots, \alpha_k} := \frac{n!}{\alpha_1! \cdot \ldots \cdot \alpha_k!}$$

Die Interpretation von $\binom{n}{\alpha}$ ist Folgende: Wir haben $\binom{n}{\alpha_1}$ Möglichkeiten, aus einer Menge A mit $|A| = n$ eine Menge A_1 mit $|A_1| = \alpha_1$ auszuwählen. Dann wählen wir aus $A \setminus A_1$ mit $|A \setminus A_1| = n - \alpha_1$ eine Menge A_2 mit $|A_2| = \alpha_2$ aus und haben dazu $\binom{n-\alpha_1}{\alpha_2}$ Möglichkeiten usw. Wegen $n = \alpha_1 + \ldots + \alpha_k$ ist

$$\begin{aligned}
&\binom{n}{\alpha_1} \cdot \binom{n-\alpha_1}{\alpha_2} \cdot \ldots \cdot \binom{n-\alpha_1-\ldots-\alpha_{k-1}}{\alpha_k} \\
&= \frac{n!}{\alpha_1!(n-\alpha_1)!} \cdot \frac{(n-\alpha_1)!}{\alpha_2!(n-\alpha_1-\alpha_2)!} \cdot \ldots \cdot \frac{n-\alpha_1-\ldots-\alpha_{k-1}}{\alpha_k!(n-\alpha_1-\ldots-\alpha_k)!} \\
&= \frac{n!}{\alpha_1! \cdot \ldots \cdot \alpha_k! \cdot (n-\alpha_1-\ldots-\alpha_k)!} = \frac{n!}{\alpha_1! \cdot \ldots \cdot \alpha_k!} = \binom{n}{\alpha} .
\end{aligned}$$

Es gibt also $\binom{n}{\alpha}$ die Zahl der Möglichkeiten an, aus einer Menge A mit $|A| = n$ Teilmengen $A_1, \ldots, A_k$ auszuwählen mit $|A_j| = \alpha_j$, wobei $\alpha_1 + \ldots + \alpha_k = n$.

Unsere Überlegungen zur Ableitung der binomischen Formel führen uns also auf analog Weise zu folgender *Multinomialformel.*

Satz 4.4: Sind $x_1, \ldots, x_k \in \mathbb{R}$ reelle Zahlen und $n \in \mathbb{N}$, so gilt

$$(x_1 + \ldots + x_k)^n = \sum_{\alpha \in \mathbb{N}^k :\, |\alpha| = n} \binom{n}{\alpha} x_1^{\alpha_1} \cdot \ldots \cdot x_k^{\alpha_k}$$

Aufgaben

Aufgabe 4.10 (Binomische Formeln)
Schreiben Sie explizit unter Verwendung der Binomialformel:

a) $(a+b)^2$ b) $(a+b)^3$
c) $(a+b)^4$ d) $(a+b)^5$

Aufgabe 4.11 (Multinomiale Formeln)

1. Schreiben Sie explizit unter Verwendung der Multinomialformel:

   a) $(a+b+c)^2$ b) $(a+b+c)^3$
   c) $(a+b+c+d)^2$ d) $(a+b+c+d)^3$

2. Berechnen Sie die Koeffizienten von a^3bc^4 und a^5b^2c in $(a+b+c)^8$.

Aufgabe 4.12 (Anwendung der Multinomialformel)
Wieviel Möglichkeiten gibt es, aus einer Menge mit 7 Elementen

(i) 2 Teilmengen der Mächtigkeiten 2 und 5
(ii) 3 Teilmengen der Mächtigkeit 2, 2 und 3

auszuwählen?

Aufgabe 4.13 (Multinomialformel und binomische Formel)
Leiten Sie aus der Multinomialformel die binomische Formel ab.

Aufgabe 4.14 (Beweis des binomischen Lehrsatzes)
Beweisen Sie den binomischen Lehrsatz vermittels vollständiger Induktion.

4.4 Das Inklusions-Exklusions-Prinzip

Sind A und B zwei endliche Mengen, so ist

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

und für drei endliche Mengen A, B und C überzeugt man sich von

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

Allgemeiner gilt nun das folgende *Inklusions-Exklusions-Prinzip.*

Satz 4.5: Es sei $I = \{1, 2, \ldots, n\}$ eine endliche Indexmenge. Ferner seien A_i mit $i \in I$ endliche Mengen. Wir setzen

$$A := \bigcup_{i \in I} A_i \quad \text{und} \quad A_J := \bigcap_{i \in J} A_i$$

für eine Teilmenge $J \subset I$. Dann gilt

$$|A| = \sum_{i=1}^{|I|} \sum_{J \subset I\,:\,|J|=i} (-1)^{i+1} |A_J|.$$

Beweis. Es sei ein $a \in A$ fest gewählt. Es gibt genau $1 \leq t \leq n$ Mengen A_i mit $a \in A_i$, wobei t natürlich von a abhängt. Dann gibt es aber auch genau $\binom{t}{i}$ Durchschnitte A_J mit $a \in A_J$ und $|J| = i$, genauer

$$\big|\{J \subset I \,:\, a \in A_J \text{ und } |J| = i\}\big| = \binom{t}{i} \quad \text{bzw.} \quad \sum_{J \subset I\,:\,|J|=i} \chi_{A_J}(a) = \binom{t}{i}$$

mit der *charakteristischen Funktion*

$$\chi_{A_J}(a) := \begin{cases} 1, & a \in A_J \\ 0, & a \notin A_J \end{cases} .$$

Es folgt

$$\begin{aligned} \sum_{i=1}^{|I|} \sum_{J \subset I\,:\,|J|=i} (-1)^{i+1} \chi_{A_J}(a) \;&=\; \sum_{i=1}^{|I|} (-1)^{i+1} \sum_{J \subset I\,:\,|J|=i} \chi_{A_J}(a) \\ &= \binom{t}{1} - \binom{t}{2} + \ldots + (-1)^{t+1} \binom{t}{t} \\ &= 1 - \left\{ 1 - t + \binom{t}{2} - \ldots + (-1)^t \binom{t}{t} \right\} \\ &= 1 - \left\{ 1 + \sum_{k=1}^{t} (-1)^k \binom{t}{k} \right\} \;=\; 1 - \left\{ 1 + \sum_{k=0}^{t} (-1)^k \binom{t}{k} - 1 \right\}. \end{aligned}$$

Zusammen mit Aufgabe 4.8, Teil (ii) gelangen wir zu

$$\sum_{i=1}^{|I|} \sum_{J \subset I\,:\,|J|=i} (-1)^{i+1} \chi_{A_J}(a) = 1 - (1-1) = 1.$$

Wir erhalten (beachte das Vertauschen der endlichen Summen):

$$\begin{aligned} |A| &= \sum_{a \in A} 1 = \sum_{a \in A} \left\{ \sum_{i=1}^{|I|} (-1)^{i+1} \sum_{J \subset I\,:\,|J|=i} \chi_{A_J}(a) \right\} \\ &= \sum_{i=1}^{|I|} \sum_{J \subset I\,:\,|J|=i} (-1)^{i+1} \sum_{a \in A} \chi_{A_J}(a) = \sum_{i=1}^{|I|} \sum_{J \subset I\,:\,|J|=i} (-1)^{i+1} |A_J|. \end{aligned}$$

Das zeigt die Behauptung. ∎

Aufgaben

Aufgabe 4.15 (Spezialfälle des Inklusions-Exklusions-Prinzip)
Leiten Sie aus dem Inklusions-Exklusions-Prinzip obige Darstellungen für $|A \cup B|$ und $|A \cup B \cup C|$ ab.

Aufgabe 4.16 (Anwendung des Inklusions-Exklusions-Prinzips)
Es seien A, B, C und D endliche Mengen.

(i) Leiten Sie aus dem Inklusions-Exklusions-Prinzip eine Darstellung für die Zahl $|A \cup B \cup C \cup D|$ ab.
(ii) Die vier Mengen seien nun paarweise disjunkt. Was können Sie folgern?
(iii) Es seien nun $A = \{1, 2, \ldots, 10\}$, $B = \{2, 4, 7, 8, 9\}$, $C = \{1, 5, 6, 8, 9, 10\}$ und $D = \{2, 4, 6, 8, 10\}$. Bestimmen Sie $|A \cup B \cup C \cup D|$.

Aufgabe 4.17 (Beweis eines Spezialfalls des Inklusions-Exklusions-Prinzips)
Beweisen Sie obige Darstellung für $|A \cup B|$ erneut ohne Verwendung des Inklusions-Exklusions-Prinzips.

Aufgabe 4.18 (Alternativer Beweis des Inklusions-Exklusions-Prinzips)
Beweisen Sie das Inklusions-Exklusions-Prinzip mittels vollständiger Induktion.

Aufgabe 4.19 (Das Inklusions-Exklusions-Prinzip und SageMath)
Es sei M die Menge aller der natürlichen Zahlen kleiner gleich 2.000, die ohne Rest durch 3 oder 7 oder 11 teilbar sind.

(i) Ermitteln Sie $|M|$ mit Hilfe des Inklusions-Exklusions-Prinzips.
(ii) Schreiben Sie eine SageMath-Routine zur Bestimmung der Menge M.

4.5 Zerlegungen

Ist A eine endliche Menge, so heißt

$$\mathcal{Z} := \{A_1, \ldots, A_p\}$$

eine *Zerlegung* von A in Teilmengen $A_1, \ldots, A_p$, mit einem $p \in \mathbb{N}_+$ wenn $A_j \neq \emptyset$ for alle $j = 1, \ldots, p$ und

$$A_i \cap A_j = \emptyset \text{ für } i \neq j \quad \text{und} \quad A_1 \cup \cdots \cup A_p = A$$

gültig ist. Ist $|A| = n$, so heißt die Anzahl der Zerlegungen von A die *n-te Bellsche Zahl* B_n.

Beispiel. Die einzige Zerlegung der leeren Menge $\emptyset$ ist die leere Menge selbst, so dass $B_0 = 1$ richtig ist. Weiter ist $B_1 = 1$. Sämtlich Zerlegungen der zweielementigen Menge $\{a, b\}$ sind schließlich $\{\{a\}, \{b\}\}$ und $\{\{a, b\}\}$, so dass $B_2 = 2$. Als Übung verifiziere man folgende Tabelle:

n	0	1	2	3	4	5
B_n	1	1	2	5	15	52

Satz 4.6: Es sei $n \in \mathbb{N}$. Dann gilt $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$.

Beweis. Betrachte eine Menge A mit $|A| = n + 1$, $n \in \mathbb{N}$, und eine Zerlegung $\mathcal{Z} = \{A_1, \ldots, A_p\}$. Wähle ein $a \in A$ beliebig aus. Es gibt dann genau ein $A^* \in \mathcal{Z}$ mit $a \in A^*$ und $|A^*| = n + 1 - k$ für ein $k \in [0, n + 1]$. Die Restmenge $A \setminus A^*$ erlaubt B_k Zerlegungen, und zur Auswahl einer $(n - k)$-elementigen Menge gibt es $\binom{n}{n-k} = \binom{n}{k}$ Möglichkeiten. Es ergibt sich die Behauptung. ∎

Die B_n können wir auch mit dem sogenannten *Bellschen Dreieck* berechnen:

1. Die n-te Zeile besteht aus n Elementen.
2. Die erste Zeile besteht nur aus der Zahl 1.
3. Das letzte Element der n-ten Zeile ist das erste Element der $(n + 1)$-ten Zeile.
4. Der k-te Eintrag der n-ten Zeile ist die Summe des $(k - 1)$-ten Elementes der n-ten Zeile und des $(k-1)$-ten Elementes der $(n-1)$-ten Zeile.

1				
1	2			
2	3	5		
5	7	10	15	
15	20	27	37	52

Satz 4.7: B_n ist der letzte Eintrag in der n-ten Zeile des Bellschen Dreiecks.

Beweis. Sei $A_{k,n}$ die Anzahl der Zerlegungen einer $n+1$-elementigen Mengen mit folgender Eigenschaften:

1. Die Menge $\{k+1\}$ (Singleton) gehört zur Zerlegung.
2. Jedes Element $j > k+1$ ist in einer Menge der Zerlegung, welche mindestens zwei Elemente enthält. (Also $\{k+1\}$ ist das letzte Singleton.)

Mit $A_{-1,n}$ bezeichen wir somit alle Zerlegungen ohne Singletons. Wir setzen $A_{n,n} := B_n$. Insbesondere $A_{1,1} = B_1 = 1$.
Ist $k < n$ und wenn wir das Element $k+1$ aus eine Zerlegung in $A_{k,n}$ streichen, so erhalten wir eine Element aus $A_{j,n-1}$ für ein $j \leq k-1$. Deshalb gilt

$$A_{k,n} = \sum_{j=-1}^{k-1} A_{j,n-1}$$

Anwendung auf $k-1$ statt k und Subtraktion führt zu der Formel

$$A_{k,n} = A_{k-1,n-1} + A_{k-1,n}.$$

Diese Gleichung gilt auch für $k = n$. Mit $B_n = A_{n,n}$ und Z eine Zerlegung von A, so ämlich entweder ist $\{n\}$ ein Singleton von Z und wir haben ein Element aus $A_{n-1,n}$ oder wir streichen n und erhälten ein Element aus $B_{n-1} = A_{n-1,n-1}$.
Es ist noch zu zeigen, dass $B_n = A_{1,n+1}$. Es sei eine Zerlegung von $\{3,\ldots,n+2\}$ gegeben. Dann nehmen wir alle Singletons dieser Zerlegung zusammen und nehmen noch die 1 dazu. Die andere Teilmengen von $\{3,\ldots,n+2\}$ lassen wir unverändert und nehmen das Singleton $\{2\}$ dazu. Wir erhalten ein Element von $A_{1,n+1}$. Umgekehrt lässt sich aus dem Element von $A_{1,n+1}$ die Zerlegung von $\{3,\ldots,n+2\}$ aus B_n wiederherstellen. ∎

Aufgaben

Aufgabe 4.20

1. Bestimmen Sie alle Zerlegungen von $\{1,2,3\}$ und von $\{1,2,3,4\}$.
2. Berechnen Sie mit der Hand B_6 und B_7, sowohl mit Satz ?? als auch mit dem Bellschen Dreieck.
3. Schreiben Sie ein SAGEMATH Programm, das die Bellsche Zahlen berechnet.

Aufgabe 4.21 Sei A eine Menge mit n Elementen und $Z_k(A)$ die Menge der Zerlegungen von A in k Teilmengen. Wir schreiben $\left\{ {n \atop k} \right\}$ für $|Z_k(A)|$ und nennen diese Zahlen Stirlingsche Zahlen zweiter Art. Zeigen Sie für $n \geq 1$

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}.$$

Beschreiben Sie einen Art Pascalschen Dreiceck für diese Stirlingsche Zahlen.

4.6 Permutationen

1. Ist A eine (endliche) Menge, so nennt man eine bijektive Abbildung $\sigma\colon A \to A$ auch eine Permutation von A.
2. Die Menge der Permutationen von A bezeichnen wir mit $S(A)$.
3. Mit $e \in S(A)$ bezeihnen wir die identische Permutation: $e(a) = a$ für alle $a \in A$.
4. Sind σ, τ Permutationen von A so ist die Verknüpfung $\sigma \circ \tau$ ebenfalls eine Permutation. Also gilt $\sigma\tau(a) = \sigma(\tau(a))$ für alle $a \in A$.
5. Für $\sigma \in S(A)$ definieren wir $\sigma^{-1} \in S(A)$ durch: $\sigma(a) = b \iff a = \sigma^{-1}(b)$.

Man kann eine Permutation der Menge A in Tabellenform schreiben, indem man unter jedes Element sein Bild schriebt:

$$\sigma = \begin{array}{c|c|c|c} a_1 & a_2 & \dots & a_n \\ \hline \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_n) \end{array}.$$

σ ist genau dann eine Permutation, wenn in der zweite Zeile dieser Tabelle alle Elemente von A genau einmal vorkommen.
Für $A = \{1, 2, \dots, n\}$ schreibt man S_n statt $S(\{1, 2, \dots, n\})$ und nennt diese die *symmetrische Gruppe* vom Grad n. Bemerke, dass S_n genau $n!$ Elemente hat.

Beispiel:

1. S_2 hat die $2! = 2$ Elemente $\sigma = \begin{array}{c|c} 1 & 2 \\ \hline 1 & 2 \end{array}$ und $\tau = \begin{array}{c|c} 1 & 2 \\ \hline 2 & 1 \end{array}$. Also gilt $\sigma(1) = 1$, $\sigma(2) = 2$, $\tau(1) = 2$, $\tau(2) = 1$.
2. Für das Element $\sigma = \begin{array}{c|c|c} a & b & c \\ \hline c & a & b \end{array} \in S(\{a, b, c\})$ gilt $\sigma(a) = c$, $\sigma(b) = a$, $\sigma(c) = b$.
3. S_3 hat die folgenden $3! = 6$ Elemente

$$\begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 1 & 2 & 3 \end{array}, \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 2 & 1 & 3 \end{array}, \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 3 & 2 & 1 \end{array}, \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 1 & 3 & 2 \end{array}, \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 2 & 3 & 1 \end{array}, \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 3 & 1 & 2 \end{array}.$$

Beispiel: Für $\sigma = \begin{array}{c|c|c|c} 1 & 2 & 3 & 4 \\ \hline 2 & 1 & 4 & 3 \end{array}$, $\tau = \begin{array}{c|c|c|c} 1 & 2 & 3 & 4 \\ \hline 4 & 1 & 2 & 3 \end{array} \in S_4$ gilt:

$$\begin{aligned} \sigma\tau(1) &= \sigma(4) = 3, & \sigma\tau(2) &= \sigma(1) = 2, \\ \sigma\tau(3) &= \sigma(2) = 1, & \sigma\tau(4) &= \sigma(3) = 4. \end{aligned}$$

Also $\sigma\tau = \begin{array}{c|c|c|c} 1 & 2 & 3 & 4 \\ \hline 3 & 2 & 1 & 4 \end{array}$. Genauso rechnet man nach: $\tau\sigma = \begin{array}{c|c|c|c} 1 & 2 & 3 & 4 \\ \hline 1 & 4 & 3 & 2 \end{array}$.

Wie wir im obigen Beispiel sehen, gilt im Allgemeinen nicht $\sigma\tau = \tau\sigma$. Daher ist diese Operation nicht kommutativ. Allerdings ist sie assoziativ, da die Komposition von Abbildungen bereits assoziativ ist.

Beispiel: Für $\sigma = \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 4 & 1 & 2 & 3 \\ \hline \end{array} \in S_4$ gilt:

$$\sigma^{-1} = \begin{array}{|c|c|c|c|}\hline 4 & 1 & 2 & 3 \\ \hline 1 & 2 & 3 & 4 \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 2 & 3 & 4 & 1 \\ \hline \end{array}.$$

Aufgaben

Aufgabe 4.22 *(Mächtigkeit der symmetrischen Gruppe)*
Es sei $n \in \mathbb{N}_+$. Beweisen Sie, dass S_n genau $n!$ Elemente besitzt.

Aufgabe 4.23 Es sei

$$\sigma = \begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 3 & 4 & 5 \\ \hline 5 & 3 & 4 & 1 & 2 \\ \hline \end{array}$$

und

$$\tau = \begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 3 & 4 & 5 \\ \hline 2 & 1 & 4 & 3 & 5 \\ \hline \end{array}$$

Berechnen Sie $\sigma\tau, \tau\sigma, \sigma^{-1}$ und σ^3.

Aufgabe 4.24 Es sei

$$\sigma = \begin{array}{|c|c|c|c|c|c|}\hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 5 & 3 & 6 & 4 & 1 & 2 \\ \hline \end{array}$$

und

$$\tau = \begin{array}{|c|c|c|c|c|c|}\hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 6 & 1 & 2 & 3 & 5 & 4 \\ \hline \end{array}$$

Berechnen Sie $\sigma\tau, \tau\sigma, \sigma^{-1}$ und σ^3.

4.7 Zyklusschreibweise einer Permutation

1. Für eine endliche Menge A und $b_1, \ldots, b_k \in A$ mit $b_i \neq b_j$ für $i \neq j$ definieren wir das Elemente $\sigma = (b_1, b_2, \ldots, b_k) \in S(A)$ durch:

$$\sigma(b_1) = b_2,\ \sigma(b_2) = b_3,\ \cdots\ \sigma(b_{k-1}) = b_k,\ \sigma(b_k) = b_1$$

$$\sigma(a) = a \text{ für } a \in A \setminus \{b_1, b_2, \ldots, b_k\}.$$

   Wir nennen $(b_1 \ldots b_k)$ einen *Zyklus* der Länge k.

2. Zwei Zyklus $(b_1, \ldots, b_k)$ und $(c_1, \ldots, c_m)$ heißen *disjunkt*, wenn $b_i \neq c_j$ für $i = 1, \ldots k$ und $j = 1, \ldots m$.

Beachte, dass gilt:

$$(b_1, b_2, \ldots, b_k) = (b_2, b_3, \ldots b_k, b_1) = (b_3, b_4, \ldots, b_k, b_1, b_2) = \ldots = (b_k, b_1, \ldots, b_{k-1}),$$
$$(b_1, b_2, \ldots, b_{k-1}, b_k)^{-1} = (b_k, b_{k-1}, \ldots b_2, b_1).$$

Beispiel: Für $\sigma = (1, 2, 3) \in S_4$ gilt:

$$\begin{aligned} \sigma(1) &= 2,\ \sigma(2) = 3,\ \sigma(3) = 1,\ \sigma(4) = 4, \\ \sigma &= (1,2,3) = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 2 & 3 & 1 & 4 \\ \hline \end{array} \neq \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 1 & 2 & 4 \\ \hline \end{array} = (3,2,1) = \sigma^{-1}, \\ \sigma &= (1,2,3) = (2,3,1) = (3,1,2). \end{aligned}$$

Satz 4.1

1. Für zwei diskjunkte Zyklus σ, τ gilt: $\sigma\tau = \tau\sigma$.
2. Ist A eine endliche Menge, so lässt sich jedes Element von $S(A)$ als Produkt von disjunkten Zyklen schreiben. Diese Darstellung ist eindeutig bis auf Reihenfolge.

Beweis.

1. Kommt b nicht in σ und nicht in τ vor, so gilt $\sigma\tau(b) = \tau\sigma(b) = b$. Kommt b in σ vor, aber nicht in τ, so gilt $\sigma\tau(b) = \tau\sigma(b) = \sigma(b)$. Kommt b in τ vor, aber nicht in σ, so gilt $\sigma\tau(b) = \tau\sigma(b) = \tau(b)$.

2. Induktion Sei k minimal mit $\sigma^k(1) = 1$. Dann kommt der Zyklus

$$\sigma_1 := (1, \sigma(1), \ldots, \sigma^{k-1}(1))$$

   in einer Darstellung von σ als Produkt von disjunkten Zyklen vor. Wende jetzt Induktion auf $\sigma_1^{-1} \cdot \sigma$ an. Dann ist $\sigma_1^{-1} \cdot \sigma = \sigma_2 \cdot \ldots \cdot \sigma_t$ ein Produkt von disjunkten Zyklen und $\sigma = \sigma_1 \cdot \sigma_2 \cdot \ldots \cdot \sigma_t$ auch.

Beispiel: In S_7 gilt:

$$\sigma = \begin{array}{|c|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline 4 & 1 & 5 & 2 & 7 & 3 & 6 \\ \hline \end{array} = (1,4,2)\cdot(3,5,7,6)$$

Ist σ ein k-Zyklus, so ist $\sigma^k = e$. Weiterhin gilt für disjunkte $k - Zyklus$ $\sigma_1, \cdots, \sigma_\ell$, dass $(\sigma_1 \cdot \ldots \cdot \sigma_\ell^k = \sigma_1^k \cdot \ldots \cdot \sigma_\ell^k$, vgl. Aufgabe 4.25. Somit gilt in obigen Beispie

$$\sigma^4 = (1,4,2)^4 \cdot (3,5,7,6)^4 = (1,4,2)^3 \cdot (1,4,2) \cdot e = (1,4,2).$$

Aufgaben

Aufgabe 4.25 Zeigen Sie mit Induktion nach k: Gilt $\sigma\tau = \tau\sigma$, so ist $(\sigma\tau)^k = \sigma^k\tau^k$. Finden Sie nicht kommutierende σ und τ für die gilt $(\sigma\tau)^2 \neq \sigma^2\tau^2$.

Aufgabe 4.26 Schreiben Sie die nachfolgende Permutation σ als Produkt von disjunkten Zyklen und berechnen Sie σ^9.

1. $\sigma = \begin{array}{|c|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline 4 & 7 & 6 & 3 & 2 & 1 & 5 \\ \hline \end{array}$

2. $\sigma = \begin{array}{|c|c|c|c|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \hline 9 & 4 & 6 & 6 & 3 & 10 & 2 & 5 & 8 & 1 \\ \hline \end{array}$

3. $\sigma = \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ \hline 6 & 4 & 12 & 13 & 1 & 5 & 2 & 3 & 9 & 8 & 10 & 11 & 7 \\ \hline \end{array}$

4. $\sigma = (3,6,7,8)(1,7,5,4)(2,6)$.

Aufgabe 4.27 Schreiben Sie für die nachfolgende σ das Inverse σ^{-1} ebenfalls in Zyklusschreibweise.
1. $\sigma = (1,2,3,4)$, 2. $\sigma = (1,2,3,4,5,6,7)$, 3. $\sigma = (1,2,3,4)(5,6,7)$

Aufgabe 4.28 Schreiben Sie ein SAGEMATH-Programm, das eine Permutation als Produkt disjunkter Zyklusen schreibt.

Aufgabe 4.29 Es sei $\tau = (1,2,3,4,\ldots,k)$ ein k-Zyklus in S_n und $\sigma \in S_n$ beliebig. Warum ist

$$\sigma \cdot \tau \cdot \sigma^{-1}$$

ebenfalls ein k-Zyklus. Wie sieht er aus?

4.8 Paarvertauschungen

1. Ein Zyklus der Länge zwei heißt *Transposition* oder auch *Paarvertauschung.*
2. Für $A = \{1, \ldots, n\}$ heißen Zyklus der Form $(i, i+1) = (i+1, i)$ für $1 \leq i \leq n-1$ *Nachbarvertauschungen.*

Satz 4.2 1. Jede Permutation lässt sich als Produkt von Nachbarvertauschungen schreiben.

2. Jede Paarvertauschung ist das Produkt von ungerade viele Nachbarvertauschungen.
3. Jeder Zyklus der Länge k lässt sich als Produkt von $k-1$ Transpositionen schreiben.

Beweis.

1. Induktion nach n. Ist $\sigma(n) = n$, so können wir direkt die Induktionsvoraussetzung anwenden. Sei $\sigma(i) = n$. Wir machen Induktion nach $n - i$, für $n = i$ ist die Aussage war. Sei also $i < n$ und Sei $\tau = \sigma \cdot (i, i+1)$. Dan ist $\tau(i+1) = n$ und mit Induktion ist τ ein Produkt von Nachbarvertauschungen und somit $\sigma = \tau \cdot (i, i+1)$ auch.
2. Es gilt $(i, j) = (i, i+1) \cdot (i+1, i+2) \cdot \ldots \cdot (j-1, j) \cdot (j-1, j-2) \cdot \ldots \cdot (i+1, i)$.
3. Es gilt $(b_1, \ldots, b_k) = (b_1, b_2) \cdot (b_2, b_3) \cdot \ldots \cdot (b_{k-1}, b_k)$. ———

Beispiel: In S_4 gilt:

1. $(1, 3, 4, 2) = (1, 3) \cdot (3, 4) \cdot (4, 2)$.
2. $(1, 4) = (1, 2) \cdot (2, 3) \cdot (3, 4) \cdot (3, 2) \cdot (2, 1)$.

Aufgaben

Aufgabe 4.1 *(Zyklus als Produkt von Paarvertauschungen II)*
Stellen Sie folgende Zyklus ϑ der Länge 4 als Produkt $\vartheta = \sigma \circ \tau \circ \omega$ von drei Paarvertauschungen σ, τ, ω dar.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ *bzw.* $\begin{pmatrix} 1 & 3 & 2 & 4 \end{pmatrix}$

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ *bzw.* $\begin{pmatrix} 1 & 4 & 2 & 3 \end{pmatrix}$

Aufgabe 4.2 *(Vorzeichen von Permutationen II)*
Bestimmen Sie die Vorzeichen folgender Permutation

$$\sigma \in S_7 \quad \textit{vermöge} \quad \sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 1 & 3 & 2 & 5 & 7 \end{pmatrix}.$$

Aufgabe 4.30 Es sei $\sigma_i = (i, i+1)$ eine Nachbarvertauschung von S_n für $i = 1, \ldots, n-1$. Zeigen Sie, dass:

1. $\sigma_i^2 = e$
2. $(\sigma_i \sigma_j)^2 = e$ für $j - i \geq 2$.
3. $(\sigma_i \sigma_{i+1})^3 = e$

Aufgabe 4.31

1. Zeigen Sie: Sind $a, b, c \in \{1, \ldots, n\{$ paarweise verschieden, so gilt
$$(a\,b) \cdot (b\,c)$$
2. Zeigen Sie: Sind $(a, b, c, d) \in \{1, \ldots, n\}$ paarweise verschieden, so gilt
$$(a\,b) \cdot (c\,d) = (a\,b\,c) \cdot (b\,c\,d).$$

4.9 Das Vorzeichen einer Permutation

Sei $\sigma \in S_n$.

1. Ein Paar (i, j) heißt Inversion von σ wenn $1 \leq i < j \leq n$ und $\sigma(i) > \sigma(j)$.
2. Das *Vorzeichen* oder *Signum* von σ ist gleich 1 wenn die Anzahl der Inversionen von σ gerade und gleich -1, wenn die Anzahl der Inversionen von σ ungerade ist.

Beispiel: $\sigma = (1, 2, 3, 4) \in S_5$ hat das Vorzeichen $(-1) = (-1)^3$, da die Inversionen von σ die Menge $\{(1, 4), (2, 4), (3, 4)\}$. bilden.

Satz 4.3 1. Für $\sigma, \tau \in S_n$ gilt:

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau).$$

2. Ist σ das Produkt von s Paarvertauschungen, so gilt $\operatorname{sgn}(\sigma) = (-1)^s$. Insbesondere: Ein $k-$Zyklus ist gerade genau dann, wenn k ungerade ist.

Beweis.

1. Es sei $\sigma \in S_n$ und $1 \leq k \leq n-1$ gegeben. und $\tau = (k, k+1)$. Dann gilt:

   (a) Ist $i < k$ und $k+1 < j$, so ist (i, j) eine Inversion von σ genau dann, wenn sie eine Inversion von $\sigma \cdot (k, k+1)$ ist, denn $\sigma \cdot (k, k+1)(i) = \sigma(i)$ und analog für j.

   (b) (i, k) ist eine Inversion von σ, genau dann, wenn $(i, k+1)$ eine Inversion von $\sigma \cdot (k, k+1)$ ist, denn $\sigma(i) > \sigma(k)$ und $\sigma \cdot (k, k+1)(i) = \sigma(i) > \sigma(k) = \sigma \cdot (k, k+1)(k+1)$.

   (c) Analog ist $(k+1, j)$ eine Inversion von σ genau dann, wenn (k, j) eine Inversion von $\sigma \cdot (k, k+1)$ ist.

   (d) Ist $(k, k+1)$ eine Inversion von σ, so ist $\sigma(k) > \sigma(k+1)$ und $\sigma \cdot (k, k+1)(k) < \sigma \cdot (k, k+1)(k+1)$, so dass $(k, k+1)$ keine Inversion von $\sigma \cdot (k, k+1)$ ist. Die Umkehrung gilt auch.

   Somit ist die Anzahl der Inversionen von σ eins mehr oder eins weniger als die Anzahl der Inversionen von $\sigma \cdot (k, k+1)$. Somit ist die Aussage wahr für $\tau = (k, k+1)$ eine Nachbarvertauschung. Eine Induktion zeigt dann, dass $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)(-1)^s$ ist, wenn τ als Produkt von s Nachbarvertauschungen geschrieben werden kann. Für $\sigma = e$ folgt, dass $\operatorname{sgn}(\tau) = (-1)^s$ und somit gilt $\operatorname{sgn}(\sigma \cdot \tau) = \operatorname{sgn}(\sigma) \cdot (-1)^s = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$.

2. Eine Paarvertauschung ist das Produkt von ungerade viele Nachbarvertauschungen, somit nach dem Beweis im ersten Teil eine ungerade Permutation. Jetzt

benutze,

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma_1) \cdot \ldots \cdot \sigma(\sigma_s) = (-1)^s$$

wenn σ_i Paarvertauschungen sind. ∎

Beispiel: Für

$$\sigma = \begin{array}{c|c|c|c|c|c|c|c|c|c} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 6 & 1 & 10 & 8 & 3 & 9 & 4 & 2 & 7 \end{array}$$

gilt $\sigma = (1, 5, 8, 4, 10, 7, 9, 2, 6, 3)$, als ist σ ein 10-Zyklus ist somit ungerade.

Aufgaben

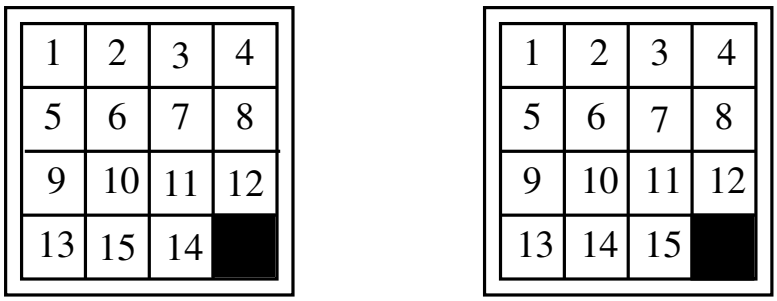
Aufgabe 4.32 Es sei $\sigma \in S_n$ eine Permutation mit der Inversen $\sigma^{-1} \in S_n$. Zeigen Sie, dass $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$.

Aufgabe 4.33 Berechnene Sie $\operatorname{sgn}(\sigma)$ für die nachfolgenden Permutationen σ.

1. $\sigma = \begin{array}{c|c|c|c|c|c|c|c|c|c} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 6 & 1 & 9 & 8 & 3 & 10 & 4 & 2 & 5 \end{array}$

2. $\sigma = \begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c|c|c} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 8 & 3 & 9 & 15 & 1 & 6 & 13 & 11 & 5 & 12 & 14 & 2 & 7 & 10 \end{array}$

Aufgabe 4.34 Samuel Loyd erfand 1878 das auch jetzt noch populäre Schiebepuzzle. Er forderte seine Leser auf, ausgehend von der linken Position durch Verschieben die rechte Position zu erreichen.
Samuel Loyd hatte 1000 Dollar ausgesetzt für denjenigen, der zuerst eine Lösung einschickt, was dazu führte, dass Arbeitgeber Schilder aufstellten, die es den Angestellten verboten, während der Arbeitszeit das Puzzle zu spielen. Es war in dieser Hinsicht also ein Vorbote einiger heutzutage populären Computerspiele.



Zeigen Sie, dass dieses Puzzle unlösbar ist!

Aufgabe 4.35 Zeigen Sie, das jede gerade Permutation als Produkt von 3-Zyklen geschrieben werden kann (nicht notwendigerweise disjunkt).

4.10 Verwirrungen

Eine Verwirrung ist eine Permutation $\sigma \in S_n$, sodass $\sigma(i) \neq i$ für alle $i \in \{1, \ldots, n\}$.

Satz 4.4 Die Anzahl von Verwirrungen in S_n ist gleich

$$n! \cdot \left(\frac{1}{2!} + \ldots + (-1)^n \cdot \frac{1}{n!} \right)$$

Beweis. Die Anzahl von Verwirrungen ist gleich $n!$ minus die Anzahl Elemente der Menge

$$P := \{\sigma \in S_n \colon \exists i \text{ mit } \sigma(i) = i\}.$$

Es sei $P_i := \{\sigma \in S_n \colon \sigma(i) = i\}$. Dann ist $P = P_1 \cup \cdots \cup P_n$. Für verschiedene $i_1, \ldots, i_s$ gilt

$$\#(P_{i_1} \cap \cdots \cap P_{i_s}) = (n-s)!.$$

Aus dem Inklusion-Exklusionprinzip folgt deshalb:

$$\begin{aligned} \#P &= \binom{n}{1}(n-1)! - \binom{n}{2}(n-2)! - \cdots + (-1)^{n-1}\binom{n}{n}0! \\ &= n! \cdot \left(1 - \frac{1}{2!} + \ldots + (-1)^{n-1} n \cdot \frac{1}{n!}\right) \end{aligned}$$

woraus die Behauptung des Satzes folgt. ∎

Wir geben noch einen zweiten Beweis mit Induktion. Es sei D_n die Anzahl der Verwirrungen. Dann gilt $D_2 = 1$ und $D_1 = 0$. Sei $n \geq 2$ und $\sigma(n) = n - 1$. Dann gibt es zwei Möglichkeiten.

1. $\sigma(n-1) = n$. Davon gibt es D_{n-2} Stück.
2. $\sigma(n-1) \neq n$. Dann definiert τ mit

$$\tau(i) = \begin{cases} \sigma(i) & \text{falls } \sigma(i) \neq n \\ n-1 & \text{falls } \sigma(i) = n \end{cases}$$

für $i = 1, \ldots, n-1$ eine Verwirrung. Analog für $\sigma(n) = i$ für $i < n - 1$. Somit gilt

$$D_n = (n-1) \cdot \Big(D_{n-1} + D_{n-2} \Big).$$

Jetzt beweist man mit Induktion die gewünschte Formel, siehe Aufgabe 4.36.

Aufgaben

Aufgabe 4.36 Es sei $D_1 = 0$ und $D_2 = 0$ und es gelte $D_n = (n-1) \cdot \Big(D_{n-1} + D_{n-2}\Big)$ für $n \geq 3$. Zeigen Sie, dass

$$n! \cdot \left(1 - \frac{1}{1!} + \frac{1}{2!} + \ldots + (-1)^n \cdot \frac{1}{n!}\right)$$

Aufgabe 4.37 *(Fixpunktfreie Permutationen)*
Bestimmen Sie alle fixpunktfreien Permutationen $\sigma \in S_4$, und verifizieren Sie die Identität

$$d_4 = \left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!}\right) \cdot 4!$$

für die Anzahl aller fixpunktfreien Permutationen aus S_4.

Aufgabe 4.38 Schreiben Sie ein SAGEMATH-Programm, das alle Verwirrungen in S_n aufschreibt. Bis zu welchem n funktioniert Ihr Programm?

4.11 Die Stirlingsche Zahlen erster Art.

Wir definieren die Stirlingsche Zahlen erster Art, Notation, $\left[\begin{array}{c} n \\ k \end{array} \right]$ als die Anzahl der Permationen von n Elementen mit genau k Zyklen (die 1-Zyklen mitgerechnet).

Also

- $\left[\begin{array}{c} n \\ n \end{array} \right] = 1$
- $\left[\begin{array}{c} n \\ k \end{array} \right] = 0$ falls $k = 0$ oder $k > n$
- $\left[\begin{array}{c} n \\ 1 \end{array} \right] = (n-1)!$
- $\left[\begin{array}{c} n+1 \\ k \end{array} \right] = \left[\begin{array}{c} n \\ k-1 \end{array} \right] + n \left[\begin{array}{c} n \\ k \end{array} \right]$
- $\sum_{k=1}^{n} \left[\begin{array}{c} n \\ k \end{array} \right] = n!$

Für die vorletzte Gleichung, das letzte Element ist entweder einen 1-Zyklus und wir brauchen dann noch $k-1$ Zyklen aus den übrigen Elementen, oder man nimmt k Zyklen aus n Elementen und man hat dann n Möglickeiten, das restliche Element vor einem zu stellen. Wir erhalten wieder ein Art Pascalsche Dreiecks.

						1						
					1		1					
				2		3		1				
			6		11		6		1			
		24		50		35		10		1		
	120		274		225		85		15		1	

Kapitel 5

Elementare Zahlentheorie

5.1 Teilung mit Rest

In der Schule kommt nach der Addition und Multiplikation von natürlichen Zahlen als nächstes Teilung mit Rest.

Satz 5.1 Es seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}_+$. Dann gibt es eindeutig bestimmte Zahlen $q \in \mathbb{Z}$ und $r \in \mathbb{N}$ mit

1. $a = qb + r$
2. $0 \leq r \leq b - 1$.

Beweis. **Existenz.** Für $a \geq 0$ führen wir (starken) Induktion nach a durch. Ist $a < b$, so nehme $q = 0$ und $r = a$. Sonst ist $a \geq b$. Dann ist $a' := a - b < a$ und nach Induktion gibt es ein $q' \in \mathbb{N}_0$ und $r \in \mathbb{N}_0$ mit $0 \leq r < b - 1$ und $a' = q' \cdot b + r$. Dann ist $a = a' + b = (q' + 1) \cdot b + r$. Nehme $q = q' + 1$.

Ist $a < 0$, so ist $-a > 0$ und $-a = q'b + r'$ und $a = -q'b - r'$. Ist $r' = 0$, so nehmen $r = 0$ und $q' = q$. Sonst $a = (-q' - 1)b + n - r'$ und nehmen $q = -q' - 1$ und $r = n - r'$.

Eindeutigkeit. Sei $a > 0$. Ist $a = qb + r = q'b + r'$ mit o.B.d.A. $q \geq q'$. Dann folgt $(q - q') \cdot b = r' - r$ und $r' \geq r$. Ist $q > q'$ so ist die linke Seite größer als b, die rechte Seite kleiner als b. Das ist nicht möglich. Somit ist $q = q'$ und auch $r = r'$ folgt. Der Fall $a < 0$ geht analog. ∎

Es sei n eine natürliche Zahl mit $n \geq 2$. Wir betrachten eine Menge $\underline{n} = \{0, 1 \ldots, n-1\}$ mit n Elementen, die wir in diesem Zusammenhang mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnen. Wir definieren auf dieser Menge zwei Verknupfüngen, eine "Addition" $+_n$ und eine "Multiplikation" $\cdot_n$ vermöge:

$$\begin{aligned} a +_n b &:= (a + b) \bmod n \\ a \cdot_n b &:= (a \cdot b) \bmod n \end{aligned}$$

Die Erklärung, weshalb solche Operationen interessant sind und Anwendungen hiervon kommen später. Vorab können wir aber sagen, dass wenn wir in $\mathbb{Z}/n\mathbb{Z}$ rechnen, die Zahlen nie größer als n werden können. Das ist als speichertechnische Gründe vorteilhaft.

Bemerkung. Wenn aus dem Kontekst klar ist, was n ist so schreiben wir auch einfach $+$ statt $+_n$ und ebenso $\cdot$ statt $\cdot_n$. Oft wird auch $\cdot$ weggelassen, aber ich werde versuchen diese Versuchung zu widerstehen.
wieder a statt $\overline{a}$. **Beispiel.**

1. In $\mathbb{Z}/6\mathbb{Z}$ gilt $2 \cdot 3 = 0$.
2. In $\mathbb{Z}/101\mathbb{Z}$ gilt $22 \cdot 23 = 506 = 1 \bmod 101$.

Satz 5.2 Die Menge $\mathbb{Z}/n\mathbb{Z}$ zusammen mit der Addition und Multiplikation bilden einen sogenannten kommutativen Ring mit 1. Dies bedeutet, dass

1. Die Addition ist kommutativ und assoziativ. Es gilt $a+0=a$ und für jedes a gibt es ein negativem $-a = n - a \bmod n$ mit $a + (-a) = 0$.
2. Die Multiplikation ist kommutativ und assoziativ. Es gilt $a \cdot 1 = a$ für jedes a.
3. Es gilt das Distributivgesetz: $a \cdot (b + c) = a \cdot b + a \cdot c$ in $\mathbb{Z}/n\mathbb{Z}$.

Beweis. Es gilt $a \bmod n = b \bmod n$ genau dann, wenn $a = q_1 n + r$ und $b = g_2 n + r$ für bestimmte q_1, q_2 und r. Dies gilt genau dann, wenn $n \mid (a - b)$ Es folgt

$$(a +_n b) +_n c = ((a +_n b) + c) \bmod n = (a + b + c) \bmod n,$$

woraus die Assoziativität jetzt direkt folgt, denn die gleiche Aussage gilt auch für $a +_n (b +_n c)$.
Ein Negativum existiert, denn $a+(n-a) = 0$. Die Kommutativität und Assoziativität der Multiplikation beweist man genauso, sowie auch die Distributivität. ∎

Aufgaben

Aufgabe 5.1 Berechnen Sie:

1. $6 + 5 \bmod 11$
2. $7 \cdot 8 \bmod 10$
3. $22 \cdot 23 \bmod 101$
4. $2^{10} \bmod 11$
5. $10 \cdot 10 \bmod 100$.

Aufgabe 5.2 Füllen Sie die nachfolgende Mutliplikationstabelle modulo 11 aus. Was fällt auf?

·	1	2	3	4	5	6	7	9	10
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									

5.2 Teiler und euklidischer Algorithmus

Es sei $a \in \mathbb{Z}$ und $b \in \mathbb{N}_+$. Wir sagen, dass b die Zahl a teilt, wenn es eine natürliche Zahl q gibt mit $a = qb$, Notation $b \mid a$.

Zum Beispiel ist $7 \mid 1001$, weil $1001 = 7 \cdot 143$.
Es gilt also:

$$\begin{aligned} a \mid b &\iff b \bmod a = 0 \\ &\iff \exists q \in \mathbb{N} \ : \ b = q \cdot a. \end{aligned}$$

Satz 5.3 Es gilt:

1. $a \mid b$ und $b \mid c \implies a \mid c$.
2. $a \mid b$ und $a \mid c \implies a \mid (b+c)$ und $a \mid (b-c)$.
3. $a \mid b$ und $c \mid d \implies a \cdot c \mid b \cdot d$.
4. Sind $a, b \in \mathbb{N}$ und $a \mid b$ dann ist $a \leq b$.
5. $1 \mid a$, $a \mid a$. Die Zahlen 1 und a heißen *triviale* Teiler von a.

Beweis. Diese Aussagen lassen sich alle leicht zeigen. Zum Beispiel die zweiter Aussage. Ist $a \mid b$, so ist $b = q \cdot a$ für ein $q \in \mathbb{N}$. Ist $a \mid c$, so ist $b = s \cdot a$ für ein $s \in \mathbb{N}$. Daher $(b+c) = (q+s) \cdot a$, sodass $a \mid (b+c)$ folgt. Die andere Aussagen zeigt man auf ähnliche Weise. ∎

1. Sei $a \in \mathbb{N}$, so definieren wir $T(a) := \{b \in \mathbb{N}_+ \colon b \mid a\}$ die Menge der Teiler von a.
2. Sind $a, b \in \mathbb{N}$, so definieren wir $T(a,b) = T(a) \cap T(b)$, die Menge der gemeinsamen Teiler.
3. Wir definieren $\mathrm{ggT}(a,b)$, der größte gemeinsame Teiler von a und b, also das Maximum von $T(a,b)$.

Sei d ein Teiler von b und $a = qb + r$. Dann gilt $d \mid a \iff d \mid r$. Es gilt deshalb $T(a,b) = T(b,r)$ und insbesondere $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r)$. Weil außerdem $\mathrm{ggT}(a,0) = a$, funktioniert der nachfolgende euklidischer Algorithmus.

```
def euklid(a,b):
    while b!=0:
        a,b = b, a%b
    return a
```

Aufgaben

Aufgabe 5.3 Bestimmen Sie $T(30), T(42)$ und $T(30, 42)$.

Aufgabe 5.4 Erweitern Sie das Programm `euklid(a,b)`, indem Sie zusätzlich die Anzahl der Schleifen ausgibt, welche der euklidischen Algorithmus braucht. Experimentieren Sie hiermit. Zählen Sie die Anzahl Schleifen für zufällige Zahlen a und b mit 100 Dezimalstellen. Was fällt auf?

Aufgabe 5.5 Berechnen Sie handschriftlich den größten gemeinsamen Teiler von a und b:

1. $a = 81,\ b = 15$
2. $a = 861,\ b = 651$
3. $a = 8415,\ b = 3003.$

Aufgabe 5.6 Wir nehmen $a > b$ mit $a, b \in \mathbb{N}$ un schreibe der euklidische Algorithmus als Sequenz von Teilungen mit Rest: Sei $a = r_n$ und $b = r_{n-1}$ und

$$\begin{aligned} r_n &= q_{n-1}r_{n-1} + r_{n-2} \\ &\vdots \\ r_2 &= q_1 r_1 + r_0 \end{aligned}$$

mit $r_0 = 0$. Es sei F_n die Fibonacci Folge, $F_0 = 0$, $F_1 = 1$ und $F_n = F_{n-1} + F_{n-2}$ für $n \geq 2$.

1. Zeigen Sie, dass $r_n \geq F_n$.
2. Zeigen Sie, dass $F_n = \dfrac{1}{\sqrt{5}}\left(\left(\dfrac{1+\sqrt{5}}{2}\right)^n - \left(\dfrac{1-\sqrt{5}}{2}\right)^n\right)$.
3. Zeigen Sie, dass $a = r_n \leq \left\lceil \frac{1}{\sqrt{5}}\varphi^n \right\rceil$.
4. Zeigen Sie, dass $n \leq 5\log_{10}(a)$.

5.3 Primzahlen

Die Zahl $a \in \mathbb{N}_+$ ist eine Primzahl, wenn $|T(a)| = 2$, die einzige Teiler von a sind somit 1 und a und $a \neq 1$.

Die Zahl 1 wird nicht als Primzahl betrachtet. Das ist kein Naturgesetz. Im 19. Jahrhundert war es noch üblich auch die Zahl 1 als Primzahl zu betrachten. Die Zahl 1 wird nicht als Primzahl betrachtet, weil man sonst viele Aussage anfangen sollte mit "Sei p eine Primzahl ungleich 1", statt "Sei p eine Primzahl".

Einen einfachen, naiven Primzahltest basiert auf folgende Tatsache.

Satz 5.4 Sei $n \in \mathbb{N}, n \geq 2$. Entweder n ist ein Primzahl, oder es existiert einen Teiler a mit $1 < a \leq \sqrt{n}$ mit a eine Primzahl.

Beweis. Mit starken Induktion nach n. Für $n = 2$ ist die Aussage richtig und die Aussage ist auch richtig, wenn n eine Primzahl ist. Ist n keine Primzahl, so sei $n = a \cdot b$ mit $1 < a$ und $1 < b$. O.B.d.A. ist $a \leq b$. Dann ist $a^2 \leq a \cdot b = n$, also $a \leq \sqrt{n}$. Ist a eine Primzahl, so sind wir fertig. Sonst wenden wir starken Induktion auf a an: a hat eine Primteiler $p \leq \sqrt{a} \leq \sqrt{n}$. Dann ist p einen Primteiler von n. ∎

Haben wir somit alle natürliche Zahlen von 2 bis $\sqrt{n}$ durchprobiert und festgestellt, dass diese alle die Zahl n nicht teilen, so ist n eine Primzahl.
Die einfachste Art und Weise, eine Liste von Primzahlen zu bestimmen, ist mit Hilfe des sogenannten **Sieb von Eratosthenes**

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~

Man schreibt alle natürlichen Zahlen bis zu einer gewissen Zahl auf und streicht dann nacheinander alle Vielfachen von 2, dann alle noch nicht gestrichenen Vielfachen von 3, und immer weiter alle noch nicht gestrichenen Vielfachen der nächsten nicht gestrichenen Zahl. Zum Schluss bleiben genau die Primzahlen übrig.

Die Primzahlen ≤ 40 sind also

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37.$$

Satz 5.5 Es gibt unendlich viele Primzahlen.

Beweis. Angenommen falsch. Sei $p_1, \ldots, p_s$ die endlich viele Primzahlen. Sei $n = p_1 \cdot \ldots \cdot p_s + 1$. Dann ist $n > p_i$ für jedes i und deshalb ist n keine Primzahl. Somit

hat n einen echten Teiler, und damit einen echten Primteiler. Aber $p_i \nmid n$ für jedes i, Widerspruch! ∎

Für eine natürliche Zahl n bezeichnen wir mit $\pi(n)$ die Anzahl der Primzahlen kleiner oder gleich n.
Nachfolgend sehen Sie eine kleine Tabelle von $\pi(n)$, wobei wir in die dritte Zeile die Werte für $n/\pi(n)$ geschrieben haben. In SAGEMATH ruft man `prime_pi(n)` auf, um $\pi(n)$ zu erhalten.

n	$=$	10	100	1000	10^4	10^5	10^6	10^7	10^8	10^9
$\pi(n)$	$=$	4	25	168	1229	9592	78498	664579	5761455	50847534
$n/\pi(n)$	$\approx$	$2,5$	$4,0$	$5,95$	$8,14$	$10,43$	$12,74$	$15,05$	$17,36$	$19,67$

Aus der Tabelle wird ersichtlich, dass wenn n durch $10n$ ersetzt wird, $n/\pi(n)$ mit ca. $2,3$ wächst. Diese Zahl ist der natürliche Logarithmus von 10. Der Primzahlsatz–von Gauß Anfang des 19. Jahrhunderts vermutet und unabhängig von Hadamard und de la Vallée Poussin in 1896 bewiesen–besagt, dass $\frac{\pi(n)}{n} \cdot \ln(n) \to 1$, wenn $n \to \infty$. Für den Beweis braucht man viel mehr Theorie, als wir Platz zur Verfügung haben. Wir werden später eine etwas schwächere Aussage beweisen.

Aufgaben

Aufgabe 5.7 Bestimmen Sie mit dem Sieb von Eratosthenos alle Primzahlen kleiner als 110.

Aufgabe 5.8 Zeigen Sie mit der naieven primzahltest, dass folgende Zahlen Primzahlen sind.

1.
2. 1009
3. 2003
4. 10007

Aufgabe 5.9 Schreiben Sie ein Computerprogramm, dass der Algorithmus des Sieb des Erasthostenes umsetzt. Bestimmen Sie hiermit die Anzahl der Primzahlen kleiner oder gleich 32.451. Vergleichen Sie mit dem eingebauten Befehl `prime_pi(n)`.

Aufgabe 5.10 Schreiben Sie ein SAGEMATH-Programm, das den naiven Primzahltest aus Satz 5.4 umsetzt. Wie groß können Sie n nehmen, damit Ihr Programm noch funktioniert?

5.4 Erweiterter euklidischer Algorithmus

Satz 5.1: (Erweiterter euklidischer Algorithmus)
Sind $a, b \in \mathbb{N}_+$ mit größten gemeinsamen Teiler $d = \text{ggT}(a, b)$, so gibt es ganze Zahlen x, y, sodass

$$d = x \cdot a + y \cdot b.$$

Die Zahlen x und y heißen Bézoutkoeffizienten.

Beweis. Wir geben zwei Beweise, ein rekursiver und ein iterativer.

Rekursiv. Es sei $a = qb + r$. Wir machen Induktion nach r. Wenn $r = 0$, so ist $\text{ggT}(a, b) = b$ und wir können $x = 0$ und $y = 1$ nhemen.
Mit Induktion gibt es x' und y' mit $d = x'b + y'r$. Mit $r = a - qb$ folgt $d = x'b + y'(a - qb) = y'a + (x' - qy')b$. Nehme $x = y'$ und $y = x' - qy'$.

Iterativ. Wir betrachten Tripel $T_i = (a_i, x_i, y_i)$ mit der Eigenschaft

$$a_i = x_i \cdot a + y_i \cdot b$$

Wir setzen $T_0 = (a, 1, 0)$ und $T_1 = (b, 0, 1)$. Sei a_{i+1} bestimmt durch Teilung mit Rest:

$$a_{i+1} := a_{i-1} - q_i \cdot a_i;\ 0 \leq a_{i+1} < a_i$$

Dann definiere x_{i+1} and y_{i+1} rekursiv durch

$$x_{i+1} := x_{i-1} - q_i \cdot x_i$$
$$y_{i+1} := y_{i-1} - q_i \cdot y_i.$$

Ist $a_{n+1} = 0$ und $a_n \neq 0$, so besagt der euklidische Algorithmus, dass $a_n = \text{ggT}(a, b)$. Wir zeigen mit Induktion

$$a_i \quad = \quad x_i \cdot + y_i \cdot b.$$

Für $i = n$ is das die erwünschte Aussage und für $i = 0$ und $i = 1$ offenbar gültig. Sind die Ausagen für $i - 1$ und i gültig, so haben wir

$$\begin{aligned} a_{i-1} &= x_{i-1} \cdot a + y_{i-1} \cdot b \\ a_i &= x_i \cdot a + y_i \cdot b \end{aligned}$$

Der Induktionsschritt folgt durch die zweite Gleichung mit q_i zu multiplizieren und von der ersten Gleichung zu subtahieren. ∎

Beispiel Den erweiterten eukldischen Algorithmus können wir mithilfe einer Tabelle durchführen. Wir führen dies durch für $a = 62$ und $b = 17$, eimmal rekursiv und eimal iterativ.

a	62	17	11	6	5
b	17	11	6	5	1
q	3	1	1	1	
x	-3	2	-1	1	0
y	11	-3	2	-1	1
hline					

i	0	1	2	3	4	5
a_i	62	17	11	6	5	1
x_i	1	0	1	-1	2	-3
y_i	0	1	-3	4	-7	11
q_i		3	1	1	1	

Somit gilt $1 = -3 \cdot 62 + 11 \cdot 17$.

Mit der Hand ist rekursiv einfacher, aber mit dem Rechner ist iterativ schneller. Hier kommen Programme.

```
def xggTr(a,b):
    if b == 0:
        return a,1,0
    A = xggTr(b,a%b)
    return A[0],A[2],A[1]-(a//b)*A[2]
```

```
def xggTi(a,b):
    A0,A1 = 1,0
    B0,B1 = 0,1
    while b!= 0:
        q = a//b
        a,b = b,a%b
        A0,A1B = A1, A0-q*A1
        B0,B1 = B1,B0-q*B1
    return a,A0,B0
```

Satz 5.6 Sei n eine natürliche Zahl und $a \in \mathbb{Z}/n\mathbb{Z}$. Dann hat die Gleichung $a \cdot x = 1$ in $\mathbb{Z}/n\mathbb{Z}$ eine Lösung genau dann, wenn $\mathrm{ggT}(a, n) = 1$.

Beweis. Ist $\mathrm{ggT}(a, n) = 1$ so gibt es nach dem erweiterten euklidischen Algorithmus $\widetilde{x}$, $\widetilde{y} \in \mathbb{Z}$ (die Bézoutkoeffizienten), sodass $\widetilde{x} \cdot a + \widetilde{y} \cdot n = 1$. Wir führen Teilung mit Rest durch: $\widetilde{x} = q \cdot n + x$ mit $x \in \{0, 1 \ldots, n-1\}$. Dann gilt

$$x \cdot a = 1 + (-aq - \widetilde{y}) \cdot n$$

Somit ist $x \cdot a = 1 \in \mathbb{Z}/n\mathbb{Z}$. Ist umgekehrt $a \cdot x = 1$ in $\mathbb{Z}/n\mathbb{Z}$, so gibt es ein q, sodass $a \cdot x = 1 + q \cdot n$. Hieraus folgt $\mathrm{ggT}(a, n) = 1$. ∎

Aufgaben

Aufgabe 5.11 Führen Sie mit der Hand den erweiterten euklidischen Algorithmus in den folgenden Fälle durch.
1. $a = 213, b = 413$, 2. $a = 145, b = 43$, 3. $a = 1234, b = 512$

Aufgabe 5.12 Lösen Sie, wenn möglich, die folgende Gleichungen in $\mathbb{Z}/n\mathbb{Z}$. 1) $4x = 1$, $n = 101$, 2) $4x = 13$, $n = 101$, 3) $11x = 1$, $n = 125$ 4) $23x = 13$, $n = 812$.

5.5 Hauptsatz der elementaren Zahlentheorie.

Satz 5.7 Es sei p eine Primzahl und p ein Teiler des Produkts $a \cdot b$. Dann ist p ein Teiler von a oder p ein Teiler von b.

Beweis. Angenommen, p ist kein Teiler von a. Dann ist zu zeigen, dass p ein Teiler von b ist. Weil $\mathrm{ggT}(a, p) = 1$, gibt es Bézoutkoeffizienten x, y, sodass

$$1 = x \cdot a + y \cdot p.$$

Nach Multiplizieren dieser Gleichung mit b folgt

$$b = x \cdot (ab) + (y \cdot p) \cdot b.$$

Dann teilt b jeden Term auf der rechten Seite, also auch auf der linken Seite. ———

Mit Induktion nach s zeigt man jetzt die Aussage.

Satz 5.8 Ist p eine Primzahl und teilt p die Zahl $a_1 \cdot a_2 \cdot \ldots \cdot a_s$, so gibt es ein i mit $1 \leq i \leq s$ und p teilt a_i.

Beweis. Mit Induktion nach s. Für $s = 1$ ist nicht zu zeigen. Sonst teilt p die Zahl $a \cdot b_s$ mit $a = b_1 \cdot \ldots \cdot b_{s-1}$. Entweder p ist ein Teiler von b_s oder, nach dem vorherigen Satz, ist p ein Teiler von $b_1 \cdot \ldots \cdot b_{s-1}$. Nach Induktion ist p ein Teiler von b_i für ein $i \leq s - 1$. ———

Satz 5.9 Hauptsatz der elementaren Zahlentheorie Es sei n eine natürliche Zahl mit $n \geq 2$. Dann gibt es eindeutig bestimmte Primzahlen $p_1, p_2, \ldots, p_s$ mit

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$$

und

$$p_1 \leq p_2 \leq \cdots \leq p_s.$$

Beweis. **Existenz.** Es sei p_s die größte Primzahl kleiner oder gleich n, mit $p_s \mid n$. Dann ist n/p_s entweder gleich 1, somit $n = p_s$, oder $2 \leq n/p_s < n$. Mit Induktion gibt es Primzahlen $p_1 \leq \cdots \leq p_{s-1}$ mit $n/p_s = p_1 \cdot p_2 \cdot \ldots \cdot p_{s-1}$. Dann ist $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$.

Eindeutigkeit. Es sei $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot \ldots q_t$, mit auch q_i Primzahlen und $q_1 \leq \cdots \leq q_t$. Wir dürfen annehmen, dass p_s der größte Primteiler von n ist. Wir machen Induktion nach s. Ist $s = 1$, so ist $p_s = q_1 \cdot \ldots q_t$ und weil p_s eine Primzahl ist, folgt $t = 1$ und $p_s = q_t$.
Jetzt der Induktionsschritt. Es folgt, dass p_s das Produkt $q_1 \cdot \ldots q_t$ teilt, nach der vorherigen Bemerkung teilt p_s die Primzahl q_i für ein i. Weil p_s der größte Primteiler von n ist, folgt $p_s = q_t$. Dann folgt nach Teilung durch $p_s = q_t$, dass

$$p_1 \cdot p_2 \cdot \ldots \cdot p_{s-1} = q_1 \cdot \ldots q_{t-1}$$

Nach Induktionsvoraussetzung ist $s = t$ und $p_i = q_i$ für $i = 1, \ldots, s-1$. ———

Obwohl diese eindeutige Zerlegung von natürlichen Zahlen in einem Produkt von Primzahlen zu beweisen ist, bedeutet es in der Praxis nicht, dass sie auch leicht zu bestimmen ist. Tatsächlich ist eine rechnerisch sehr schwere Aufgabe, die Faktorisierung einer 200 oder 300 stellige Zahl zu finden. Auf diese Schwierigkeit ist das kryptographische System RSA basiert. Wir kommen hierauf zurück.

Aufgaben

Aufgabe 5.13 Es sei $\mathrm{ggT}(a, b) = 1$ und ca ein Teiler von b. Zeigen Sie, dass c ein Teiler von b ist.

5.6 Die eulersche Totientfunktion

Für eine natürliche Zahl n definieren wir

$$(\mathbb{Z}/n\mathbb{Z})^* := \{a \in \{1, \ldots, n-1 \colon \text{ggT}(a, n) = 1\}$$

und die eulersche Totientfunktion $\varphi(n)$ als die Anzahl der Elemente von $(\mathbb{Z}/n\mathbb{Z})^*$.

Satz 5.10 Es seien $p_1, \ldots, p_r$ die verschiedene Primteiler von n. Dann gilt

$$\varphi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Beweis. Sei $A_i = \{a \colon p_i \mid a \text{ und } 1 \leq a \leq n\}$. Dann ist $|A_i| = n/p_i$. Die Menge $\{1, \ldots, n\} \setminus A_1 \cup \cdots \cup A_r$ besteht aus die Zahlen in $\{1, \ldots, n\}$, welche mit n keinen gemeinsamen Teiler mit n größer als 1 haben. Nach dem Inklusions-Exklusionsprinzip hat $\{1, \ldots, n\} \setminus A_1 \cup \cdots \cup A_r$

$$n - \sum_{i=1}^{r} \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} + \cdots = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Elemente. ∎

Die eulersche Totientfunktion erfüllt deshalb folgende Identitäten:

1. Ist p eine Primzahl, so gilt $\varphi(p^k) = p^k - p^{k-1}$
2. Ist $\text{ggT}(n, m) = 1$, so gilt

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m).$$

Hiermit können wir $\varphi(n)$ berechnen, vorausgesetzt, wir können die Primzahlfaktorisierung von n bestimmen. Für große Zahlen n ist dies jedoch nicht einfach.

1. $\varphi(100) = \varphi(25) \cdot \varphi(4) = (25 - 5) \cdot (4 - 2) = 40$.
2. $\varphi(581) = \varphi(7) \cdot \varphi(83) = 6 \cdot 82 = 492$.

In SAGEMATH benutzt man `euler_phi(n)` und $\varphi(n)$ zu bestimmen. Experimentieren Sie mit SAGEMATH und stellen Sie fest, dass das Computeralgebra es selten schafft, $\varphi(n)$ für eine hunderstellige Zahl zu berechnen, wenn man die Faktorisierung von n nicht kennt. Tatsächlich versucht SAGEMATH zunächst eine Faktorisierung von n zu finden. Eine schnellere Methode ist meines Wissens nicht bekannt.
Sind $a, b \in (\mathbb{Z}/nZ)^*$, so auch $a \cdot b$. Wäre nämlich p ein Primteiler von $a \cdot b$, so gilt $p \mid a$ oder $p \mid b$. Ausserdem gilt in $(Z/n\mathbb{Z})^*$ die Kürzungsregel.

Satz 5.11 Aus $x, a, b \in (Z/nZ)^*$ mit $xa = xb \bmod n$ folg $a = b$.

Beweis. Weil $\mathrm{ggT}(x, n) = 1$ gibt es ein $y \in (\mathbb{Z}/n\mathbb{Z})^*$ mit $x \cdot y = 1 \bmod n$. Ist also $x \cdot a = x \cdot b$, so folgt nach Multiplikation von Links mit y:

$$a = (yx)a = y(xa) = y(xb) = (yx)b = b \bmod n. \qquad \blacksquare$$

Satz 5.12 (Satz von Euler) Sei $n \geq 2$ eine natürliche Zahl. Ist $\mathrm{ggT}(a, n) = 1$, so gilt $a^{\varphi(n)} = 1 \bmod n$.
(Kleiner Satz von Fermat) Ist $n = p$ eine Primzahl, so folgt $a^{p-1} = 1 \bmod p$.

Beweis. Setze $k := \varphi(n)$. Betrachte die Abbildung

$$\begin{aligned} \alpha\colon (\mathbb{Z}/n\mathbb{Z})^* &\to (\mathbb{Z}/n\mathbb{Z})^* \\ m &\mapsto a \cdot m \end{aligned}$$

Aus der Kürzungsregel folgt, dass α injektiv ist. Deshalb permutiert α die Elemente von $(\mathbb{Z}/n\mathbb{Z})^*$. Sei

$$b = \prod_{x \in (Z/n\mathbb{Z})^*} x \bmod n.$$

Dann gilt modulo n:

$$b = \prod_{x \in (\mathbb{Z}/nZ)^*} x = \prod_{x \in (\mathbb{Z}/nZ)^*} (a \cdot x) = a^{\varphi(n)} \cdot \prod_{x \in (\mathbb{Z}/nZ)^*} x = a^{\varphi(n)} \cdot b.$$

Es folgt durch Kürzung, dass $a^{\varphi(n)} = 1 \bmod n$.
Der kleine Satz von Fermat ist ein Spezialfall des Satzes von Euler. $\blacksquare$

Beispiel.

1. Wir berechnen $3^{1922} \bmod 2425$. Weil $2425 = 97 \cdot 25$ gilt $\varphi(2425) = 96 \cdot 20 = 1920$. Es folgt
$$3^{1922} \bmod 2425 = 3^{1920} \cdot 3^2 \bmod 2425 = 9 \bmod 2425.$$
2. $\varphi(15) = \varphi(3 \cdot 5) = 2 \cdot 4 = 8$, aber $3^8 = 6561 = 6 \bmod 15$. Der Satz von Euler ist demnach i.A. falsch, wenn $\mathrm{ggT}(a, n) \neq 1$.

der Satz von Euler

Aufgabe 5.14 Berechnen Sie:
1. $\varphi(145)$
2. $\varphi(1262)$
3. $\varphi(191)$
$\varphi(1233)$
4. 5. $3^{103} \bmod 101$
6. $6^{83} \bmod 79$
7. $7^{384} \bmod 884$
8. $2^{114} \bmod 145$
9. $3^{200} \bmod 303$

Aufgabe 5.15 Beweisen Sie den kleinen Satz von Fermat durch Induktion nach a.

5.7 Primzahltests

Aus dem kleinen Satz von Fermat folgt im Umkehrschluss, dass Zahlen $n \in \mathbb{N}$, $a \in \{2, \ldots, n-2\}$ mit

$$a^{n-1} \neq 1 \bmod n,$$

zusammengesetzt sind. Hierbei finden wir dann nicht notwendigerweise einen echten Teiler von n.

Fermat Test.

- EINGABE: Eine ungerade Zahl $n \geq 3$.
- AUSGABE: Nachweis, dass n zusammengesetzt ist oder eine Mitteilung, dass n wahrscheinlich eine Primzahl ist.

1. Wähle ein $a \in \{2, \ldots, n-2\}$
2. $a^{n-1} \bmod n$.
3. Ist $a^{n-1} \neq 1 \bmod n$, so ist n **nicht** prim!
4. Ist $a^{n-1} = 1 \bmod n$, so ist n **wahrscheinlich** eine Primzahl.

Um diese Berechnung durchzuführen, benutzen wir sogenanntes schnelles Potenzieren. Zunächst bemerken wird, dass wir um a^{2^s} zu berechnen, lediglich s Multiplikationen brauchen.

$$a^2 = a \cdot a,\ a^4 = a^2 \cdot a^2,\ \cdots$$

Für die Berechnung von

$$a^{101} = a^{64} \cdot a^{32} \cdot a^4 \cdot a$$

brauchen wir deshalb lediglich $6 + 3 = 9$ Multiplikation, welche wir natürlich nach jeder Multiplikation den Rest von bei Teilung durch n nehmen.
Damit man die Potenzen a^{2^i} von a nicht speichern muss benutzen wir die Zahlen $k(i) := k \bmod 2^i$. Es ist $k(1) = 0$ wenn k gerade ist und $k(1) = 1$ für k ungerade. Ist

$$k = b_n 2^n + b_{n-1} 2^{n-1} + \ldots + b_1 \cdot 2 + b_0,$$

so gilt $k(i) = b_{i-1} 2^{i-1} + \ldots + b_1 2 + b_0$ und

$$k(i+1) = \begin{cases} k(i) & \text{falls } b_i = 0 \\ 2^i + k(i) & \text{falls } b_i = 1 \end{cases}$$

und somit

$$a^{k(i+1)} = \begin{cases} a^{k(i)} \text{ falls } b_i = 0 \\ a^{k(i)} \cdot a^{2^i} \qquad \text{falls } b_i = 0 \end{cases}$$

Im Algorithmus berechnen wir somit gleichzeitig $a^{k(i)}$ und $a^{2(i)}$, letzteres durch wiederholt quadrieren. Die Bits b_i berechnet man wie im Abschnitt ?? Folgender Algorithmus setzt diese Idee um.

```
def Pot(a,k,n):   #Berechnet a^k modulo n
    s = ZZ(k); z = ZZ(a); y = 1
    while s!=0:
        if s%2 == 1:
            y *= z, y %=n
            s -= 1
        z *= z; z%=n
        s /= 2
    return y
```

Aufgaben

Aufgabe 5.16 1. Schreiben Sie ein SAGEMATH-Programm, dass die kleinste ungerade zusammengesetzte Zahl findet mit $2^{n-1} = 1 \bmod n$. Diese Zahl besteht deshalb den Fermat-Test obwohl sie keine Primzahl ist.

2. Zeigen Sie für diese Zahl, dass $3^{n-1} \neq 1 \bmod n$.

3. Finden Sie die kleinste zusammengesetzte Zahl, so dass für alle $a \in \{1, \ldots n-1\}$ mit $\mathrm{ggT}(a, n) = 1$ gilt $a^{n-1} = 1 \bmod n$.
Zahlen mit dieser Eigenschaft werden Carmichael Zahlen genannt.

Aufgabe 5.17 1. Es sei p eine (ungerade) Primzahl. Zeigen Sie, dass die Gleichung $x^2 = 1 \bmod p$ nur die Lösungen $x = \pm 1 \bmod p$ hat.

2. (Miller-Rabin-Test) Für jede ungerade Zahl schreibe $n-1 = 2^s \cdot d$ mit d ungerade. Zeigen Sie: Ist n eine Primzahl, so gilt entweder

$$a^d = 1 \bmod n$$

oder es gibt ein i mit $1 \leq i < s$, sodass

$$a^{2^i \cdot d} = -1 \bmod n.$$

3. Zeigen Sie mit dieser Methode, dass die Zahl aus dem dritten Teil der vorherigen Aufgabe keine Primzahl ist.

4. Zeigen Sie, dass die nachfolgende Zahl keine Primzahl ist.

$$963225335162084300026095186890506160954226888238586$$
$$316073628447707725561632662650907598969104164941177$$
$$542443843244622704772665133824213359104708240486161$$

5.8 Der chinesische Restsatz

Es seien eine natürliche Zahl n gegeben sowie eine Faktorisierung

$$n = n_1 \cdot n_2 \cdot \ldots \cdot n_s$$

mit $s \geq 2$ und $\mathrm{ggT}(n_i, n_j) = 1$ für $i \neq j$. Oft, aber nicht immer, sind die Zahlen n_i Primzahlen. Wir betrachten die Abbildung

$$\begin{array}{rcl} \mathbb{Z} & \stackrel{\sim}{\to} & \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z} \\ x & \mapsto & (x \bmod n_1,\, a \bmod n_2,\, \ldots,\quad x \bmod n_s) \end{array}$$

Dann wird x auf die $(0, 0, \ldots, 0)$ abgebildet, genau dann wenn $n_1 \mid x$, $n_2 \mid x, \ldots, n_s \mid x$. Weil die verschiedene n_i teilerfremd sind, folgt $n \mid x$. Werden x und y auf das gleiche Element $(c_1, c_2, \ldots, c_s)$ abgebildet, dann $n \mid (x - y)$. Wir haben den sogenannten chinesischen Restsatz gezeigt.

Satz 5.13 Ist n eine natürliche Zahl mit $n = n_1 \cdot \ldots \cdot n_s$ und $\mathrm{ggT}(n_i, n_j) = 1$ für $i \neq j$, so ist die Abbildung

$$\begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} & \stackrel{\sim}{\to} & \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z} \\ x & \mapsto & (x \bmod n_1,\, a \bmod n_2,\, \ldots,\quad x \bmod n_s) \end{array}$$

eine Bijektion.

Ist somit ein Gleichungssystem

$$\begin{array}{rcl} x & = & c_1 \bmod n_1 \\ x & = & c_2 \bmod n_2 \\ & \vdots & \\ x & = & c_s \bmod n_s \end{array}$$

so gibt es einen eindeutig bestimmte Lösung $x \in \mathbb{N}$ mit $0 \leq x < n$.

Im obigen Beweis wurde die Existenz der Lösung gezeigt, jedoch wurde nicht angegeben, wie man diese Lösung findet. Dazu wenden wir uns jetzt. Dazu betrachten wir erst als Spezialfall das Gleichungssystem

$$x = 1 \bmod n_i \;\; x = 0 \bmod n_j \text{ für } j \neq i.$$

mit Lösung e_i. Haben wir das erreicht, so ist unsere Lösung

$$x = c_1 e_1 + \ldots + c_s e_s \bmod n.$$

Um die Lösung e_i zu finden, betrachten wir $\widehat{n}_i := \prod_{j \neq i} n_j = \frac{n}{n_i}$. Weil $\widehat{n}_i$ und n_i keinen gemeinsamen Teiler haben, können wir mit dem erweiterten euklidischen Algorithmus a_i und b_i finden, so dass

$$1 = a_i \cdot \widehat{n}_i + b_i \cdot n_i.$$

Sei $e_i := a_i \cdot \widehat{n}_i$ Diese Gleichung besagt, dass

$$e_i = \begin{cases} 1 \bmod n_j & \text{für } i = j \\ 0 \bmod n_j & \text{sonst.} \end{cases}$$

Bespiel. $n = 1001 = 7 \cdot 11 \cdot 13$. Dann gilt

i	n_i	$\widehat{n}_i$	a_i	e_i
1	7	143	-2	-286
2	11	91	4	364
3	13	77	-1	-77

wobei die a_i mit dem erweiterten euklidischen Algorithmus berechnet wurden.
Für $x = 3 \bmod 7$, $x = 7 \bmod 11$ und $x = 11 \bmod 13$ gilt somit

$$x = 3 \cdot (-286) + 7 \cdot 364 + 11 \cdot (-77) = 843.$$

Im diesen Fall ist $0 \leq x < n$, aber das muss nicht immer sein. Oft muss noch Teilung mit Rest durchgeführt werden.

Aufgaben

Aufgabe 5.18 Schreiben Sie ein SAGEMATH-Programm `CRS(c,N)`, das diesen chinesischen Restssatzes umsetzt. Hierbei ist N eine liste von Zahlen $n_1, \ldots, n_s$ und c eine Liste von Zahlen $c_1, \ldots, c_s$.
Bemerkung: in SAGEMATH ist der chinesische Restsatz implementiert.

Aufgabe 5.19 Lösen die nachfolgenden Gleichungen

1. $0 \leq x < 232,\ x = 5 \bmod 11,\ x = 8 \bmod 21$
2. $0 \leq x < 1001,\ x = 23 \bmod 13,\ x = 31 \bmod 77$
3. $0 \leq x < 1763,\ x = 16 \bmod 41,\ x = 11 \bmod 43$
4. $0 \leq x < 1053,\ x = 22 \bmod 27,\ x = 16 \bmod 39$

5.9 RSA

Um geheime Nachrichten zu entschlüsseln braucht man einen Schlüssel, in unserem Fall ein Geheimnis. In der RSA Verschlüsselung macht jede Person, welche eine geheime Nachricht empfangen möchte, sein eigenes Geheimnis folgendermaßen.

1. Bestimme zwei verschiedene große Primzahlen p und q zum Beispiel mit dem
2. Bilde $n = p \cdot q$.
3. Öffentlich: n
4. Das Geheimnis: Kenntnis von p und q.

Mithilfe von p und q kann man $\varphi(n) = (p-1)\cdot(q-1)$ bestimmen. Weiterhin wird eine Zufallszahl e zwischen kleiner als n gewählt. Nur der Empfänger ist in der Praxis in der Lage die Zahl d zu bestimmen, sodass $d \cdot e = 1 \bmod \varphi(n)$. Hier wird der erweiterten euklidischen Algorithmus benutzt. Die Zahl e ist nicht geheim und wird von einem Sender benutzt, um die Nachricht zu verschlüsseln, wie wir jetzt erklären werden.
Wir wandeln zunächst die Nachricht in eine Zahl um. An diese Umwandlung ist nichts geheimes daran. Man hat eine endliche Menge von Buchstaben

$$\text{Buchstbaben} = \{' \ ', b_1, \ldots, b_s\} = \{' \ ', a, b, c, \ldots z, A, B, C, \ldots, Z, ., \ldots, ??\}$$

Der erste Buchstabe ist das Leerzeichen und der letzte Buchstabe '??' ist eingebaut um abzufangen das ein Zeichen im Text nicht vorkommt in meinem Alphabet. Im unserem Beispiel nehmen wir $s = 127$, sodass wir 128 Zeichen zur Verfügung haben für unsere Nachrichtentext. Ein Text ist eine Folge von Buchstaben, wobei Leerzeichen, Sonderzeichen usw auch als Buchstaben betrachtet werden. Der Text

"Dieser Affe ist schlau."

korrespondiert mit der Zeichenkette

$$b_{30}b_9b_5b_{19}b_5b_{18}b_0b_{27}b_6b_6b_5b_0b_9b_{19}b_{20}b_0b_{19}b_3b_8b_{12}b_1b_{21}b_{53}$$

Das sind 23 Zeichen. Wir definieren nun die Zahl:

$$\begin{aligned} Z &= 30 \cdot 128^{22} + 9 \cdot 128^{21} + 5 \cdot 128^{20} + \ldots + 21 \cdot 128 + 53 \\ &= 800871537881502677613028091824676861570784971419 \end{aligned}$$

Weil in dem Rechner Zahlen in Binärdarstellung speicher können, ist hierfür überhaupt keine Berechnung nötig. Auf diese Weise kann man also jedem Text eine Zahl zuordnen und aus dieser Zahl lässt sich der Text wieder herleiten.

Eine Nachricht ist für uns deshalb nichts anderes als eine Zahl Z. Wir verschluesseln diese Zahl Z mit Mathematik.Wie oben erklärt, hat der Empfänger zwei Zahlen n und

e bestimmt. Diese Zahlen sind öffentlich verfügbar und nicht geheim und vor allem n ist groß. Zum Beispiel steht das Paar (n, e) auf der Website des Empfängers.
Statt den Bericht Z zu senden, versendet man die Verschlüsselung

$$Z_{\text{geheim}} := Z^e \bmod n.$$

Um in der Praxis die Nachricht zu entschlüsseln, also die ursprüngliche Nachricht Z wieder zu erhalten, benutzt man die Zahl d mit $d \cdot e = 1 \bmod \varphi(n)$. Dann gilt $d \cdot e = q\varphi(n) + 1$ und nach dem Satz von Euler

$$Z^d_{\text{geheim}} = (Z^e)^d = (Z^{\varphi(n)})^q \cdot Z = Z.$$

Somit erhält der Empfänger die Zahl Z zurück, welche man dan einfach in den gewöhnlichen Textnachricht umwandeln kann.
In unserem Fall nehmen wir $n \approx 10^{616} \approx 2^{2000}$. Mit 7 Bits pro Buchstabe ist die maximale Anzahl der Buchstaben in etwa 290. Ist die Nachricht größer, so sollte diese in Einzelteile zerlegt werden. Probieren Sie einfach mal eine zu lange Text aus.

Padding oder Auffüllen. Man sollte das obige Verfahren allerdings nicht benutzen um kleine Nachrichten zu verschicken. Nehmen wir das Beispiel von Pincodes. Davon gibt es ingesammt 10^4 Stück. Ein Bösewicht, Catherine, könnte schlicht und einfach für alle mögliche Pincodes die Verschlüsselung berechnen und vergleichen mit dem eingetroffenen Bericht. Zum Beispiel hört Catherine folgende Zahl ab (mit dem öffentlichen Verschlüsselungsdaten (n, e) wie oben und dem Programm.

$$Z_{geheim} = 207048302240297419170893990160929766000252563845739310505685017352215408345986840418228834032$$

Wenn Catherine vermutet, dass hier nur ein Pincode verschluesselt ist, kann sie diesen ohne f zu kennen mit dem folgendem Programm finden.

```
for i in range(10^4):
    Text = str(i)
    if i < 1000:
       Text = '0'+Text
    if i < 100:
       Text = '0'+Text
    if i < 10:
       Text = '0'+Text
    ZZ = Verschluessel(Text)
    if ZZ == Zgeheim:
       print(i)
       break
```

Um eine solche Attacke zu verhindern, halbieren wir die mögliche Textlänge und füllen auf (englisch: padding) mit einer Zufallszahl von 1000 Bits, die wir bei der Entschluesselung wieder entfernen. Es gibt bessere Auffülmethoden als die oben genannte z.B. OAEP (Optimal Asymmetric Encryption Padding), aber dann kommt man wirklich zu weit weg von der wirklichen Mathematik.

Kapitel 6

Die reellen Zahlen

6.1 Existenz nichtrationaler Zahlen

Auf der Zahlengeraden haben wir nun die natürlichen, die ganzen und die rationalen Zahlen identifiziert. Die Zahlengerade besitzt aber unendlich viel mehr Punkte, welche keiner rationalen Zahl zugeordnet werden können. Trägt man beispielsweise die Länge der Diagonalen des Einheitsquadrates vom Nullpunkt der Zahlengeraden ab, so kommt ihr Ende auf einem Punkt zu liegen, der keiner rationalen Zahl entspricht.

Wir formulieren und beweisen diese Tatsache rein analytisch.

Satz 6.1: Es existiert kein $x \in \mathbb{Q}$ mit der Eigenschaft $x^2 = 2$.

Beweis. Angenommen, $x \in \mathbb{Q}$ erfüllt $x^2 = 2$. Dann existieren $p \in \mathbb{Z}$ und $q \in \mathbb{N}$ mit $q > 0$, so dass $x = \frac{p}{q}$. Dabei wählen wir p und q nicht beide gerade sind, denn sonst kürzen wir gemeinsamen Teiler 2 heraus. Es folgt

$$2 = x^2 = \frac{p^2}{q^2} \quad \text{bzw.} \quad p^2 = 2q^2 \,.$$

Es ist also p^2 eine gerade Zahl und damit auch p selbst, etwa $p = 2m$ mit $m \in \mathbb{Z}$ geeignet. Es folgen

$$p^2 = (2m)^2 = 4m^2 \quad \text{und} \quad p^2 = 2q^2 \,, \quad \text{also} \quad q^2 = 2m^2 \,,$$

weshalb auch q^2 und damit q gerade sind. Es besitzen also p und q den gemeinsamen Teiler 2 im Widerspruch zur Voraussetzung der Teilerfremdheit. ∎

Bemerkung. Wir können die Voraussetzung „beide nicht gerade“ ersetzen durch „teilerfremd“, wenn sicher ist, dass sich Zähler und Nenner überhaupt stets in geeignete Faktoren zerlegen lassen. Hierzu können wir den *Hauptsatz der elementaren Zahlentheorie* heranziehen, nach dem sich jede natürliche Zahl als Produkt endlich vieler Primzahlen darstellen lässt. Primzahlen sind natürliche Zahlen größer als 1, die nur durch sich selbst und durch 1 ohne Rest teilbar sind, also 2, 3, 5, 7, 11, 13, 17, 19, 23 usw. Beispielsweise gilt

$$132 = 2 \cdot 2 \cdot 3 \cdot 11.$$

Eine solche Darstellung als Primzahlprodukt ist eindeutig, wenn man die Faktoren der Größe nach anordnet. Wir kommen hierauf in Kapitel 5 zurück.

Aufgaben

Aufgabe 6.1 ($\sqrt{3}$ ist nicht rational)
Beweisen Sie, dass es keine rationale Zahl $x \in \mathbb{Q}$ gibt mit $x^2 = 3$.

6.2 Die reellen Zahlen

Reelle Zahlen führen wir als unendliche Dezimalzahlen ein.

Eine *reelle Zahl* ist ein Ausdruck $+x$ oder $-x$ der Form

$$x = \dots x_{k+1}x_k x_{k-1} \dots x_1 x_0 \,.\, x_{-1}x_{-2}x_{-3} \dots$$
$$\text{mit} \quad x_k \in \{0, 1, 2, \dots, 9\}\,, \quad k \in \mathbb{Z},$$

i.Z. auch $x = (x_k)_{k\in\mathbb{Z}}$, so dass folgende Eigenschaften erfüllt sind:

1. Es existiert ein $n \in \mathbb{N}$ mit $0 = x_{n+1} = x_{n+2} = x_{n+3} = \dots$
2. Es existiert kein $\ell \in \mathbb{N}$ mit $9 = x_{-\ell} = x_{-\ell-1} = x_{-\ell-2} = \dots$.

Die Menge der reellen Zahlen bezeichnen wir mit $\mathbb{R}$.

Man bezeichnet $x_0, x_1, \dots, x_n$ auch als die *Vorkommastellen* und $x_{-1}, x_{-2}, \dots$ als die *Nachkommastellen* bzw. *Dezimalstellen* der Zahl x.

Bemerkungen.

(i) Ausdrücke der Form $3.499999\dots$ oder $-0.199999\dots$ sind in unserer Methode ausgeschlossen, was wir später genauer erläutern. Andere Ansätze identifizieren solche Dezimalzahlen nach Definition oder durch einen Satz.

(ii) Eine ganze Zahl $m \in \mathbb{Z}$ fassen wir als eine reelle Zahl mit verschwindenden Nachkommastellen auf. Die Dezimaldarstellung der natürlichen Zahl $n = 2$ lautet so beispielsweise $2.000\dots$ mit der Vorkommastelle 2.

(iii) Dezimaldarstellungen rationaler Zahlen diskutieren wir in den untenstehenden Aufgaben.

Zwei reelle Zahlen $x = \dots x_n x_{n-1} \dots$ und $y = \dots y_n y_{n-1} \dots$ heißen *gleich,* i.Z. $x = y$, falls gilt

$$x_k = y_k \quad \text{für alle } k \in \mathbb{Z}.$$

Ist $x_k = 0$ für alle $k \in \mathbb{Z}$, so schreiben wir $+x = -x =: 0$. Insbesondere ist $+0 = -0$. Desweiteren vereinbaren wir $-(+x) := -x$ und $-(-x) := x$. Im Fall $x \neq 0$ heißt die Zahl $+x$ *positiv,* i.Z. $x > 0$, die Zahl $-x$ *negativ,* also $x < 0$. Statt $+x$ schreiben wir kurz x, und $x \geq 0$ bedeutet $x > 0$ oder $x = 0$. Entsprechend verstehen wir $<$ und $\leq$.

Beispiel. Die Eulersche Zahl $2.718281828\dots$ und die Kreiszahl $3.141592653\dots$ sind Beispiele positiver reeller Zahlen.

Es sei $x \in \mathbb{R}$. Dann definieren wir ihren *Betrag* vermöge

$$|x| := \begin{cases} x, & \text{falls } x \geq 0 \\ -x, & \text{falls } x < 0 \end{cases}.$$

Offenbar gilt $|x| \geq 0$ für alle $x \in \mathbb{R}$.

Aufgaben

Aufgabe 6.2 (Dezimaldarstellung rationaler Zahlen)

In dieser Aufgabe werden wir jeder - hier: positiven - rationalen Zahl eine reelle Zahl zuordnen. Es seien $a, b \in \mathbb{N}$.

(i) Zeigen Sie induktiv, dass es Zahlen $q, r \in \mathbb{N}$ gibt mit

$$a = q \cdot b + r, \quad \text{wobei } r \in \{0, 1, \ldots, b-1\}.$$

(ii) Zeigen Sie, dass q und r aus (i) eindeutig durch a und b bestimmt sind.

Die Dezimalentwicklung von q ergibt bereits die Vorkommastellen von $\frac{a}{b}$.

Zur Bestimmung der weiteren Stellen nehmen wir $a < b$ an. Setze $x_k := 0$ für $k \geq 0$ sowie $y_0 := a$. Wie in (i) bestimmen wir nun sukzessive Zahlen $x_{-k} \in \{0, 1, \ldots, 9\}$ und $y_{-k} \in \{0, \ldots, b-1\}$ aus

$$\begin{aligned} 10y_0 &= x_{-1}b + y_{-1} \\ 10y_{-1} &= x_{-2}b + y_{-2} \\ &\vdots \\ 10y_{-k+1} &= x_{-k}b + y_{-k} \qquad \text{usw.} \end{aligned}$$

Die Dezimalentwicklung des Bruches $\frac{a}{b}$ ergibt sich dann zu $x_0 \,.\, x_{-1}x_{-2}\ldots$

(iii) Ermitteln Sie die Dezimalentwicklungen von $\frac{1}{2}$, $\frac{1}{3}$, $\frac{3}{5}$ und $\frac{1}{3}$, $\frac{1}{7}$, $\frac{5}{7}$.

(iv) Warum sind diese Entwicklung endlich oder periodisch?

(v) Bestimmen Sie die Entwicklungen von $\frac{1}{9}$, $\frac{1}{99}$, $\frac{1}{999}$. Erläutern Sie.

(vi) Bestimmen Sie nun die rationalen Zahlen zu den Dezimalentwicklungen

- 0.25
- 0.7341
- $0.\overline{4} = 0.444\ldots$
- $0,\overline{123} = 0.123123123\ldots$
- $0.0\overline{123} = 0.0123123123\ldots$

(vii) Weshalb bestimmen endliche oder periodische Dezimalentwicklungen stets rationale Zahlen?

Aufgabe 6.3 (Dezimalentwicklungen in SageMath)

Schreiben Sie in SageMath ein Programm, dass die Dezimalentwicklung einer positiven rationalen Zahl berechnet. Im Fall nicht endlicher Entwicklungen soll zusätzlich der periodische Anteil ausgegeben werden.

6.3 Ordnungsstruktur der reellen Zahlen

Wir führen nun eine Ordnungsstruktur auf den reellen Zahlen ein.

Seien $x = (x_k)_{k\in\mathbb{Z}}$, $y = (y_k)_{k\in\mathbb{Z}}$ reelle Zahlen. Wir schreiben $x < y$, falls

- $x < 0$ und $y \geq 0$,
- $x, y \geq 0$ und $x_k < y_k$ für das größte $k \in \mathbb{Z}$ mit $x_k \neq y_k$,
- oder $x, y < 0$ und $-y < -x$.

Ferner bedeutet $x \leq y$, dass entweder $x < y$ oder $x = y$. Entsprechend sind $>$ und $\geq$ zu verstehen.

Die Relation $\leq$ ist reflexiv, antisymmetrisch, transitiv und total, siehe hierzu Abschnitt 3.1. Die Relation $<$ ist ebenfalls transitiv, erfüllt aber auch folgende *Trichotomieeigenschaft:*

- Für alle $x, y \in \mathbb{R}$ gilt $x = y$, $x > y$ oder $x < y$.

Sei nun $x = (x_k)_{k\in\mathbb{Z}}$. Für $n, \ell \in \mathbb{N}$ definieren im Fall $x \geq 0$ die

$$\begin{aligned} &\textit{ℓ-te Abrundefunktion} && \lfloor x\rfloor_\ell := \dots x_n \dots x_0, x_{-1} \dots x_{-\ell}\, 0\, 0\, 0 \dots , \\ &\textit{ℓ-te Aufrundefunktion} && \lceil x\rceil_\ell := \begin{cases} x, & \text{falls } x = \lfloor x\rfloor_\ell \\ \lfloor x\rfloor_\ell + 10^{-\ell} & \text{sonst} \end{cases} \end{aligned}$$

und diese Funktionen setzen wir für Zahlen $x < 0$ wie folgt fort

$$\lfloor x\rfloor_\ell := -\lceil -x\rceil_\ell\,, \quad \lceil x\rceil_\ell := -\lfloor -x\rfloor_\ell\,.$$

Die abgeschnittenen Nachkommastellen $x_{-k} = 0$ für $k > \ell$ werden wir häufig unterdrücken. Der Ausdruck $\lfloor x\rfloor_0$ bedeutet die sogenannte *Gaußklammer* $\lfloor x\rfloor$.

Beispiel. Für $x = 1,24374158\dots$ und $y = 1,24374997$ ermitteln wir

$$\begin{aligned} \lfloor x\rfloor_7 &= 1,2437415, \quad & \lceil x\rceil_7 &= 1,2437415 + 10^{-7} = 1,2437416, \\ \lfloor y\rfloor_7 &= 1,2437499, \quad & \lceil y\rceil_7 &= 1,2437499 + 10^{-7} = 1,2437500. \end{aligned}$$

In diesem Beispiel gilt $x \leq \lceil x\rceil_7 < \lfloor y\rfloor_7 \leq y$, und mit $z = 1,2437427$ ist sogar $x \leq \lceil x\rceil_7 < z < \lfloor y\rfloor_7 \leq y$. Das gilt auch allgemein, vgl. de Jong [**?**], Satz 1.2:

Satz 6.2: Es seien $x, y \in \mathbb{R}$ mit $x < y$. Dann existieren ein $\ell \in \mathbb{N}$ und ein $z \in \mathbb{R}$ mit

$$x \leq \lceil x\rceil_\ell < z < \lfloor y\rfloor_\ell \leq y.$$

Beachte, dass eine solche Aussage für die beiden Dezimalzahlen $x = 0.999\dots$ und $y = 1.000$ falsch wäre, was den Ausschluss von auf $999\dots$ endende Zahlen bereits begründet.

Aufgaben

Aufgabe 6.4 (Eigenschaften der $\leq$-Relation)
Beweisen Sie: Die Relation $\leq$ ist reflexiv, antisymmetrisch, transitiv und total.

Aufgabe 6.5 (Abrunden und Aufrunden)
Berechnen Sie $\lfloor x \rfloor_4$ und $\lceil x \rceil_4$ in den nachfolgenden Fällen.

a) $x = 1,23456\cdots$ b) $x = 3,99999\cdots$
c) $x = -0,23789\cdots$ d) $x = 12,34$

Aufgabe 6.6 (Eigenschaften der Auf- und Abrundefunktion)
Es sei $\ell \in \mathbb{N}$. Beweisen Sie, dass für alle $x \in \mathbb{R}$ gelten:

a) $\lceil x \rceil_\ell + \lfloor -x \rfloor_\ell = 0$ b) $\lfloor x \rfloor_\ell \leq x \leq \lfloor x \rfloor_\ell + 10^{-\ell}$
c) $\lceil x \rceil_\ell - 10^{-\ell} \leq x \leq \lceil x \rceil_\ell$

Ist ferner $m \in \mathbb{Z}$, so gilt

(iv) $\left\lfloor \frac{m}{2} \right\rfloor_\ell + \left\lceil \frac{m}{2} \right\rceil_\ell = m$

Aufgabe 6.7 (Die Menge $10^{-k}\mathbb{Z}$)
Wir definieren $10^{-k}\mathbb{Z} = \{x \in \mathbb{R} \colon x = \lfloor x \rfloor_k\}$.

(i) Zeigen Sie, dass $x \in 10^{-k}\mathbb{Z}$ genau dann, wenn $x = \frac{a}{10^k}$ mit $a \in \mathbb{Z}$.

(ii) Es sei $x \in \mathbb{R}$. Zeigen Sie, dass

$$\lfloor x \rfloor_k = \max\left\{a \in 10^{-k}\mathbb{Z} \colon a \leq x\right\} .$$

(iii) Formulieren und beweisen Sie eine analoge Aussage für $\lceil x \rceil_k$.

Aufgabe 6.8 (Monotonie der Abrunde- und Aufrundefunktion)
Sei $x \in \mathbb{R}$. Weshalb gelten

$$\lfloor x \rfloor_0 \leq \lfloor x \rfloor_1 \leq \lfloor x \rfloor_2 \leq \cdots \leq x \quad \text{und} \quad x \leq \cdots \leq \lceil x \rceil_2 \leq \lfloor x \rfloor_1 \leq \lceil x \rceil_0 \,?$$

Aufgabe 6.9 (Auf- und Abrundefunktion und SageMath)
Schreiben Sie jeweils eine SageMath-Routine `fl(x,k)` und `ce(x,k)` zur Berechnung von $\lfloor x \rfloor_k$ bzw. $\lceil x \rceil_k$.

Aufgabe 6.10 (Beweis des Satzes)
Beweisen Sie Satz 6.3.

Aufgabe 6.11 (Charakterisierung der Betragsfunktion)
Es sei $a > 0$ reell. Beweisen Sie, dass $|x| \leq a$ genau dann, wenn $-a \leq x \leq a$.

6.4 Reelle Zahlenfolgen und Konvergenz

Unter einer *reellen Zahlenfolge* verstehen wir eine Abbildung $\mathbb{N} \ni n \mapsto x_n \in \mathbb{R}$. Wir schreiben $\{x_n\}_{n=0,1,2,\ldots} \subset \mathbb{R}$.

Es heißt $x \in \mathbb{R}$ *Grenzwert* der Zahlenfolge $\{x_n\}_{n=0,1,2,\ldots} \subset \mathbb{R}$ genau dann, wenn zu beliebig gewählten $a, b \in \mathbb{R}$ mit $a < x < b$ ein $N(a,b) \in \mathbb{N}$ existiert mit

$$a < x_n < b \quad \text{für alle } n \geq N(a,b).$$

Wir sagen auch: $a < x_n < b$ gilt für *fast alle* $n \in \mathbb{N}$, und das bedeutet für alle n bis auf endlich viele. So wollen wir jetzt auch argumentieren:

Satz 6.3: Der Grenzwert einer reellen Zahlenfolge ist eindeutig.

Beweis. Angenommen, $x < x^*$ seien zwei verschiedene Grenzwerte der Folge $\{x_n\}_{n=0,1,2,\ldots}$. Es gibt $a, b^* \in \mathbb{R}$ mit $a < x$ und $x^* < b$, und nach Satz 6.3 auch ein $b \in \mathbb{R}$ mit $x < b < x^*$ und ein $a^* \in \mathbb{R}$ mit $b < a^* < x^*$, also

$$a < x < b < a^* < x^* < b^* .$$

Es folgen $a < x_n < b$ und $a^* < x_n < b^*$ für fast alle $n \in \mathbb{N}$ und damit $x_n < x_n$ für fast alle $n \in \mathbb{N}$ wegen $b < a^*$. Widerspruch. ∎

Diese Eindeutigkeit des Grenzwertes $x \in \mathbb{R}$ berechtigt uns zu der Sprechweise, die Zahlenfolge $\{x_n\}_{n=0,1,2,\ldots}$ *konvergiert gegen* $x \in \mathbb{R}$, in Zeichen

$$\lim_{n\to\infty} x_n = x \quad \text{oder} \quad x_n \to x \text{ für } n \to \infty .$$

Eine Folge mit Grenzwert $x = 0$ heißt eine *Nullfolge,* und eine nicht konvergente Folge bezeichnet man als *divergent.*

Satz 6.4: Es sei $x \in \mathbb{R}$ eine reelle Zahl. Dann gilt

$$\lim_{n\to\infty} \lfloor x \rfloor_n = x = \lim_{n\to\infty} \lceil x \rceil_n .$$

Beweis. Nehme $x > 0$ an, und wähle $a, b > 0$ mit $a < x < b$. Nach Anwendung von Satz 6.3 existieren dann $\ell, \ell^* \in \mathbb{N}$ mit $a < \lfloor x \rfloor_\ell \leq x$ und $x \leq \lceil x \rceil_{\ell^*} < b$. Wegen $\lfloor x \rfloor_m \leq \lfloor x \rfloor_n \leq x$ und $x \geq \lceil x \rceil_m \geq \lceil x \rceil_n$ für $m \leq n$ folgen

$$a < \lfloor x \rfloor_n < b, \quad a < \lceil x \rceil_n < b \quad \text{für alle } n \geq M := \max\{\ell, \ell^*\} .$$

Also konvergieren $\{\lfloor x \rfloor_n\}_{n=0,1,2,\ldots}$ und $\{\lceil x \rceil\}_{n=0,1,2,\ldots}$ gegen x. ∎

Aufgaben

Aufgabe 6.12 (Abschätzen von Grenzwerten)
Beweisen Sie: Ist $\lim\limits_{n\to\infty} x_n = x$ und $\lim\limits_{n\to\infty} y_n = y$ mit $x_n \leq y_n$ für fast alle $n \in \mathbb{N}$, so ist auch $x \leq y$.

Aufgabe 6.13 (Beschränktheit konvergenter Zahlenfolgen)
Beweisen Sie: Konvergiert $\{x_n\}_{n=0,1,2,\ldots} \subset \mathbb{R}$, so existiert ein $C \in \mathbb{R}$ mit

$$|x_n| \leq C \quad \text{für alle } n = 0, 1, 2, \ldots$$

Aufgabe 6.14 (Einschließungssatz)
Die reellen Zahlenfolgen $\{x_n\}_{n=0,1,2,\ldots}$, $\{y_n\}_{n=0,1,2,\ldots}$ und $\{z_n\}_{n=0,1,2,\ldots}$ genügen

$$x_n \leq y_n \leq z_n \quad \text{für fast alle } n \in \mathbb{N}.$$

Ferner konvergieren $\{x_n\}_{n=0,1,2,\ldots}$ und $\{z_n\}_{n=0,1,2,\ldots}$ gegen den einen Grenzwert $a \in \mathbb{R}$. Beweisen Sie, dass dann auch $\{y_n\}_{n=0,1,2,\ldots}$ gegen a konvergiert.

Aufgabe 6.15 (Ermitteln von Grenzwerten)
Beweisen Sie unter Verwendung von Aufgabe 3.9.5, dass nachstehende Zahlenfolgen konvergieren, und bestimmen Sie deren Grenzwerte.

a) $\left\{\frac{1}{n}\right\}_{n=1,2,\ldots}$ b) $\left\{\frac{1}{n^2}\right\}_{n=1,2,\ldots}$ c) $\left\{\frac{1}{n^3-1}\right\}_{n=2,3,\ldots}$

d) $\left\{\frac{n+3}{5n-2}\right\}_{n=1,2,\ldots}$ e) $\left\{\frac{3n}{1+n^2}\right\}_{n=1,2,\ldots}$ f) $\left\{\frac{n^2+1}{n^5}\right\}_{n=1,2,\ldots}$

Unter SageMath lassen sich solche Grenzwerte wie folgt bestimmen:

```
var = ('n')
term = 1/n
term.limit(n=oo)
```

Aufgabe 6.16 (Grenzwerte und SageMath)
Ermitteln Sie die Grenzwerte aus Aufgabe 4.3.5 mittels SageMath.

Aufgabe 6.17 (Aufstellen expliziter Summenausdrücke)
Es sei $n \in \mathbb{N}_+$, $n \geq 2$. Bestimmen Sie einen expliziten Ausdruck für die Summe

$$S_n := \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \ldots + \frac{1}{(n-1)\cdot n}$$

Liegt für $n \to \infty$ Konvergenz vor? Bestimmen Sie ggf. den Grenzwert analytisch sowie unter Verwendung von SageMath.

6.5 $\mathbb{R}$ als angeordneter Körper

Unter Verwendung der Addition und die Multiplikation rationaler Zahlen sowie unter Beachtung des untenstehenden Vollständigkeitssatzes führen wir nun die Addition und die Multiplikation zwischen reellen Zahlen ein.

Für $x, y \in \mathbb{R}$ definieren wir die *Addition* $+_{\mathbb{R}} \colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ vermöge

$$x +_{\mathbb{R}} y := \lim_{n\to\infty} (\lfloor x \rfloor_n + \lfloor x \rfloor_n).$$

Sind ferner $x, y \geq 0$, so definieren wir die *Multiplikation* $\cdot_{\mathbb{R}} \colon \mathbb{R} \times \mathbb{R}$ vermöge

$$x \cdot_{\mathbb{R}} y := \lim_{n\to\infty} \lfloor x \rfloor_n \cdot \lfloor y \rfloor_n .$$

Die Multiplikation setzen wir auf ganz $\mathbb{R}$ wie folgt fort

$$(-x) \cdot_{\mathbb{R}} y := -(x \cdot_{\mathbb{R}} y), \quad x \cdot_{\mathbb{R}} (-y) := -(x \cdot_{\mathbb{R}} y), \quad (-x) \cdot_{\mathbb{R}} (-y) := x \cdot_{\mathbb{R}} y.$$

Es ist $\mathbb{R}$ mit dieser Addition und Multiplikation ein Körper, siehe Abschnitt 3.9. Das neutrale Element der Addition ist die ganze Zahl $0 \in \mathbb{Z}$, das der Multiplikation die Zahl $1 \in \mathbb{Z}$; die multiplikative Inverse betrachten wir im folgenden Abschnitt genauer. Zudem gelten (wir schreiben wieder $+$ und $\cdot$)

$$0 \cdot x = 0, \quad (-1) \cdot x = -x \quad \text{für alle } x \in \mathbb{R},$$

als auch die Kürzungsregeln für die Addition und die Multiplikation. Ferner ist $\mathbb{R}$ archimedisch angeordnet, und die Relation $\leq$ genügt folgenden Eigenschaften:

(i) Aus $x \leq y$ und $u \leq v$ folgt $x + u \leq y + v$.
(ii) Aus $x \leq y$ und $0 \leq z$ folgt $x \cdot z \leq y \cdot z$.

Schließlich ist $\mathbb{R}$ *vollständig* im folgenden Sinn:

Satz 6.5: Ist $\{x_n\}_{n=0,1,2,\ldots} \subset \mathbb{R}$ eine beschränkte und monoton wachsende Zahlenfolge, d.h. gilt

$$x_0 \leq x_1 \leq x_2 \leq x_3 \leq \ldots \leq C$$

mit einem $C \in \mathbb{R}$, so ist die Folge konvergent gegen ein $x \in \mathbb{R}$.

Für einen Beweis dieses Satzes, der wegen der Monotonie der Abrunde- und Aufrundefunktion obige Definitionen von Addition und Multiplikation ermöglicht, verweisen wir auf [**?**], Abschnitt 1.3.

Beispiel. Die beschränkte und monoton wachsende Zahlenfolge $x_0 = 0$, $x_1 = 0,9$, $x_2 = 0,99$, $x_3 = 0,999$ usw. konvergiert gegen die reelle Zahl $1 \in \mathbb{R}$.

Aufgaben

Aufgabe 6.18 (Kommutativität)
Formulieren und beweisen Sie das Kommutativgesetz der Addition und der Multiplikation.

Aufgabe 6.19 (Assoziativität)
Formulieren und beweisen Sie das Assoziativgesetz der Addition und der Multiplikation. Verwenden Sie dazu den späteren Satz 6.6.

Aufgabe 6.20 (Distributivität)
Formulieren und beweisen Sie das Distributivgesetz. Verwenden Sie dazu den späteren Satz 6.6.

Aufgabe 6.21 (Betrag von Produkten)
Beweisen Sie die Identität $|x \cdot y| = |x| \cdot |y|$ für alle $x, y \in \mathbb{R}$.

Aufgabe 6.22 (Dreiecksungleichung für die Betragsfunktion)
Beweisen Sie die Ungleichung $|x + y| \leq |x| + |y|$ für alle $x, y \in \mathbb{R}$.

Aufgabe 6.23 (Verallgemeinerte Dreiecksungleichung)
Beweisen Sie: Ist $n \in \mathbb{N}_+$, und sind $x_i \in \mathbb{R}$ für $i = 1, \ldots, n$, so gilt

$$\left| \sum_{i=1}^{n} x_i \right| \leq \sum_{i=1}^{n} |x_i|.$$

Aufgabe 6.24 (Inverse Dreiecksungleichung für die Betragsfunktion)
Beweisen Sie die Ungleichung $||x| - |y|| \leq |x - y|$ für alle $x, y \in \mathbb{R}$.

Aufgabe 6.25 (Produkte beschränkter Zahlentripel)

(i) Zeigen Sie $xy \leq \frac{1}{2} x^2 + \frac{1}{2} y^2$ für alle $x, y \in \mathbb{R}$.

(ii) Es seien nun $a, b, c, x, y, z \in \mathbb{R}$ reelle Zahlen mit $a^2+b^2+c^2 \leq 1$ und $x^2+y^2+z^2 \leq 1$. Beweisen Sie, dass dann gilt

$$|ax + by + cz| \leq 1.$$

Aufgabe 6.26 (Differenzfolgen)
Es seien $\{x_n\}_{n=0,1,2,\ldots}$ und $\{y_n\}_{n=0,1,2,\ldots}$ zwei konvergente Zahlenfolgen mit dem gemeinsamen Grenzwert $z \in \mathbb{R}$. Beweisen Sie, dass dann die Differenzfolge $\{x_n - y_n\}_{n=0,1,2,\ldots}$ eine Nullfolge ist.

6.6 Der Kehrwert

Zunächst benötigen wir folgende Eigenschaften konvergenter Zahlenfolgen, für deren Beweis wir auf [**?**], Abschnitt 1.4 verweisen.

Satz 6.6: Es seien $\{x_n\}_{n=0,1,2,\ldots}$ und $\{y_n\}_{n=0,1,2,\ldots}$ zwei konvergente reelle Zahlenfolgen mit Grenzwerten

$$x := \lim_{n\to\infty} x_n\,, \quad y := \lim_{n\to\infty} y_n\,.$$

Dann gelten:

a) $\lim_{n\to\infty}(x_n + y_n) = x + y$ b) $\lim_{n\to\infty}(x_n \cdot y_n) = x \cdot y$

Damit kommen wir zum Hauptresultat dieses Abschnittes.

Satz 6.7: Zu jeder reellen Zahl $x \neq 0$ existiert genau ein $y \in \mathbb{R} \setminus \{0\}$ mit der Eigenschaft $x \cdot y = 1$.

Für dieses y schreiben wir auch $y = x^{-1}$ oder $y = \frac{1}{x}$.

Beweis. Ohne Einschränkung sei $x > 0$. Dann gibt es nach untenstehender Aufgabe ein $k \in \mathbb{N}$ mit $10^{-k} < x$ und damit $10^k \cdot x > 1$. Wegen $0 \cdot x = 0$ existiert also ein größtes $y_0 \in \mathbb{N}$ mit $x \cdot y_0 \leq 1$. Beginnend mit diesem y_0, definieren wir nun rekursiv eine Zahlenfolge $\{y_n\}_{n=0,1,2,\ldots} \subset \mathbb{R}$ vermöge

$$y_{n+1} := y_n + k \cdot 10^{-n-1}$$
$$\text{mit } k \in \{0, 1, \ldots, 9\} \text{ maximal, so dass } x(y_n + k \cdot 10^{-n-1}) \leq 1.$$

(i) Offenbar ist diese Zahlenfolge monoton wachsend. Weiter lesen wir ab

$$y_1 \leq y_0 + \frac{9}{10}\,, \quad y_2 \leq y_1 + \frac{9}{10^2} \leq y_0 + \frac{9}{10} + \frac{9}{10^2} \quad \text{usw.}$$

und allgemein nach Anwendung der geometrischen Summenformel aus untenstehender Aufgabe

$$y_n \leq y_0 + \frac{9}{10} + \frac{9}{10^2} + \ldots + \frac{9}{10^n} < y_0 + \frac{9}{9} = y_0 + 1.$$

Nach Satz 6.5 besitzt $\{y_n\}_{n=0,1,2,\ldots}$ also einen Grenzwert $y \in \mathbb{R}$.

(ii) Weiter gilt $xy_n \leq 1$ für alle $n \in \mathbb{N}$. Nach Voraussetzung ist bereits $xy_0 \leq 1$, und nach Definition der y_{n+1} folgt sofort

$$xy_{n+1} = x(y_n + k \cdot 10^{-n-1}) \leq 1.$$

(iii) Als Übung belassen wir einen Beweis von

$$x(y_n + 10^{-n}) \geq 1 \quad \text{für alle } n \in \mathbb{N}.$$

Zusammenfassend folgt $xy = 1$, denn

$$1 \leq \lim_{n\to\infty} x(y_n + 10^{-n}) = xy = \lim_{n\to\infty} xy_n \leq 1.$$

Dieses y ist auch eindeutig. Wäre nämlich $1 = xz$ mit einem $z \in \mathbb{R}$, so folgt

$$y = y \cdot (x \cdot z) = (y \cdot x) \cdot z = 1 \cdot z = z.$$

Damit ist der Satz bewiesen. ∎

Eine Methode zur Berechnung des Kehrwertes unter Verwendung von SageMath lernen wir in den Aufgaben zum nachfolgenden Abschnitt kennen.

Aufgaben

Aufgabe 6.27 (Anordnung der Kehrwerte)

Es seien $0 < x < y$ reelle Zahlen. Beweisen Sie, dass dann gilt $0 < \dfrac{1}{y} < \dfrac{1}{x}$.

Aufgabe 6.28 (Stetigkeit des Kehrwertes)

Es sei $\{x_n\}_{n=0,1,2,\ldots} \subset \mathbb{R}$ eine konvergente Zahlenfolge mit $x_n \neq 0$ für alle $n \in \mathbb{R}$ und mit Grenzwert $x \neq 0$. Zeigen Sie, dass dann gilt

$$\lim_{n\to\infty} \frac{1}{x_n} = \frac{1}{x}\,.$$

Aufgabe 6.29 (Vervollständigung des Beweises I)

Beweisen Sie: Ist $x > 0$ reell, so existiert ein $k \in \mathbb{N}$ mit $10^{-k} < x$.

Aufgabe 6.30 (Geometrische Summenformel)

Es sei $n \in \mathbb{N}$. Beweisen Sie, dass für alle $x \in \mathbb{R} \setminus \{0\}$ gilt

$$\sum_{k=0}^{n} x^k = \frac{1 - x^{n+1}}{1 - x} \quad \text{mit dem } k\text{-fachen Produkt } x^k = x \cdot \ldots \cdot x.$$

Wenden Sie diese Formel auf $x = \frac{1}{2}$ und $x = \frac{1}{10}$ an. Veranschaulichen Sie sich Ihre Ergebnisse anhand der Zahlengeraden.

Aufgabe 6.31 (Vervollständigung des Beweises II)

Beweisen Sie die behauptete Abschätzung aus obigen Beweispunkt (iii).

6.7 Die Quadratwurzel

Satz 6.8: Es sei $x \geq 0$ eine reelle Zahl. Dann existiert genau eine reelle Zahl $y \geq 0$ mit der Eigenschaft $y^2 = x$, in Zeichen $y := \sqrt{x}$.

Für dieses y schreiben wir auch $y = \sqrt{x}$.

Beweis. Im Fall $x = 0$ wählen wir $y = 0$; diese Wahl ist eindeutig. Sei also $x > 0$, und sei $y_0 \in \mathbb{N}$ maximal mit $y_0^2 \leq x$. Wir definieren die Zahlenfolge $\{y_n\}_{n=0,1,2,\ldots} \subset \mathbb{R}$ vermöge

$$y_{n+1} := y_n + k \cdot 10^{-n-1}$$
$$\text{mit } k \in \{0, 1, \ldots, 9\} \text{ maximal, so dass } (y_n + k \cdot 10^{-n-1})^2 \leq x.$$

(i) Diese Zahlenfolge ist monoton wachsend und nach oben beschränkt, und besitzt daher nach Satz 6.5 einen Grenzwert $y \in \mathbb{R}$.

(ii) Nach Definition der Folge gilt $y_n^2 \leq x$ für alle $n \in \mathbb{N}$. Ferner ist

$$(y_n + 10^{-n})^2 \geq x \quad \text{für alle } n \in \mathbb{N}.$$

Zusammenfassend folgt $y^2 = x$, denn

$$x \leq \lim_{n\to\infty} (y_n + 10^{-n})^2 = y^2 = \lim_{n\to\infty} y_n^2 \leq x.$$

Dieses y ist eindeutig. Wäre nämlich $x = z^2$ mit einem $z > y$, so überlegt man sich $z^2 > x^2$ im Widerspruch zu $x = y^2 = z^2$. Das beweist den Satz. ∎

Aufgaben

Aufgabe 6.32 (Produkt und Anordnung von Quadratwurzeln)

(i) Es seien $x, y \geq 0$ reelle Zahlen. Beweisen Sie, dass $\sqrt{x \cdot y} = \sqrt{x} \cdot \sqrt{y}$.

(ii) Es seien $0 \leq x < y$ reelle Zahlen. Beweisen Sie, dass $\sqrt{x} < \sqrt{y}$.

Aufgabe 6.33 (Grenzwerte aus Wurzelausdrücken)
Ermitteln Sie, wenn möglich, die folgenden Grenzwerte.

a) $\lim_{n\to\infty} \left(\sqrt{n+1} - \sqrt{n}\right)$ b) $\lim_{n\to\infty} \left(-n + \sqrt{1+n+n^2}\right)$

c) $\lim_{n\to\infty} \left(\sqrt{n+3} - \sqrt{n-1}\right)\sqrt{n}$ d) $\lim_{n\to\infty} \left(n - \sqrt{n+1}\sqrt{n+2}\right)$

Aufgabe 6.34 ($\sqrt{2} + \sqrt{6}$ ist nicht rational)
Beweisen Sie, dass $\sqrt{2} + \sqrt{6}$ nicht rational ist.

Aufgabe 6.35 (Dedekinds Verallgemeinerung)
Beweisen Sie: Ist $k \in \mathbb{N}$ keine Quadratzahl, d.h. gilt nicht $k = a^2$ mit einem $a \in \mathbb{N}$, so gibt es kein $x \in \mathbb{Q}$ mit $x^2 = k$.

Aufgabe 6.36 (Das Heron-Verfahren)
In dieser Aufgabe geben wir das sogenannte *Heron-Verfahren* an, mit dessen Hilfe sehr schnell Wurzeln $\sqrt{a}$ ermittelt werden können. Im Folgenden sei o.B.d.A. $a > 1$ gewählt. Wir betrachten die rekursive Folge

$$\{x_n\}_{n=1,2,\ldots} \quad \text{vermöge} \quad x_1 := a, \quad x_{n+1} := \frac{1}{2}\left(x_n + \frac{a}{x_n}\right) \text{ für } n = 2, 3, \ldots$$

(i) Skizzieren Sie die Graphen der Funktionen $y = x$ und $y = \frac{1}{2}(x + a/x)$ für $a = 2$ in ein gemeinsames Koordinatensystem.
(ii) Ermitteln Sie näherungsweise die Werte x_n für $n = 2, 3, 4$ und $a = 2$.
(iii) Verifizieren Sie

$$(x_{n+1} - x_n)^2 = x_{n+1}^2 - a \quad \text{für alle } n = 1, 2, \ldots$$

Folgern Sie $x_n^2 \geq a$ für alle $n = 1, 2, \ldots$
(iv) Verifizieren Sie damit

$$x_1 \geq x_2 \geq x_3 \geq \ldots \geq 1.$$

Folgern Sie, dass die Folge $\{x_n\}_{n=1,2,\ldots}$ gegen $\sqrt{a}$ konvergiert.
(v) Schreiben Sie unter SageMath eine Routine `heron(a)` zur näherungsweisen Bestimmung der Quadratwurzel $\sqrt{a}$ einer reellen Zahl $a > 1$.

Aufgabe 6.37 (Noch einmal zum Kehrwert)
Es sei $0 < a < 1$ eine reelle Zahl. Wir betrachten die rekursive Folge

$$\{x_n\}_{n=0,1,2,\ldots} \quad \text{vermöge} \quad x_0 := 1, \quad x_{n+1} := 2x_n - ax_n^2\,.$$

(i) Ermitteln Sie näherungsweise die Werte x_n für $n = 1, 2, 3$ und $a = \frac{1}{2}$.
(ii) Zeigen Sie $x_n < \frac{1}{a}$ für alle $n = 0, 1, 2, \ldots$
(iii) Zeigen Sie $x_n > 0$ für alle $n = 0, 1, 2, \ldots$
(iv) Zeigen Sie weiter $x_{n+1} - x_n > 0$ für alle $n = 0, 1, 2, \ldots$
(v) Schließen Sie, dass $\{x_n\}_{n=0,1,2,\ldots}$ monoton wachsend und damit konvergent gegen ein $x \in \mathbb{R}$ ist.
(vi) Verifizieren Sie $x = \frac{1}{a}$.
(vii) Schreiben Sie unter SageMath eine Routing `inv(a)` zur näherungsweisen Bestimmung des Kehrwertes $\frac{1}{a}$ einer reellen Zahl $0 < a < 1$.

6.8 Binärdarstellung reeller Zahlen

Wir können reelle Zahlen auch im Binärsystem darstellen. Weil wir für natürliche Zahlen dies schon können, konzentrieren wir uns auf reelle Zahlen zwischen 0 und 1.

Eine Binärentwicklung ist ein Ausdruck $+x$ oder $-x$ der Form

$$x = \ldots x_{k+1}x_kx_{k-1}\ldots x_1x_0\,.\,x_{-1}x_{-2}x_{-3}\ldots$$
$$\text{mit} \quad x_k \in \{0,1\}, \quad k \in \mathbb{Z},$$

i.Z. auch $x = (x_k)_{k\in\mathbb{Z}}$, so dass folgende Eigenschaften erfüllt sind:

1. Es existiert ein $n \in \mathbb{N}$ mit $0 = x_{n+1} = x_{n+2} = x_{n+3} = \ldots$
2. Es existiert kein $\ell \in \mathbb{N}$ mit $1 = x_{-\ell} = x_{-\ell-1} = x_{-\ell-2} = \ldots$.

Wir können jede Binärentwicklung eine reelle Zahl (Dezimalentwicklung) zuordnen. Dazu interpretieren wir eine (positive) Binärentwicklung als Folge X_k von rationalen Zahlen:

$$X_k = x_n2^n + \ldots + x_12^1 + x_0 + x_{-1}2^{-1} + \ldots + x_{-k}2^{-k}$$

Bemerke, dass $\{X_k\}$ eine wachsende Folge ist und

$$x_{-1}2^{-1} + \ldots + x_{-k}2^{-k} \leq \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^k} = \frac{2^k - 1}{2^k} < 1.$$

Somit konvergiert X_k gegen eine reelle Zahl.
Umgekehrt können wir jeder reellen Zahl eine Binärentwicklung zuorden. Weil wir dies für natürliche Zahlen schon können, beschreiben wir dies für reelle Zahlen a mit $0 < a < 1$. Dazu

$$\begin{aligned} x_i &= 0 \text{ für } i \geq 0 \\ x_{-i} &= \begin{cases} 1 & \text{falls } \left(x_{-1}2^{-1} + \ldots + x_{i-1}2^{-i-1} + 1\cdot 2^{-i}\right) \leq a \\ 0 & \text{sonst .} \end{cases} \end{aligned}$$

Um die Binärdarstellung zu berechnen, sollte man sich realisieren, dass Multiplikation mit 2 im binären System bedeutet, dass man das Komma um eine Stelle nach rechts verschiebt. Ist $0 < a < 1$, so ist das erste Bit $x_{-1} = 1$, genau dann, wenn $1 \leq 2a$. Dann zieht man das Bit ab, also bildet $2a - x_{-1}$ und multiplizieren wiederum mit 2. Dann ist $x_{-2} = 1$ genau dann, wenn $1 \leq\leq 4a - 2x_{-1}$ und so weiter.
Deshalb ist die Methode ähnlich wie bei der Berechnung der Binärentwicklung einer natürlichen Zahl, nur geht man nach rechts statt links. Hier ist ein Algorithmus um Nachkommabits einer reellen Zahl $0 < a < 1$ zu berechnen. In SAGEMATH kann man das Befehl `a.str(base=2)` benutzen.

```
def bits(a,n):
    x=[]
    for i in range(n):
        a *=2
        if floor(a)==1:
            x.append(1)
            a-=1
        else: x.append(0)
    return x
```

Beispiel $a = 0,364$.

i	1	2	3	4	5	6	
a	$0,728$	$0,456$	$0,912$	$0,824$	$0,648$	$0,296$	$0,592$
x_{-i}	0	1	0	1	1	1	0

Analog hat man einen Algorithmus um aus einer Binärentwicklung einer reellen Zahl a Dezimalen von a zu berechnen.

Aufgaben

Aufgabe 6.38 Es sei $a > 1$ eine reelle Zahl. Zeigen Sie, dass a^{-k} gegen 0 konvergiert.

Aufgabe 6.39 Schreiben Sie die folgenden Dezimalentwicklungen in Binärentwicklungen mit der Methode der letzten Seite (10 Nachkommastellen).

1. $0,743$
2. $2,718$
3. $3,142$

Aufgabe 6.40 Bestimmen Sie die ersten zwei Nachkommastellen der Dezimalentwicklung der nachfolgenden Zahlen.

1. $0,100\,100\,110$
2. $11,011011$

Aufgabe 6.41 Da $1024 = 2^{10} \approx 10^3$, kann man relativ schnell mit der Hand etwa drei Dezimalstellen in ca. 10 Bits und umgekehrt umschreiben.

1. (a) Sei $a = 0,324$. Berechnen Sie mit der Hand $1024 \cdot a = 1000 \cdot a + 20 \cdot a + 4 \cdot a$.
   (b) Berechnen Sie jetzt 10 Nachkommabits von a.
2. (a) Sei $a = 0,110\,011\,010\,1$. Berechnen Sie $1000 \cdot a = 2^{10} \cdot a - 2^4 \cdot a - 2^2 \cdot a$.
   (b) Berechnen Sie drei Nachkommadezimalstellen von a.

6.9 Die Exponentialfunktion

Ist $a \in \mathbb{R}$ und $n \in \mathbb{N}_0$, so ist bekanntlich a^n rekursiv definiert durch $a^0 = 1$ und $a^n = a \cdot a^{n-1}$. Für negative Zahlen $-n$ und $a \neq 0$ gilt $a^{-n} = 1/a^n$. Wir haben die bekannten Rechenregeln $a^{n+m} = a^n \cdot a^m$ und $(a^n)^m = a^{nm}$. Ist $a > 1$, so folgt $a^n < a^m$, wenn $a \neq m$. Wenn wir diese Eigenschaften beibehalten wollen für Exponenten $x \in \mathbb{R}$, so sind wir gezwungen,

$$a^{1/2} = \sqrt{a}$$

Insbesondere ist diese Definition nur sinnvoll für $a \geq 0$. Wenn for $x > 0$ in Binärdarstellung

$$x = x_k 2^k + \ldots + x_0 2^0 + x_{-1} 2^{-1} + x_{-2} 2^{-2} + \ldots$$

schreiben, so definieren wir

$$\langle x \rangle_n = x_k 2^k + \ldots + x_0 2^0 + x_{-1} 2^{-1} + x_{-2} 2^{-2} + \cdots + x_{-n} 2^{-n}$$

dann muss

$$a^{\langle x \rangle_{n+1}} = \begin{cases} a^{\langle x \rangle_{n+1}} & \text{falls } x_{-n-1} = 0 \\ a^{\langle x \rangle_{n+1}} \cdot a^{1/2^{n+1}} & \text{falls } x_{-n-1} = 1. \end{cases}$$

Die $a^{1/2^n}$ können wir durch wiederholtes Quadratwurzel ziehen berechnen:

$$a^{1/2} = \sqrt{a},\ a^{1/4} = \sqrt{a^{1/2}},\ a^{1/8} = \sqrt{a^{1/4}}, \cdots$$

Für $x \in \mathbb{R}$ und $a \geq 0$ definieren wir

$$a^x := \lim_{n \to \infty} a^{\langle x \rangle_n}$$

und $a^{-x} = 1/a^x$.

Satz 6.9: Es sei $a > 0$.

1. Ist $x < y$ und $a > 1$, dann ist $a^x < a^y$.
2. Ist $\{x_n\}$ konvergent, so gilt $\lim_{n \to \infty} a^{x_n} = a^x$
3. $a^x \cdot a^y = a^{x+y}$.
4. $(a \cdot b)^x = a^x \cdot b^x$ für $b > 0$.
5. $(a^x)^y = a^{xy}$.
6. Ist $\{x_n\}$ eine konvergente Folge positiver reelen Zahlen, so gilt $\lim_{n \to \infty} x_n^a = x^a$.

Beispiel.

i	0	1	2	3	4	5	6	7
$3^{1/2^i}$	3	$1,73205$	$1,31607$	$1,14720$	$1,07107$	$1,03492$	$1,01731$	$1,00861$
x_i	1	0	1	1	0	1	0	1
$3^{\langle x\rangle_i}$	3	3	3,94822	4,52941	4,52941	4,68761	4,68761	4,72801

Also $3^{\sqrt{2}} \approx 4,72801$. Der "richtige" Wert ist $4,72880\ldots$

```
def exp(a,x,n):
    exp = a^(floor(x))
    x -= floor(x)
    for i in range(n):
        a = sqrt(a); x *= 2
        if floor(x)==1:
            exp *= a; x -= 1
    return exp
```

Kapitel 7

Elementare Wahrscheinlichkeitsrechnung

7.1 Ergebnisse und Ereignisse

Ausgangspunkt unserer Untersuchungen sind die möglichen *Ergebnisse* ω eines nicht näher spezifizierten *Zufallsexperiments.* Die Menge aller Ergebnisse heißt der *Ergebnisraum* Ω.

Beispiele.

1. Die möglichen Ergebnisse eines Würfelexperiments mit einem sechseitigen, unverfälschten Würfel sind beispielsweise die Elemente des Ergebnisraumes $\Omega = \{1, 2, 3, 4, 5, 6\}$.
2. Die möglichen Ergebnisse eines Würfelexperiments mit zwei ebensolchen Würfeln sind die Elemente der Menge $\Omega = \{(i, j) : 1 \leq i, j \leq 6\}$.
3. Die möglichen Ergebnisse eines Würfelexperiments mit einem sechseitigen, farbigen und unverfälschten Würfel können aber auch die Elemente des Ergebnisraumes $\Omega = \{\text{weiß}, \text{gelb}, \text{rot}, \text{blau}, \text{braun}, \text{schwarz}\}$ sein.
4. Misst man die Lebensdauer einer Glühbirne, so werden wir sinnvollverweise $\Omega = [0, \infty)$ ansetzen.

Ein *Ereignis* ist eine Teilmenge $A \subset \Omega$. Unter einem *Elementarereignis* versteht man ein einelementiges Ereignis.

Man sagt, ein Ereignis A *tritt ein,* wenn das Ergebnis des Zufallsexperiments zur Teilmenge A gehört.

Beispiel.

1. Fällt bei obigem Würfelexperiment die Zahl 6, so ist das Ergebnis $\omega = 6$ Element des Ereignisses $A = \{2, 4, 6\}$. Es tritt das Ereignis A des *Werfens einer geraden Zahl* ein.
2. Beim Würfeln mit zwei Würfeln entspricht das Ereignis, in der Summe 5 Augen zu würfeln, der Menge $A = \{(1, 4), (2, 3), (3, 2), (4, 1)\}$. Achten Sie hierbei auf die Anordnung der Zahlenpaare.
3. Für obiges Beispiel der Glühbirne bedeutet das Ereignis $A = (10, \infty)$ eine Lebensdauer der Glühbirne von mehr als 10 Stunden, $B = [0, 100]$ für eine höchstens 100stündige Lebensdauer.

Auch das *unmögliche Ereignis* $\emptyset \subset \Omega$ und das *sichere Ereignis* Ω sind Ereignisse. Denn ein Ergebnis gehört nie zu $\emptyset$, und jedes mögliche Ergebnis gehört zu Ω. Sind ferner A und B Ereignisse, so auch

$$A \cup B, \quad A \setminus B, \quad A \cap B, \quad A^c = \Omega \setminus A.$$

In diesem Kapitel ist Ω stets eine *endliche* Menge. Für den allgemeinen Fall unendlicher Ereignisräume benötigen wir Methoden der mathematischen Analysis, die wir aber erst später entwickeln werden.

Aufgaben

Aufgabe 7.1 (Beispiele von Ergebnisräumen I)

(i) Eine unverfälschte Münze mit den beiden Seiten „Kopf“ und „Zahl“ wird geworfen. Beschreiben Sie einen geeigneten Ergebnisraum.

(ii) Eine ebensolche Münze und ein unverfälschter Würfel werden gleichzeitig geworfen. Beschreiben Sie einen geeigneten Ergebnisraum.

Aufgabe 7.2 (Beispiele von Ergebnisräumen II)

An der Johannes Gutenberg-Universität wird eine Statistik über die Zahl der männlichen und weiblichen Studierenden geführt. Beschreiben Sie einen möglichen Ergebnisraum.

Aufgabe 7.3 (Wurf eines Würfels)

Ein unverfälschter Würfel wird einmal geworfen.

(i) Beschreiben Sie einen geeigneten Ergebnisraum.

(ii) Welchen Teilmengen von Ω entspricht das Ereignis A : „die Augenzahl ist gerade“?

(iii) Welcher Teilmenge entspricht das Ereignis A^c? Erläutern Sie.

Aufgabe 7.4 (Zweimaliger Wurf eines Würfel I)

Ein unverfälschter Würfel wird zweimal geworfen. Wir betrachten die Ereignisse

A : „beim ersten Wurf wird eine 3 geworfen“
B : „beim zweiten Wurf wird eine 4 geworfen“

(i) Geben Sie einen geeigneten Ergebnisraum Ω an.

(ii) Welchen Teilmengen von Ω entsprechen die Ereignisse A und B?

(iii) Welchen Ereignissen entsprechen die Teilmengen

$$A \cup B, \quad A \cap B, \quad A \setminus B?$$

Aufgabe 7.5 (Zweimaliger Wurf eines Würfel II)

Ein unverfälschter Würfel wird zweimal geworfen. Wir betrachten die Ereignisse

A : „die Augensumme ist 8“
B : „die Augensumme ist wenigstens 3“
C : „die Augensumme ist höchstens 6“

(i) Geben Sie einen geeigneten Ergebnisraum Ω an.

(ii) Welchen Teilmengen von Ω entsprechen die Ereignisse A, B und C?

(iii) Welchen Ereignisse entsprechen die Teilmengen

$$A \cup B \cup C, \quad A \cap B \cap C, \quad B \cap C, \quad C \setminus B?$$

7.2 Endliche Wahrscheinlichkeitsräume

Ereignissen $A \subset \Omega$ einer Ergebnismenge Ω ordnen wir nun Wahrscheinlichkeiten zu, nach denen diese Ereignisse im Zufallsexperiment eintreten.

Satz 7.1 Ein *endlicher Wahrscheinlichkeitsraum* ist ein Paar (Ω, P) mit

1. einer nichtleeren und endlichen Menge Ω
2. und eine Wahrscheinlichkeitsfunktion $P\colon \Omega \to [0,1]$, so dass $\sum_{\omega\in\Omega} P(\omega) = 1$.

Ist (Ω, P) ein endlicher Wahrscheinlichkeitsraum, und $A \subset \Omega$, so schreiben wir

$$P(A) = \sum_{\omega\in A} P(\omega).$$

Wir erhalten die sogenannte *Wahrscheinlichkeitsverteilung* $P\colon \mathcal{P}(\Omega) \to [0,1]$ auf der Potenzmenge $\mathcal{P}(\Omega)$ von Ω,. Es gilt

- $P(\Omega) = 1$,
- $P(A \cup B) = P(A) + P(B)$ für disjunkte Ereignisse A, B.

Es heißt $P(A)$ die *Wahrscheinlichkeit* des Ereignisses $A \in \mathcal{P}(\Omega)$.

Beispiel. Setzen wir als Wahrscheinlichkeitsverteilung

$$P(\omega) := \frac{1}{|\Omega|} \quad \text{für alle} \omega \in \Omega$$

, so erhalten wir die sogenannte *Laplaceschen Wahrscheinlichkeitsverteilung.* Das trifft insbesondere auf das Würfelexperiment mit einem unverfälschten Würfel zu. Dass es sich bei (Ω, P) tatsächlich um einen endlichen Wahrscheinlichkeitsraum handelt, verifizieren wir als Übung.

Beispiel. Wir ziehen $1 \le m \le n$ Kugeln aus einer Urne mit n Kugeln ohne Zurücklegen und ohne Beachtung der Reihenfolge. Wir setzen also

$$\Omega := \{A \subset \{1,\dots,n\} \,:\, |A| = m\}\,.$$

Nach Abschnitt 4.1 existieren $\binom{n}{m}$ solche Teilmengen A mit $|A| = m$. Bezeichnen wir die n Kugeln mit $K_1, \dots, K_n$, so ergibt sich unter Annahme einer Laplaceschen Wahrscheinlichkeitsverteilung die Wahrscheinlichkeit, m Kugeln $K_{i_1}, \dots, K_{i_m}$ mit Nummern $1 \le i_1 < \dots < i_m \le n$ zu ziehen, zu

$$P(\{i_1,\dots,i_m\}) = \frac{1}{\binom{n}{m}}\,.$$

Aufgaben

Aufgabe 7.6 (Eigenschaften der Wahrscheinlichkeitsverteilung I)
Beweisen Sie:

a) $\sum_{\omega\in\Omega} P(\{\omega\}) = 1$ b) $P(A) = \sum_{\omega\in A} P(\{\omega\})$, $A \subset \Omega$

Aufgabe 7.7 (Eigenschaften der Wahrscheinlichkeitsverteilung II)
Es seien $A, B \subset \Omega$ beliebig. Beweisen Sie:

a) $P(\emptyset) = 0$ b) $P(A^c) = 1 - P(A)$
c) $P(A) \leq P(B)$, falls $A \subset B$
d) $P(B \setminus A) = P(B) - P(A)$, falls $A \subset B$
e) $P(A \cup B) \leq P(A) + P(B)$
f) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

Aufgabe 7.8 (Zur Laplaceschen Wahrscheinlichkeitsverteilung)
Es sei P die Laplacesche Wahrscheinlichkeitsfunktion auf der Potenzmenge $\mathcal{P}$ einer endlichen, nichtleeren Menge Ω. Beweisen Sie, dass (Ω, P) einen endlichen Wahrscheinlichkeitsraum darstellt.

Aufgabe 7.9 (Die Farbe Rot beim Roulette)
Beim Roulettespiel gibt es 18 Zahlen schwarz, 18 Zahlen rot und die Zahl 0 farblos. Wie hoch ist die Wahrscheinlichkeit, nach einer Drehung eine rote Zahl zu erhalten unter Annahme einer Laplaceschen Wahrscheinlichkeitsverteilung?

Aufgabe 7.10 (Urnenexperiment mit zwei Farben)
In einer Urne liegen n Kugeln, davon $r > 0$ rote und $w = n - r$ weiße Kugeln. Wir wollen $1 \leq m \leq n$ Kugeln ohne Zurücklegen und ohne Beachtung der Reihenfolge ziehen, und davon sollen $1 \leq k \leq r$ rot sein.

(i) Wieviel Möglichkeiten gibt es, aus den r roten Kugeln k Kugeln zu ziehen?
(ii) Es verbleibt, von den $w = n - r$ weißen Kugeln $m - k$ Kugeln zu ziehen. Wieviele Möglichkeiten gibt es hierfür?
(iii) Wieviel Möglichkeiten gibt es also insgesamt, von den n Kugeln m Kugeln zu ziehen, wobei aber k Kugeln rot sind?
(iv) Bestimmen Sie nun die Wahrscheinlichkeit einer solchen Ziehung unter Annahme einer Laplaceschen Wahrscheinlichkeitsverteilung.

Aufgabe 7.11 (Gewinnchancen beim Lotto)
Beim Lotte 6 aus 49 werden 6 Kugeln ohne Zurücklegen und ohne Beachtung der Reihenfolge aus einer Lostrommel mit anfangs 49 durchnummerierten Kugeln entnommen. Wie groß ist die Wahrscheinlichkeit, $1 \leq k \leq 6$ „Richtige“ getippt zu haben?

7.3 Produkte von Wahrscheinlichkeitsräumen

Es sei $n \in \mathbb{N}$. Der *Produktraum* der endlichen Wahrscheinlichkeitsräume $(\Omega_1, P_1), \ldots, (\Omega_r, P_n)$ ist das Paar (Ω, P) mit $\Omega := \Omega_1 \times \ldots \times \Omega_n$ als Ergebnisraum und der Wahrscheinlichkeisfunktion $P\colon \Omega \to [0,1]$ vermöge

$$P(\omega) := P_1(\omega_1) \cdot \ldots \cdot P_n(\omega_n), \quad \omega = (\omega_1, \ldots, \omega_n) \in \Omega.$$

Satz 7.2 Es ist (Ω, P) ein endlicher Wahrscheinlichkeitsraum.

Beispiele.

1. Wir werfen zwei unverfälschte Würfel, denen wir die Wahrscheinlichkeitsräume (Ω_1, P_1) und (Ω_2, P_2) mit $\Omega_1 = \Omega_2 = \{1, \ldots, 6\}$ zusammen mit den Laplaceverteilungen P_1 und P_2 zuordnen. Als Produkt erhalten wir

$$(\Omega, P) = (\{(1,1), (1,2), \ldots, (6,6)\}, P) \quad \text{mit} \quad p(\omega) = \frac{1}{36}\,,\ \omega \in \Omega.$$

2. Betrachte (Ω, P) mit $\Omega = \{0,1\}$ und $p(1) := p$, $p(0) := 1-p$ für ein $p \in [0,1]$. Die zugehörige Verteilung P heißt *Bernoulliverteilung.* Es ist

$$p(k) = p^k(1-p)^{1-k}\,, \quad k \in \{0,1\}\,.$$

Wir bezeichnen $\{1\}$ auch als *Erfolg* und $\{0\}$ als *Misserfolg.* Wiederholen wir ein solches Bernoulliexperiment n-mal, so erhalten wir $(\Omega, P)^n$ als zugehörigen Wahrscheinlichkeitsraum. Mit dem Bisherigen folgt

$$P(A) = \binom{n}{k} p^k (1-p)^{n-k}$$

für das Ereignis A : „es tritt genau k-mal Erfolg ein“.

3. In Verallgemeinerung dieses Beispiels seien nun $\Omega = \{0, \ldots, r-1\}$ und $p(i) := p_i$ mit $p_0 + \ldots + p_{r-1} = 1$, und es bedeute A das Ereignis, dass i genau k_i-mal vorkommt nach n-maliger Wiederholung des Experiments:

$$A = \{(\omega_1, \ldots, \omega_n) \,:\, |\{j \,:\, \omega_j = i\} = k_1\}| \subset \Omega^n\,.$$

Aus Abschnitt **??** wissen wir $|A| = \frac{n!}{k_0!k_1!\cdot\ldots\cdot k_{r-1}!}$ und damit

$$P(A) = \frac{n!}{k_0!k_1! \cdot \ldots \cdot k_{r-1}!}\, p_0^{k_0} \cdot \ldots \cdot p_{r-1}^{k_{r-1}}\,.$$

Aufgaben

Aufgabe 7.12 (Produkt von Wahrscheinlichkeitsräumen)
Beweisen Sie vorigen Satz.

Aufgabe 7.13 (Wurf von Würfel und Münze)
Formulieren Sie das Beispiel 1 für den Wurf eines Würfels und einer Münze.

Historisches

Folgendes Experiment geht im Wesentlichen auf B. Pascal (1654) zurück: Zwei Spieler S_1 und S_2 werfen um den Einsatz von 100 Euro eine Münze. Es wird vereinbart, dass S_1 den Einsatz gewinnt, wenn 10 Mal Kopf K geworfen wurde, ohne dass 10 Mal Zahl Z fiel, und S_2 gewinnt, wenn 10 Mal Zahl fiel, ohne dass bis dahin 10 Mal Kopf vorkam. Krankheitsbedingt müssen die Spieler nach 8 Mal Kopf und 7 Mal Zahl unterbrechen. Wie teilen Sie das Geld „gerecht“ auf? Klar ist, dass der Gewinner spätestens nach vier weiteren Würfen festgestanden hätte. Also setzen wir

$$\Omega := \{K, Z\}^4 \quad \text{und} \quad P(\omega) = \frac{1}{16} \text{ für alle } \omega \in \Omega.$$

Beachte dabei $16 = 2^4$. Wir zählen alle diese Möglichkeiten auf:

K	K	K	K	K	K	Z	Z		K	Z	Z	Z
K	K	K	Z	K	Z	K	Z		Z	K	Z	Z
K	K	Z	K	Z	K	K	Z		Z	Z	K	Z
K	Z	K	K	Z	K	Z	K		Z	Z	Z	K
Z	K	K	K	Z	Z	K	K		Z	Z	Z	Z
				K	Z	Z	K					

In 11 von 16 Fällen hätte also S_1 gewonnen, in 5 von 16 Fällen S_2. Wäre also eine Gewinnaufteilung von $\frac{11}{16}$ für S_1 und $\frac{5}{16}$ für S_2 gerecht? Hier haben wir aber den Einwand, dass die Münzwürfe doch abgebrochen werden sollten, sobald der Gewinner feststeht. Es werden also nicht unbedingt alle vier restlichen Würfe durchgeführt. Vielmehr sind die tatsächlich verbleibenden Möglichkeiten:

K	K						
K	Z	K		K	Z	Z	Z
K	Z	Z	K	Z	K	Z	Z
Z	K	K		Z	Z	K	Z
Z	K	Z	K	Z	Z	Z	
Z	Z	K	K				

Ist also eine Gewinnaufteilung von $\frac{6}{10}$ und $\frac{4}{10}$ gerecht? Beachten Sie nämlich, dass die zehn Fälle nicht alle gleich wahrscheinlich sind! Zum Beispiel beträgt die Wahrscheinlichkeit $\frac{1}{4}$ für den Fall KK, aber $\frac{1}{16}$ für $KZZZ$. Erst wenn man dies letztlich noch berücksichtigt, erhält man ein gerechtes Ergebnis.

7.4 Bedingte Wahrscheinlichkeiten

Die Wahrscheinlichkeit, dass beim Würfeln mit zwei unverfälschten Würfeln der zweite Würfel die Zahl 6 zeigt, beträgt $\frac{1}{6}$, *unabhängig* vom Wurf des ersten Würfels. Fiel beim Roulette die Kugel 12 Mal hintereinander auf Schwarz, so ist die Wahrscheinlichkeit für Rot beim dreizehnten Mal immer noch $\frac{18}{37}$, *unabhängig* vom Ausgang der vorigen 12 Ereignisse.

Mathematisch können wir *Unabhängigkeit* wie folgt formulieren.

Sei (Ω, P) ein endlicher Wahrscheinlichkeitsraum. Seien weiter $A, B \subset \Omega$ zwei Ereignisse mit $P(B) \neq 0$. Dann heißt

$$P(A|B) := \frac{P(A \cap B)}{P(B)}$$

die *bedingte Wahrscheinlichkeit von A gegeben B*. Ferner heißen A und B *unabhängig,* wenn $P(A|B) = P(A)$ bzw. gleichbedeutend

$$P(A \cap B) = P(A) \cdot P(B).$$

Wir können die Unabhängigkeit zweier Ereignisse A und B auch als *relative Häufigkeiten* wie folgt interpretieren: Es ist die relative Häufigkeit von A innerhalb der Teilmenge B gleich der relativen Häufigkeit von A innerhalb der Ausgangsmenge Ω, d.h. $\frac{|A \cap B|}{|B|} = \frac{|A|}{|\Omega|}$, und das bedeutet $\frac{P(A \cap B)}{P(B)} = \frac{P(A)}{P(\Omega)} = P(A)$ für die Wahrscheinlichkeiten. Können Sie nun auch $P(A|B)$ als relative Häufigkeit interpretieren?

Bemerkung. Im Fall $P(B) = 0$ setzen wir $P(A|B) := 0$.

Beispiel. Von einer Familie mit 2 Kindern ist bekannt, dass wenigstens eines der Kinder ein Mädchen ist. Wie groß ist die Wahrscheinlichkeit, dass das zweite Kind ebenfalls ein Mädchen ist? Zur Lösung definieren wir den Ergebnisraum

$$\Omega := \{(J, J), (J, M), (M, J), (M, M)\}$$

und setzen eine Laplaces Wahrscheinlichkeitsverteilung voraus mit Wahrscheinlichkeit $\frac{1}{4}$ für jedes Elementarereignis. Nun ist $A = \{(M, M)\}$ das Ereignis, dass beide Kinder Mädchen sind. Ferner ist $B = \{(J, M), (M, J), (M, M)\}$ das Ereignis, dass wenigstens eines der Kinder ein Mädchen ist. Beachte $A = A \cap B$. Die Wahrscheinlichkeit $P(A|B)$, dass A eintritt unter der Bedingung B, d.h. dass beide Kinder Mädchen sind unter der Bedingung, dass wenigstens eines der Kinder ein Mädchen ist, berechnet sich daher zu

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(A)}{P(B)} = \frac{\frac{1}{4}}{\frac{3}{4}} = \frac{1}{3}\,.$$

Aufgaben

Aufgabe 7.14 (Interpretation der bedingten Wahrscheinlichkeit)
Interpretieren Sie $P(A|B)$ als relative Häufigkeit.

Aufgabe 7.15 (Noch einmal zum Beispiel)
Von einer Familie mit 2 Kindern ist bekannt, dass wenigstens eines der Kinder ein Mädchen ist. Wie groß ist die Wahrscheinlichkeit, dass das zweite Kind ein Junge ist?

Aufgabe 7.16 (Augensumme bei Zweimaligem Würfeln I)
Wir würfeln zweimal mit einem unverfälschten Würfel. Wie groß ist die Wahrscheinlichkeit, dass die Augensumme gleich 8 ist, wenn beim ersten Wurf bereits eine 5 geworfen wurde? Definieren Sie Ereignisse A und B, und berechnen Sie $P(A|B)$.

Aufgabe 7.17 (Augensumme bei Zweimaligen Würfeln II)
Wir würfeln zweimal mit einem unverfälschten Würfel. Wie groß ist die Wahrscheinlichkeit, dass die Augensumme kleiner oder gleich 10 ist, wenn beim ersten Wurf bereits eine 5 geworfen wurde?

Aufgabe 7.18 (Zurück zum Urnenexperiment)
In einer Urne liegen 12 rote, 27 blaue und 23 weiße Kugeln. Wir ziehen zweimal ohne Zurücklegen. Wie groß ist Wahrscheinlichkeit, beides Mal blau zu ziehen?

Aufgabe 7.19 (Teilnehmer am Seminar)
Am Seminar zur Elementaren Wahrscheinlichkeitstheorie nehmen 12 Jungen und 17 Mädchen teil. Von den 12 Jungen wohnen 7 in Mainz, von den 17 Mädchen von 15 in Mainz. Wir betrachten die Ereignisse A :„teilnehmende Person ist ein Junge“ und B : „teilnehmende Person wohnt in Mainz“. Erläutern Sie die Bedeutung der bedingten Wahrscheinlichkeiten $P(A|B)$ und $P(B|A)$, und berechnen Sie diese.

Aufgabe 7.20 (Bonbons jeder Geschmacksrichtung)
In Berti Botts Schachtel mit Bonbons jeder Geschmacksrichtung befinden sich 24 Bonbons, eingewickelt in goldener Folie. 18 Bonbons sind mit Vollmilchschokolade überzogen, 6 mit weißer Schokolade. Die Hälfte der mit Vollmilch überzogenen Bonbons enthält die Geschmacksrichtung Spinat. Insgesamt gibt es 20 Bonbons dieser Geschmacksrichtung. Wie groß ist die Wahrscheinlichkeit, bei einmaligem Ziehen ein mit weißer Schokolade überzogenes Bonbon der Geschmacksrichtung Spinat zu bekommen?

7.5 Die Regel von Bayes

Satz 7.1: Seien (Ω, P) ein endlicher Wahrscheinlichkeitsraum und $A, B \subset \Omega$ zwei Teilmengen mit $P(B) \neq 0$.

1. Es gilt $P(A|B) = \dfrac{P(B|A)P(A)}{P(B)}$.

2. Ist $\Omega = \bigcup_{i=1}^{n} A_i$ mit $A_i \cap A_j = \emptyset$ für alle $i \neq j$ richtig, so gilt

$$P(A_j|B) = \frac{P(B|A_j)P(A_j)}{\sum_{i=1}^{n} P(A_i)P(B|A_i)}, \quad j = 1, \ldots, n.$$

Beweis. Nach Definition gelten

$$P(A|B)P(B) = P(A \cap B) \quad \text{und} \quad P(B|A)P(A) = P(B \cap A) = P(A \cap B).$$

Gleichsetzen zeigt die erste Behauptung. Für die zweite Behauptung beachte

$$B = \bigcup_{i=1}^{n} B \cap A_i \quad \text{mit} \quad (B \cap A_i) \cap (B \cap A_j) = \emptyset \quad \text{für alle } i \neq j,$$

woraus nach der Definition einer Wahrscheinlichkeitsverteilung aus Abschnitt 7.2 sowie der bedingten Wahrscheinlichkeit folgt

$$P(B) = \sum_{i=1}^{n} P(B \cap A_i) = \sum_{i=1}^{n} P(A_i)P(B|A_i).$$

Einsetzen in die erste Behauptung beweist den Satz. ∎

Beispiel. Wir werfen zwei unverfälschte Münzen mit Kopf und Zahl sowie ein verfälschte Münze, welche auf beiden Seiten Kopf zeigt. Nun nehmen wir eine dieser drei Münzen, werfen sie dreimal und stellen fest, das jedesmal Kopf erscheint. Wie groß ist die Wahrscheinlichkeit, dass es sich um die verfälschte Münze handelt? Zur Lösung setzen wir

$$\begin{aligned} A_1 &: \text{ eine unverfälschte Münze wurde genommen} \\ A_2 &: \text{ die verfälschte Münze wurde genommen} \\ B &: \text{ es wurde dreimal Kopf geworfen} \end{aligned}$$

Als Übung bestätigt man $P(A_1) = \frac{2}{3}$, $P(A_2) = \frac{1}{3}$, $P(B|A_1) = \frac{1}{8}$, $P(B|A_2) = 1$. Die zweite Identität des Satzes liefert mit $n = 2$ die gesuchte Wahrscheinlichkeit

$$P(A_2|B) = \frac{P(B|A_2)P(A_2)}{P(A_1)P(B|A_1) + P(A_2)P(B|A_2)} = \frac{\frac{1}{3} \cdot 1}{\frac{2}{3} \cdot \frac{1}{8} + \frac{1}{3}} = \frac{4}{5}.$$

Aufgaben

Aufgabe 7.21 (Ein Spezialfall des Satzes)
Verifizieren Sie die Identität aus der zweiten Behauptung des Satzes für den speziellen Fall $n = 1$, d.h. $\Omega = A_1$.

Aufgabe 7.22 (Zu obigem Beispiel)
Verifizieren Sie die angegebenen Werte der Wahrscheinlichkeiten $P(A_1)$, $P(A_2)$, $P(B|A_1)$ und $P(B|A_2)$ aus obigem Beispiel.

Aufgabe 7.23 Ein Informatikstudent nehmt an 70% der Vorlesungstage die Mainzelbahn. In 80% dieser Fälle kommt er rechtzeitig zur Vorlesung. Durchschnittlich kommt er in 60% der Vorlesungstage pünktlich.
Heute ist der Student pünktlich. Mit welcher Wahrscheinlichkeit hat er die Mainzelbahn benutzt?

Aufgabe 7.24 Gegeben sind 2 Urnen mit Murmeln. In der ersten Urne gibt es 8 rote und zwei weiße Murmeln. In der zweite Urne gibt es eine rote und 4 weiße Murmeln. Man nimmt aus einer Urne zwei Murmeln.

1. Wie groß ist die Chance, dass beide Murmeln weiß sind?
2. Angenommen, beide Kugeln sind weiß. Wie groß ist die Chance, dass diese aus der ersten Urne kommen?

Aufgabe 7.25 In vier verschiedenen Schubladen sind bunte Kugeln enthalten, gemäß der Tabelle:

	S_1	S_2	S_3	S_4
rot	5	3	2	1
blau	3	3	8	7

Talofa wählt zufällig drei Kugeln aus einer Schublade.

1. Wie groß ist die Wahrscheinlichkeit, dass zwei Kugeln blau sind und eine rot ist?
2. Wenn zwei Kugeln blau sind eine eine rot ist, wie groß ist die Wahrscheinlichkeit, dass beide aus der vierten Schublade sind?

Aufgabe 7.26 Gegeben sind drei Körbe mit Äpfeln. Im ersten Korb gibt es 5 rote und 2 grüne Äpfel, im zweiten gibt es 4 rote und einen grüne un im dritten gibt es zwei rote und sieben grüne Äpfel.

7.6 Zufallsvariablen

Es sei (Ω, P) ein endlicher Wahrscheinlichkeitsraum. Eine Abbildung

$$X\colon \Omega \longrightarrow \mathbb{R}$$

heißt *Zufallsvariable* oder auch *Zufallsgröße.* Für $D \subset \mathbb{R}$ setzen wir weiter

$$P_X(D) := P(\{\omega \in \Omega \,:\, X(\omega) \in D\}$$

und bezeichnen P_X als die *Wahrscheinlichkeitsverteilung von* X. Schließlich heißt die Abbildung $p_X\colon \mathbb{R} \to [0,1]$, definiert durch

$$p_X(k) := P(\{\omega \in \Omega \,:\, X(\omega) = k\}), \quad k \in \mathbb{R},$$

die zu P_X gehörige *Wahrscheinlichkeitsfunktion von* X.

Bemerkung. Beachte, dass $X(\Omega) \subset \mathbb{R}$ endlich, da Ω endlich ist. Ferner ist als Übung zu verifizieren, dass $(X(\Omega), P_X)$ wieder ein endlicher Wahrscheinlichkeitsraum.

Beispiel. Es sei $\Omega = \{(i,j) \,:\, 1 \le i,j \le 6\}$ der Ereignisraum für den einmaligen Wurf zweier unverfälschter Würfel. Betrachte die Zufallsvariable $X(i,j) := i+j$. Dann ist

$$p_X(7) = P(\{(i,j) \in \Omega \,:\, X(i,j) = 7\}) = \frac{6}{36} = \frac{1}{6}\,.$$

Die Zufallsvariable X heißt *binomialverteilt* mit Parametern $n \in \mathbb{N}$ und $p \in [0,1]$, wenn gilt

$$p_X(k) := \binom{n}{k} p^k (1-p)^{n-k}\,, \quad k = 0, 1, \ldots, n.$$

Die zugehörige Verteilung P_X heißt *Binomialverteilung,* i.Z. $\mathrm{Bin}(n,p)$.

Beispiel. Wir würfeln zehnmal mit einem unverfälschten Würfel. Wie groß ist die Wahrscheinlichkeit, dreimal die 6 zu würfeln? In diesem Beispiel setzen wir $\Omega := \{0,1\}^{10}$, worin 1 Erfolg und 0 Misserfolg, eine 6 zu würfeln, bedeuten. Wir betrachten die Zufallsvariable

$$X\colon \Omega \longrightarrow \mathbb{R}, \quad (\omega_1, \ldots, \omega_{10}) \mapsto \omega_1 + \ldots + \omega_{10}\,.$$

Dann steht auf der rechten Seite genau die Anzahl, wie oft 6 gewürfelt wurde. Bekannt sind $p(0) = \frac{5}{6}$ und $p(1) = \frac{1}{6}$. Es ist X binomialverteilt mit Parametern $n = 10$ und $p = \frac{1}{6}$, vergleiche Abschnitt 7.3, also

$$p_X(3) = \binom{10}{3} \left(\frac{1}{6}\right)^3 \left(\frac{5}{6}\right)^7 \approx 0.155.$$

Aufgaben

Aufgabe 7.27 (Zu obiger Bemerkung)

Es sei (Ω, P) ein endlicher Wahrscheinlichkeitsraum. Verifizieren Sie, dass dann auch $(X(\Omega), P_X)$ ein endlicher Wahrscheinlichkeitsraum ist.

Aufgabe 7.28 (Bernoulliverteilt und Binomialverteilt)

Die Zufallsvariable X sei binomialverteilt gemäß $\mathrm{Bin}(1, p)$. Zeigen Sie

$$p_X(1) = p, \quad p_X(0) = 1 - p.$$

Aufgabe 7.29 (Urnenexperiment und Binomialverteilung)

Gegeben sei eine Urne mit n Kugeln, wovon $r > 0$ rot und $w > 0$ weiß sind. Wir ziehen $1 \leq m \leq n$ Kugeln mit Zurücklegen.

(i) Das Anzahl der roten Kugeln bei einer solchen Ziehung ist binomialverteilt. Wie lauten die Zufallsvariable X und die Parameter n und p?

(ii) Wie groß ist die Wahrscheinlichkeit, genau m-mal rot zu ziehen?

Aufgabe 7.30 (Automatenspiele)

Die Wahrscheinlichkeit, bei einem Automaten ein Spiel zu gewinnen, beträgt $p = 0.1$. Wie groß ist die Wahrscheinlichkeit, dass man bei 15 Spielen

a) 1 mal b) 8 mal c) 15 mal

gewinnt?

Aufgabe 7.31 (Münzwurf und Binomialverteilung)

Eine unverfälschte Münze wird zehnmal geworfen.

(i) Wie groß ist die Wahrscheinlichkeit, genau dreimal Kopf zu werfen?

(ii) Wie groß ist die Wahrscheinlichkeit, höchstens dreimal Kopf zu werfen?

(iii) Wie groß ist die Wahrscheinlichkeit, mindestens dreimal Kopf zu werden?

7.7 Der Erwartungswert

Es seien (Ω, P) ein endlicher Wahrscheinlichkeitsraum und $X\colon \Omega \to \mathbb{R}$ eine Zufallsvariable mit Wahrscheinlichkeitsfunktion p_X. Dann ist der *Erwartungswert* $E(X)$ von X definiert durch

$$E(X) := \sum_{x \in X(\Omega)} x p_X(x).$$

Bemerkung. Es ist $E(X)$ ein *gewichteter Mittelwert* der Zahlen $x \in X(\Omega)$. Im Fall $p_X(x) = \frac{1}{|X(\Omega)|}$ für alle $x \in X(\Omega)$ gilt

$$E(X) = \frac{1}{|X(\Omega)|} \sum_{x \in X(\Omega)} x,$$

d.h. $E(X)$ stimmt mit dem *klassischen Mittelwert* der $x \in X(\Omega)$ überein.

Bemerkung. Als Übung verifiziere man $E(X) = \sum_{\omega \in \Omega} X(\omega) P(\{\omega\})$.

Beispiel. Wir würfeln mit einem unverfälschten Würfel und betrachten genauer $\Omega = \{1, \ldots, 6\}$, $X(i) = i$ und $p_X(i) = \frac{1}{6}$. Dann ist wegen $X(\Omega) = \{1, \ldots, 6\}$

$$E(X) = \sum_{i=1}^{6} i p_X(i) = \frac{1}{6} \sum_{i=1}^{6} p_X(i) = \frac{1}{6} \sum_{i=1}^{6} i = \frac{21}{6} = 3.5.$$

Ein Beweis des folgenden Satzes verbleibt als Übung.

Satz 7.3 Seien (Ω, P) ein endlicher Wahrscheinlichkeitsraum, $X, Y\colon \Omega \to \mathbb{R}$ zwei Zufallsvariablen und $a \in \mathbb{R}$. Dann gelten

$$E(X + Y) = E(X) + E(Y) \quad \text{und} \quad E(aX) = aE(X).$$

Vermittels vollständiger Induktion entnehmen wir

$$E(a_1 X_1 + \ldots + a_n X_n) = a_1 E(X_1) + \ldots + a_n E(X_n) \quad \text{für alle } n \in \mathbb{N}.$$

Satz 7.4 Es sei die Zufallsvariable X binomialverteilt mit Parametern $n \in \mathbb{N}$ und $p \in [0, 1]$. Dann gilt $E(X) = np$.

Beweis. Sei $X_i(\omega_1, \ldots, \omega_n) = \omega_i$. Dann is $E(X_i) = p$, $X = X_1 + \ldots + X_n$, somit $E(X) = np$.

Aufgaben

Aufgabe 7.32 (Wurf zweier Würfel und Erwartungswert)
Wir werfen zwei unverfälschte Würfel, also $\Omega = \{(i,j) : 1 \leq i,j \leq 6\}$ und $X(i,j) = i+j$ Laplaceverteilt. Berechnen Sie den Erwartungswert $E(X)$.

Aufgabe 7.33 (Eigenschaften des Erwartungswertes)
Beweisen Sie die im ersten Satz genannten Eigenschaften

$$E(X+Y) = E(X) + E(Y), \quad E(\alpha X) = \alpha E(X).$$

Aufgabe 7.34 Jan und Marie würfeln mit zwei Würfeln. Beträgt die Gesamtanzahl der Agen weniger als 9, so muss Jan Marie 10 Euro zhlen. In allen anderen Fällen muss Marie x Euro zahlen. Wie groß muss x sein, damit keiner der Spieler benachteiligt wird.

Aufgabe 7.35 In einer Vase gibt es vier rote und sechs grüne Kugeln. Es wird nacheinander Kugeln gezogen. Das Spiel ist zu Ende, wenn er eine rote Kugel ziehgt oder wenn er dreimal gezogen hat. Die Zufallsvariable X ist die Anzahl der gezogenen grünen Kugeln.

1. Bestimme die Warscheinlichkeitsverteilung von X.
2. Um das Spiel zu spielen, muss man 10 Euro Einsatz bezahlen. Der Gewinn ist 30 Euro, wenn man drei grüne Kugeln gezogen hat und 20 Euro, wennn man zwei grüne Kugel zieht. Was ist der Erwartungswert des Gewinnes/Verlustes?

Aufgabe 7.36 In einer Vase gibt es 2 blaue, 3 rote und 5 gelbe Kugel. Es werden 3 Kugeln gezogen. Man bekommte 6 Euro, wenn alle drei Kugeln dieselbe Farbe habe und zwei Euro, wenn alle drei Kugeln unterschiedliche Farben haben. Bei alle anderen Ausgängen muss man 1,50 Euro bezahlen.
Was der Erwartungswert des Gewinnes/Verlustes?

Aufgabe 7.37 Auf einem Glücksrad gibt es drei Felder mit den Aufschriften +20 Euro, +50 Euro und -70 Euro. Die Wahrscheinlichkeit, ein Feld mit +20 oder +50 Euro zu drehen ist 40%. Ein Spiel besteht aus zweimaligen Drehen am Glücksrad.

1. Wie groß ist die Wahrscheinlichkeit, dass man bei einem Spiel Geld gewinnt?
2. Wie groß ist die Wahrscheinlichkeit, dass ein Spieler bei 10 Spielen genau 7 mal gewinnt.
3. Wieviele Spiele müssen gespielt werden, damit der Spielanbieteer mit Einnahmen von etwa 10.000 Euro rechnen kann?

7.8 Unabhängige Zufallsvariablen

Den Begriff unabhängiger Ereignisse wollen wir nun auf Zufallsvariablen erweitern. Im Folgenden setzen wir

$$X \in I := \{\omega \in \Omega \,:\, X(\omega) \in I\}\,, \quad I \subset \mathbb{R}$$

und verwenden die kompakte und übliche Schreibweise

$$P(X_1 \in I_1, \ldots, X_r \in I_r) := P(\{\omega \in \Omega \,:\, X_1(\omega) \in I_1 \wedge \ldots \wedge X_r(\omega) \in I_r).$$

Es seien (Ω, P) ein endlicher Wahrscheinlichkeitsraum. Es heißen die Zufallsvariablen $X_1, \ldots, X_r \colon \Omega \to \mathbb{R}$ *unabhängig* genau dann, wenn für alle Intervalle $I_1, \ldots, I_r \subset \mathbb{R}$ gilt

$$P(X_1 \in I_1, \ldots, X_r \in I_r) = P(X_1 \in I_1) \cdot \ldots \cdot P(X_r \in I_r).$$

Der Erwartungswert des Produktes unabhängiger Zufallsvariablen ist einfach das Produkt der einzelnen Erwartungswerte.

Satz 7.2: Es seien X, Y zwei unabhängige Zufallsvariablen auf dem endlichen Wahrscheinlichkeitsraum (Ω, P). Dann gilt

$$E(XY) = E(X) \cdot E(Y).$$

Beweis. Zunächst bilden wir die Zerlegung

$$\{\omega \in \Omega \,:\, XY(\omega) = z\} = \bigcup_{x \neq 0} \left\{\omega \in \Omega \,:\, X(\omega) = x \wedge Y(\omega) = \frac{z}{x}\right\} =: \bigcup_{x \neq 0} M_x$$

mit disjunkten Mengen M_x, $M_{x'}$ usw. Damit berechnen wir (beachte, dass $z = 0$ liefert zur Summation keinen Beitrag)

$$\begin{aligned}
E(XY) &= \sum_{z \neq 0} z P(\{\omega \in \Omega \,:\, XY(\omega) = z\}) \\
&= \sum_{z \neq 0} z P\left(\bigcup_{x \neq 0} \left\{\omega \in \Omega \,:\, X(\omega) = x \wedge Y(\omega) = \frac{z}{x}\right\}\right) \\
&= \sum_{z \neq 0} z \sum_{x \neq 0} P\left(\left\{\omega \in \Omega \,:\, X(\omega) = x \wedge Y(\omega) = \frac{z}{x}\right\}\right) \\
&= \sum_{z \neq 0} \sum_{x \neq 0} z P\left(\left\{\omega \in \Omega \,:\, X(\omega) = x \wedge Y(\omega) = \frac{z}{x}\right\}\right).
\end{aligned}$$

Da aber X und Y unabhängig sind, folgern wir weiter

$$\begin{aligned} E(XY) &= \sum_{z\neq 0}\sum_{x\neq 0} zP\{\omega\in\Omega\,:\,X(\omega)=x\})P\left(\left\{\omega\in\Omega\,:\,Y(\omega)=\frac{z}{x}\right\}\right) \\ &= \sum_{y\neq 0}\sum_{x\neq 0} xyP(X=x)P(Y=y) \;=\; E(X)E(Y). \end{aligned}$$

Das war zu zeigen. ∎

Aufgaben

Aufgabe 7.38 (Unabhängigkeit beim zweifachem Münzwurf)
Wir werfen zweimal eine unverfälschte Münze, d.h. mit Kopf K und Zahl Z ist

$$\Omega = \{(K,K),(K,Z),(Z,K),(Z,Z)\}\,.$$

Hierauf betrachten wir die beiden Zufallsvariablen $X, Y\colon \Omega\to\mathbb{R}$ vermittels

$$\begin{aligned} &X(K,K)=0, \quad X(K,Z)=0, \quad X(Z,K)=1, \quad X(Z,Z)=1, \\ &Y(K,K)=0, \quad Y(K,Z)=1, \quad Y(Z,K)=0, \quad Y(Z,Z)=1. \end{aligned}$$

Es beschreibt also X den Ausgang des ersten Wurfes, Y den des zweiten Wurfes. Verifizieren Sie, dass X und Y unabhängig sind.

Aufgabe 7.39 (Unabhängigkeit beim zweifachen Wurf eines Würfels)
Formulieren Sie vorige Aufgabe für den zweifachen Wurf eines unverfälschten Würfels statt eines zweifachen Münzwurfes. Verifizieren Sie die Unabhängigkeit der von Ihnen aufgestellten Zufallsvariablen X und Y.

7.9 Varianz und Standardabweichung

Es sei X eine Zufallsvariable auf dem endlichen Wahrscheinlichkeitsraum (Ω, P). Die *Varianz* von X ist dann definiert durch

$$\mathrm{Var}(X) := E((X-\mu)^2) \quad \text{mit } \mu := E(X).$$

Als *Standardabweichung* verstehen wir ferner

$$\sigma(X) := \sqrt{\mathrm{Var}(X)}\,.$$

Bemerkung. Die Varianz ist gleich dem Quadrat der Abweichung der Zufallsvariablen von ihrem Erwartungswert. In Anlehnung an den Begriff des *(gewichteten) Mittelwertes* spricht man auch von *mittlerer quadratischer Abweichung.* Unter Benutzung des ersten Satzes aus Abschnitt 7.7 ermitteln wir ferner

$$\begin{aligned}\mathrm{Var}(X) &= E((X-\mu)^2) = E(X^2 - 2\mu X + \mu^2) = E(X^2) - 2\mu E(X) + E(\mu^2)\\ &= E(X^2) - 2\mu^2 + \mu^2 = E(X^2) - \mu^2 = E(X^2) - E(X)^2\,.\end{aligned}$$

Dabei verwenden wir, dass für die konstante Zufallsvariable $Z = \mu^2$ gilt

$$E(\mu^2) = \sum_{z \in Z(\Omega)} z p_Z(z) = \mu^2 P(\{\omega \in \Omega : Z(\omega) = \mu^2) = \mu^2\,,$$

da $p_Z(z) = 0$ für alle $z \neq \mu^2$.

Beispiel. Wir werfen zwei unverfälschte Würfel: $\Omega = \{(i,j) : 1 \le i,j \le 6\}$ und $X(i,j) := i + j$ Laplaceverteilt. Mit $E(X) = 7$ berechnen wir

$$\begin{aligned}\mathrm{Var}(X) &= E(X^2) - E(X)^2 = \sum_{x \in X(\Omega)} x^2 p_X(x) - 7^2 = \sum_{k=1}^{12} k^2 p_X(k) - 7^2\\ &= \sum_{k=2}^{12} k^2 p_X(k) - 7^2 = \frac{1974}{36} - 7^2 = \frac{35}{6}\,.\end{aligned}$$

Die zweite Identität folgt dabei aus der zweiten Bemerkung des vorigen Abschnittes und verbleibt als Übung. Es ist schließlich $\sigma(X) = \sqrt{\frac{35}{6}} \approx 2.42$.

Satz 7.5 Es seien X, Y zwei unabhängige Zufallsvariablen auf dem endlichen Wahrscheinlichkeitsraum (Ω, P). Dann gilt

$$\mathrm{Var}(X+Y) = \mathrm{Var}(X) + \mathrm{Var}(Y).$$

Beweis.

$$\begin{aligned} Var(X+Y) &= E((X+Y)^2) - E(X+Y)^2 \\ &= E(X^2+2XY+Y^2) - (E(X)+E(Y))^2 \\ &= E(X^2) + 2E(XY) + E(Y^2) - E(X)^2 - 2E(X)E(Y) - E(Y)^2 = Var(X) + Var(Y). \end{aligned}$$

Satz 7.6 Es sei die Zufallsvariable X binomialverteilt mit Parametern $n \in \mathbb{N}$ und $p \in [0,1]$. Dann gilt

$$\mathrm{Var}(X) = np(1-p).$$

Beweis. Sei $\Omega = \{0,1\}^n$ und $X_i(\omega_1, \ldots, \omega_n) = \omega_i$. Dann ist $Var(X_i) = p(1-p)$ und somit $Var(X) = np(1-p)$.

Aufgaben

Aufgabe 7.40 (Varianz beim Würfelwurf)
Wir werfen einen unverfälschten Würfel: $\Omega = \{1, \ldots, 6\}$, $X(i) = i$ Laplaceverteilt. Berechnen Sie $\mathrm{Var}(X)$ und σ.

Aufgabe 7.41 Rechnen Sie das Beispiel der letzten Seite nochmals durch, jetzt aber unter Benutzung des Satzes **??**.

Aufgabe 7.42 Eine Urne enthält die Wörter PRIMZAHLEN, HABEN, GENAU, ZWEI TEILER. Ein Wort wird zufällig gezogen. Es sei X die Wortlänge und Y die Anzahl der Vokale im Wort.

1. Berechne $E(X), E(Y), Var(X), Var(Y), \sigma(X), \sigma(Y)$.
2. Bestimme die Wahrscheinlichkeit, dass die Zufallsvariable X mehr als $2\sigma(X)$ oder $3\sigma(X)$ von $E(X)$ abweicht. Analog für Y.

7.10 Das schwache Gesetz der großen Zahlen

Wir beginnen mit der folgenden *Tschebyschoffschen Ungleichung.*

Satz 7.3: Auf dem endlichen Wahrscheinlichkeitsraum sei X eine Zufallsvariable mit Erwartungswert $E(X) = \mu$. Dann gilt für alle $\varepsilon > 0$

$$P(\{\omega \in \Omega \,:\, |X(\omega) - \mu| \geq \varepsilon\}) \leq \frac{\mathrm{Var}(X)}{\varepsilon^2}\,.$$

Beweis. Wir schätzen wie folgt ab

$$\begin{aligned}\mathrm{Var}(X) \;&=\; \sum_{\omega\in\Omega} \big[X(\omega)-\mu\big]^2 P(\{\omega\}) \;\geq \sum_{\omega\,:\,|X(\omega)-\mu|\geq\varepsilon} \big[X(\omega)-\mu\big]^2 P(\{\omega\}) \\ &\geq \sum_{\omega\,:\,|X(\omega)-\mu|\geq\varepsilon} \varepsilon^2 P(\{\omega\}) \;=\; \varepsilon^2 P(\{\omega\in\Omega\,:\,|X(\omega)-\mu|\geq\varepsilon\}).\end{aligned}$$

Umstellen zeigt die Behauptung. ∎

Wir können nun die folgende, auf P.F. Tschebyschoff zurückgehende Formulierung des *schwachen Gesetzes der großen Zahlen* beweisen, eines der zentralen Resultate der klassischen Wahrscheinlichkeitstheorie.

Satz 7.4: Auf dem endlichen Wahrscheinlichkeitsraum seien $X_1, \ldots, X_n$ unabhängige Zufallsvariablen mit $E(X_i) = \mu$ und $\mathrm{Var}(X_i) = V$ für alle $i = 1, \ldots, n$. Für alle $\varepsilon > 0$ gilt dann

$$P(\{\omega \in \Omega \,:\, |\overline{X}_n(\omega) - \mu| \geq \varepsilon\}) \leq \frac{V}{n\varepsilon^2}$$

für den Mittelwert $\overline{X}_n = \frac{1}{n}\,(X_1 + \ldots + X_n)$.

Beweis. Zunächst verifiziert man $E(\overline{X}_n) = \mu$ sowie $\mathrm{Var}(\overline{X}_n) = \frac{V}{n}$. Hiermit werten wir die Tschebyschoffsche Ungleichung für die Zufallsvariable $\overline{X}_n$ auf (Ω, P) aus und erhalten die Behauptung. ∎

Beispiel. Wir würfeln n-mal mit einem unverfälschten Würfel. Nun ist es nicht ausgeschlossen, dass mit jedem Wurf ein 6 fällt. Mit wachsendem n wird die Wahrscheinlichkeit hierfür aber immer kleiner. Wie genau muss das schwache Gesetz der großen Zahlen angewandt werden, um diese Tatsache zu begründen?

Kapitel 8

Der Raum $\mathbb{R}^2$

8.1 Geraden

Geraden in $\mathbb{R}^2$ sind gegeben durch Gleichungen vom Typ

$$ax + by = c.$$

Hierbei sind a, b, c gegeben und a und b nicht beide gleich 0. Genauer ist es, die Menge aufzuschreiben

$$\{(x, y \in \mathbb{R}^2 \colon ax + by = c\}.$$

In SAGEMATH kann man solche Geraden plotten.

```
var('x,y'); implicit_plot(2*x + 3*y -4, (-2,2),(-3,3))
```

Das "var('x,y')" bedeutet, dass sagemath die Variablen x und y kennenlernt. Die Bedeutung von "$(-2, 2)$" ist, dass die Lösungsmengen $2x - 3y - 4 = 0$ im Bereich $x \in (-2, 2)$ gezeichnet wird und von "$(-3, 3)$" im Bereich $y \in (-3, 3)$.
Sind zwei (verschiedene) Geraden gegeben, so haben die entweder genau einen Schnittpunkt oder sie sind parallel und haben keine Punkte gemeinsam. Es seien zwei Geraden gegeben durch die Gleichungen $a_1x + b_1y = c_1$ und $a_2x + b_1y = c_2$. Um den evtl. Schnittpunkt zu bestimmen müssen wir das Gleichungssystem

$$\begin{aligned} a_1x + b_1y &= c_1 \\ a_2x + b_2y &= c_2 \end{aligned}$$

lösen. Sie haben in der Schule gelernt, wie man das macht. So können wir die erste Gleichung mit b_2 multiplizieren, die zweite mit b_1 und subtrahieren. Wir erhalten die Gleichung $(a_1b_2 - a_2b_1)x = c_1b_2 - c_2b_1$, welche wir dann, wenn $a_1b_2 - a_2b_1 \neq 0$ ist, nach x lösen können. Analog können wir für y argumentieren.

Sind zwei Punkte oder Vektoren $a = (a_1, a_2)$ und $b = (b_1, b_2)$ in $\mathbb{R}^2$ gegeben, so definieren wir die Determinante $\det(a, b) := a_1b_2 - a_2b_1$.

Satz 8.1 (Cramersche Regel)
(Cramersche Regel) Sind die nebenstehende Gleichungen mit $(a_1, b_1) \neq (0, 0)$ und $(a_2, b_2) \neq (0, 0)$ gegeben, so gilt

$$\begin{aligned} a_1x + b_1y &= c_1 \\ a_2x + b_2y &= c_2 \end{aligned}$$

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

Ist $\det(a, b) \neq 0$, so gibt es genau eine Lösung. Ist $\det(a, b) = 0$, so hat das Gleichungssystem entweder keine Lösung oder unendlich viele Lösungen.

Beweis. Für $\det(a, b) \neq 0$ muss man prüfen, dass die angegebene Formeln

$$x = \frac{\det(c, b)}{\det(a, b)} \text{ und } y = \frac{\det(a, c)}{\det(a, b)}$$

das Gleichungssystem löst. Das ist eine relativ einfache Aufgabe.
Ist $\det(a,b) = a_1b_2 - a_2b_1 = 0$, so betrachten wir folgende Fälle

- Ist $a_1 = b_1 = 0$, so ist die erste Gleichung $0 = c_1$. Diese ist widersprüchlich wenn $c_1 \neq 0$. Ist $c_1 = 0$ so erhalten wir nur die zweite Gleichung $a_2x + b_2y = c_2$. Diese hat entweder keine oder unendlich viele Lösungen.

- $a_1 \neq 0$. Dann ist $a_2 = a_1 \cdot \lambda$ für ein λ und dann folgt aus $a_1b_2 - a_2b_1 = 0$, dass

$$b_2 = \frac{a_2b_1}{a_1} = \lambda b_1.$$

  Wenn wir die erste Gleichung mit λ multiplizieren so erhalten wir

$$\begin{aligned} a_2x + b_2y &= \lambda c_1 \\ a_2x + b_2y &= c_2. \end{aligned}$$

  Diese Gleichungen sind widerprüchlich oder es gibt unendlich viele Lösungen.

Aufgaben

Aufgabe 8.1 Lösen Sie die nachfolgenden Gleichungssysteme mithilfe des Cramerschen Regels.

1. $\begin{aligned} 3x - y &= 5 \\ x + 2y &= 5 \end{aligned}$

2. $\begin{aligned} 4x - 2y &= 1 \\ 3x + 5y &= 3 \end{aligned}$

3. $\begin{aligned} 2x - 3y &= 7 \\ x + 5y &= -4 \end{aligned}$

4. $\begin{aligned} 2x - 3y &= 3 \\ 4x - 6y &= 5 \end{aligned}$

5. $\begin{aligned} x - 3y &= 1 \\ 3x + 5y &= 5 \end{aligned}$

8.2 Vektoren

Wir stellen einen Vektor $a = (a_1, a_2)$ (Oft auch als $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ geschrieben) bildlich als einen Pfeil dar, welcher in einem beliebigen Punkt (b_1, b_2) entspringt und in dem Punkt $(a_1 + b_1, a_2 + b_2)$ endet. Entspringt der Vektor im Punkt $0 = (0, 0)$, so reden wir von einem **Ortsvektor**.

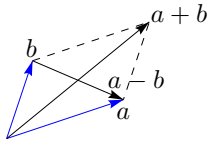
Wir definieren für Ortsvektoren (a_1, a_2), (b_1, b_2) und $\lambda \in \mathbb{R}$:

$$\begin{aligned} (a_1, a_2) + (b_1, b_2) &:= (a_1 + b_1, a_2 + b_2) \\ \lambda(a_1, a_2) &:= (\lambda a_1, \lambda a_2) \end{aligned}$$

Ein Paar von Vektoren $\mathcal{B} = (a, b)$ heißt **Basis** von $\mathbb{R}^2$, wenn es für jeden Vektor c in $\mathbb{R}^2$ genau ein Paar (x, y) von Zahlen gibt mit $c = x \cdot a + y \cdot b$. In diesem Fall nennen wir (x, y) die Koordinaten von c bezüglich der Basis $\mathcal{B}$.
Die Basis $e_1 = (1, 0)$, $e_2 = (0, 1)$ heißt die **Standardbasis** von $\mathbb{R}^2$.

Um festzustellen ob (a, b) eine Basis von $\mathbb{R}^2$ ist, müssen wir für jedes $c \in \mathbb{R}^2$ die Gleichung $c = x \cdot a + y \cdot b$ nach x und y lösen. Das führt zum Gleichungssystem

$$\begin{aligned} a_1 x + b_1 y &= c_1 \\ a_2 x + b_2 y &= c_2. \end{aligned}$$



Dieses Gleichungssystem ist eindeutig nach x und y lösbar genau dann, wenn $\det(a, b) \neq 0$.
Eine Gerade gegeben durch eine Gleichung $a_1 x + a_2 y = b$ können wir auch durch eine sogenannte Parametersdarstellung geben. Dazu folgende Definition.

Ist $a = (a_1, a_2) \in \mathbb{R}^2$, so definieren wir $a^\perp := (-a_2, a_1)$. Wir sagen, dass b senkrecht auf a steht, Notation $a \perp b$, wenn $b = \lambda \cdot a^\perp$ ist für ein $\lambda \in \mathbb{R}$.

Ist $a \neq (0, 0)$, z.B. $a_1 \neq 0$, so können wir y beliebig nehmen, zum Beispiel $y = \lambda \cdot a_1$ für $\lambda \in \mathbb{R}$ beliebig. Dann können wir die Gleichung **??** nach x lösen und erhalten

$$(x, y) = \lambda \cdot (-a_2, a_1) + (b/a_1, 0).$$

Analog argumentiert man, wenn $a_2 \neq 0$. Wir erhalten, dass die Gerade gegeben ist durch die Parameterdarstellung

$$\mathbb{R} \cdot a^\perp + (b/a_1, 0) := \{\lambda \cdot a^\perp + (b/a_1, 0) \colon \lambda \in \mathbb{R}\}$$

Der Vektor $a^\perp$ heißt Richtungsvektor der Gerade und $(b/a_1, 0)$ heißt Stützvektor. Jeder Vektor auf der Gerade kann als Stützvektor genommen werden.
Beispiel. Die Gerade mit Gleichung $2x + 3y = 4$ hat eine Parameterdarstellung $\mathbb{R} \cdot (-3, 2) + (2, 0)$.

Aufgaben

Aufgabe 8.2 Es seien a, b, c Vektoren und λ, μ reelle Zahlen. Zeigen Sie:

1. $\lambda \cdot (a + b) = \lambda \cdot a + \lambda \cdot b$
2. $(\lambda + \mu) \cdot a = \lambda \cdot a + \mu \cdot a$
3. $(a + b) + c = a + (b + c)$
4. $a + b = b + a$

Aufgabe 8.3 Es sei $a = (2, -1)$ und $b = (-1, 2)$.

1. Zeigen Sie, dass (a, b) eine Basis ist.
2. Sei $c = (3, 4)$. Berechnen Sie die Koordinaten von c bezüglich der Basis (a, b).

Aufgabe 8.4 1. Sei $a = (3, -1)$ und $b = (2, 1)$. Zeigen Sie, dass (a, b) eine Basis ist.

2. Berechnen Sie die Koordinaten von $(-1, 1)$, $(1, 3)$ und $(3, 4)$ bezüglich der Basis (a, b).

Aufgabe 8.5 Zeigen Sie:

1. $\det(a, a) = 0$
2. $\det(a, b) = -\det(b, a)$
3. $\det(a + c, b) = \det(a, b) + \det(c, b)$
4. $\det(\lambda \cdot a, b) = \lambda \cdot \det(a, b)$

Aufgabe 8.6 Bestimmen Sie für jede nachfolgende Gerade eine Gleichung.

1. $(1, 3) + \mathbb{R} \cdot (2, -1)$
2. $(4, 1) + \mathbb{R} \cdot (1, -1)$
3. $(0, 1) + \mathbb{R} \cdot (1, 0)$

Aufgabe 8.7 Bestimmen Sie eine Parameterdarstellung für die nachfolgenden Geraden.

1. $x + y = 3$
2. $3x - 4y = -4$
3. $2x + y = 5$

Aufgabe 8.8 Es seien ℓ, m zwei verschiedene Geraden. Zeigen Sie, dass der Durchschnitt entweder leer ist oder aus genau einem Punkt besteht.

Aufgabe 8.9 Es seien a, b verschiedene Punkte in $\mathbb{R}^2$. Zeigen Sie:

1. Es gibt genau eine Gerade ℓ mit $a \in \ell$ und $b \in \ell$.
2. Zeigen Sie, dass eine Gleichung der Geraden durch a und b gegeben wird durch $\det(x - a, b - a) = 0$ (siehe Aufgabe 8.5).
3. Bestimmen Sie außerdem einen Stützvektor und einen Richtungsvektor von ℓ.

Aufgabe 8.10 1. Sei $a = (2, 1)$ und $b = (4, -1)$. Bestimmen Sie eine Gleichung der Geraden durch a und b.

2. Führen Sie die gleiche Aufgabe durch für $a = (3, -2)$ und $b = (-2, 1)$.

Aufgabe 8.11 1. Es seien a, b, c drei Punkte in $\mathbb{R}^2$. Zeigen Sie: a, b, c liegen auf einer Geraden genau dann, wenn $\det(c - a, b - a) = 0$.

2. Prüfen Sie, ob $(3, 2)$, $(6, -1)$ und $(2, 3)$ auf einer Geraden liegen.

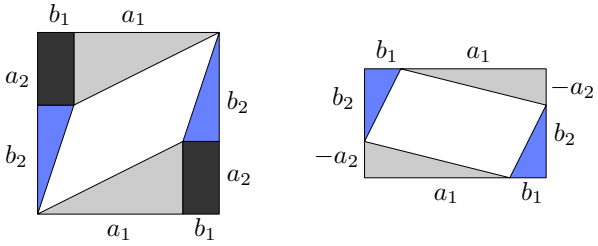
3. Die Punkte $(p, 3)$, $(8, 1)$ und $(3, 5)$ liegen auf einer Geraden. Bestimmen Sie p.

8.3 Pythagoras

Sind a, b zwei Vektoren in $\mathbb{R}^2$, so können wir das Parallelogramm

$$P(a,b) = \{x \cdot a + y \cdot b \colon 0 < x, y < 1\}$$

betrachten. Wir interessieren uns für den Flächeninhalt.



Für den Fall, dass a und b beide im ersten Quadranten liegen, betrachte das linke Bild. Das große Quadrat hat die Fläche $(a_1 + b_1) \cdot (a_2 + b_2)$. Verschiebe das obere graue Dreieck über den Vektor $-b$. Wir sehen, dass die grauen Dreiecke zusammen die Fläche $a_1 \cdot a_2$ haben. Ebenso haben die zwei blauen Dreiecke zusammen die Fläche $b_1 b_2$. Die zwei schwarzen Rechtecke haben beide die Fläche $a_2 b_1$. Deshalb hat das weiße Parallelogramm $P(a,b)$ die Fläche

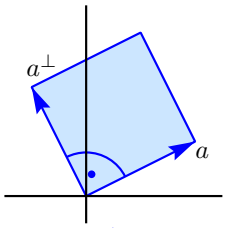
$$(a_1 + b_1) \cdot (a_2 + b_2) - a_1 \cdot a_2 - b_1 \cdot b_2 - 2 \cdot a_2 \cdot b_1 = a_1 b_2 - a_2 b_1.$$

Für den Fall, dass b im ersten Quadranten und a im zweiten Quadranten liegt, also $a_2 < 0$ ist, betrachte das Bild rechts. Die anderen Fälle sind analog. Wir erhalten den nachfolgenden Satz.

Satz 8.2 Die Fläche eines Parallelogramms $P(a,b)$ ist gleich $|\det(a,b)|$.

Ist $b = a^\perp$, so ist die Fläche des Quadrats $P(a, a^\perp)$ gleich $a_1^2 + a_2^2$, das Quadrat der Länge einer Seite des Quadrats. Somit gilt:

Die Länge eines Vektors $a = (a_1, a_2)$ ist gleich $\sqrt{a_1^2 + a_2^2}$.



Aus $\|a - b\|^2 = (a_1 - b_1)^2 + (a_2 - b_2)^2 = a_1^2 + a_2^2 + b_1^2 + b_2^2 - 2(a_1 b_1 + a_2 b_2)$ folgt:

Satz 8.3 (Pythagoras) Ist $a \perp b$, so gilt $\|a - b\|^2 = \|a\|^2 + \|b\|^2$.

Aufgaben

Aufgabe 8.12 1. Berechnen Sie die Fläche des Parallelogramms, aufgespannt durch die Vektoren $(3, 2)$ und $(-3, 4)$.

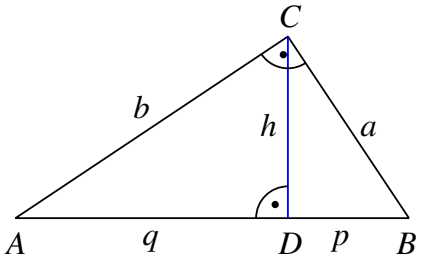
2. Führen Sie die gleiche berechnung durch für das Parallelogramm, aufgespannt durch die Vektoren $(1, 4)$ und $(3, 5)$.

Aufgabe 8.13 (Satz von Thales) Es seien a und b Vektoren mit $\|a\| = \|b\|$. Zeigen Sie, dass $a - b \perp a + b$. Zeichnen Sie ein Bild hierzu.

Aufgabe 8.14 1. Es sei ℓ eine Gerade und C ein Punkt in $\mathbb{R}^2$ mit $C \notin \ell$. Zeigen Sie, dass es genau ein Punkt D auf ℓ gibt, sodass $C - D$ ein Normalenvektor von ℓ ist. Wir nennen D den Fußpunkt von D auf ℓ.

2. **(Höhensatz)** Sei ABC ein Dreieck mit Seitenlängen a, b, c und ℓ die Gerade durch A und B. Sei D der Fußpunkt von C auf ℓ. Sei $p = \|D - B\|$, $q = \|D - A\|$ und $h = \|D - C\|$. Nehmen Sie an, dass $C - A \perp D - A$. Zeigen sie, dass $h^2 = pq$.

3. **(Kathetensatz)** Zeigen Sie unter den gleichen Voraussetzungen, dass $a^2 = pc$ und $b^2 = qc$.

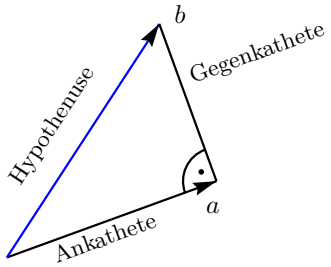


8.4 Winkel, Sinus, Cosinus

Definitionsgemäß gilt für $a, b \in \mathbb{R}^2$, beide ungleich $(0,0)$:

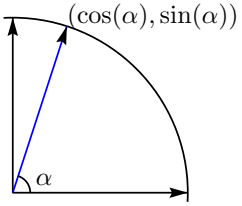
1. $\angle(a,a) = 0°$
2. $\angle(a,-a) = 180°$.
3. $\angle(a,a^\perp) = 90°$.
4. Liegt b links von a, so ist $\angle(a,b) > 0$.
5. $\angle(a,b) = -\angle(b,a)$ wenn $b \notin \mathbb{R}\cdot a$.
6. $\angle(\lambda a, b) = \angle(a,b)$ wenn $\lambda > 0$.
7. Ist $\|a\| = \|b\|$ und $m = a+b$, so ist m der Winkelhalbierende, also $\angle(a,m) = \angle(m,b)$.

Aus der Schule sind die Begriffe Sinus und Cosinus bekannt. Ist eine rechtwinkliges Dreieck gegeben, so gilt



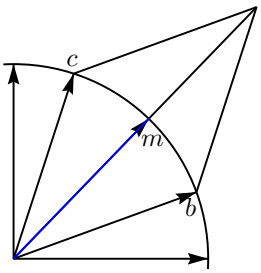
$$\sin(\angle(a,b)) = \frac{\text{Gegenkathete}}{\text{Hypothenese}}$$
$$\cos(\angle(a,b)) = \frac{\text{Ankathete}}{\text{Hypothenese}}$$

Hierbei ist $\cos(\angle(a,b))$ positiv, wenn der Winkel spitz ist, negativ wenn er stumpf und gleich 0, wenn $a \perp b$. Ausserdem ist $\sin(\angle(a,b))$ positiv, wenn der Winkel $\angle(a^\perp,b)$ spitz ist und negativ, wenn er stumpf ist und gleich 0, wenn $b \in \mathbb{R}\cdot a$. Ist $\alpha = \angle(e,a)$, $e = (1,0)$ und $\|a\| = 1$, so ist definitionsgemäß $a = (\cos(\alpha), \sin(\alpha))$.



Es gibt eine einfache Methode umd $\cos(\alpha)$ und $\sin(\alpha)$ aus α annährend zu berechnen, und wir illustrieren dies für α zwischen 0° und 90°.

Sind $b = (b_1, b_2)$ und $c = (c_1, c_2)$ auf dem Einheitskreis im ersten Quadrant gegeben, so gilt für die Mittelhalbierende m mit $\|m\| = 1$:



$$m = \frac{1}{\sqrt{2 + 2\cdot b_1c_1 + 2b_2c_2}} \cdot (b_1 + c_1, b_2 + c_2). \quad (8.1)$$

Sei $e = (1,0)$, $\beta = \angle(e,b)$ und $\gamma = \angle(e,c)$. Sind somit $b_1 = \cos(\beta), b_2 = \sin(\beta), c_1 = \cos(\gamma)$ und $c_2 = \sin(\gamma)$ bekannt, so kann man mit der Formel (8.1) $\cos((\beta+\gamma)/2)$ und $\sin((\beta+\gamma)/2))$ berechnen.

Sei $A = \alpha/90 \in (0,1)$ und schreibe A im Binärsystem aus:

$$A = A_{-1}2^{-1} + A_{-2}2^{-2} + A_{-3}2^{-3} + \cdots$$

Definiere $b^{(0)} = (1,0)$ und $c^{(0)} = (0,1)$. Sind induktiv $b^{(k)}$ und $c^{(k)}$ gegeben mit:

$$\|b^{(k)}\| = \|c^{(k)}\| = 1$$

so bestimme die Winkelhalbierende $m = (m_1, m_2)$ wie in der Formel (8.1). Wir gehen folgendermaßen vor:

- Ist $A_{-k-1} = 1$, so setze $b^{(k+1)} = m$ und $c^{(k+1)} = c^{(k)}$.
- Ist $A_{-k-1} = 0$, so setze $b^{(k+1)} = b^{(k)}$ und $c^{(k+1)} = m$.

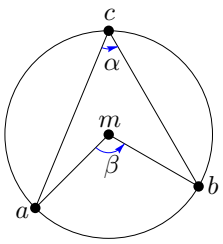
Dann ist $(b_1^{(k)}, b_2^{(k)})$ für großes k eine gute Annäherung von $(\cos(\alpha), \sin(\alpha))$.

Aufgabe 8.15 Es sei $x \in [0, 1)$, $a = (x, \sqrt{1-x^2})$ und $e = (1, 0)$. Schreiben Sie, mit der Halbierungsmethode, ein Computerprogramm `winkel(x,n)`, das $\angle(e, a)$ im Grad in n Schritte annäherend berechnet.

Aufgabe 8.16 Warum ist die Summe der Winkel in einem Dreieck gleich 180°? Warum ist die Summe der Winkel in einem Viereck gleich 360°?

Aufgabe 8.17 Es sei K ein Kreis mit Mittelpunkt m und a, b, c Punkte auf dem Kreis. Sei $\alpha = \angle(a - c, b - c)$ und $\beta = \angle(a - m, b - m)$. Zeigen Sie, dass $2\alpha = \beta$. Insbesondere ist der Winkel α "unabhängig von c".

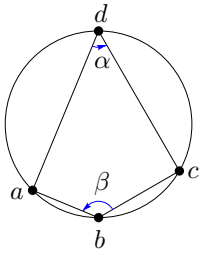
Tipp: Zeichnen Sie das Geradenstück von m nach c.



Aufgabe 8.18 (Sehnenviereck)

Es sei $abcd$ ein Viereck, wie nebenstehend gezeichnet. Nehmen Sie an, dass a, b, c, d auf einem Kreis liegen. Sei $\alpha = \angle(a-d, c-d)$ und $\beta = \angle(c-b, a-b)$. Zeigen Sie, dass $\alpha + \beta = 180°$ ist.

Tipp: Sei m der Mittelpunkt des Kreises. Wenden Sie den Satz über Peripheriewinkel an.

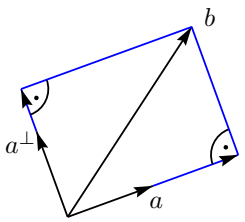


Nun addieren und folgern Sie, dass $2\alpha + 2\beta = 360°$.

Aufgabe 8.19 Zeigen Sie:
1. $\cos(90° - \alpha) = \sin(\alpha)$.
2. $\sin(90° - \alpha) = \cos(\alpha)$
3. $\cos(180° - \alpha) = -\cos(\alpha)$
4. $\sin(180° - \alpha) = \sin(\alpha)$ Was gilt für $\sin(90° - \alpha)$?

8.5 Skalarprodukt und Additionstheoreme

Ist $a \neq (0,0)$, so ist $(a, a^\perp)$ eine Basis von $\mathbb{R}^2$, denn $\det(a, a^\perp) = a_1^2 + a_2^2 \neq 0$. Ist somit $b \in \mathbb{R}^2$ gegeben, so können wir x und y finden, sodass $b = x \cdot y + y \cdot a^\perp$. Diese x und y können wir ausrechnen in Terme von a und b. Man rechnet nach, dass



$$b = \frac{\langle a, b\rangle}{\|a\|^2} \cdot a + \frac{\det(a,b)}{\|a\|^2} \cdot a^\perp. \qquad (8.2)$$

wobei $\langle a, b\rangle$ das sogenannte Skalarprodukt von a und b ist:

$$\langle a, b\rangle := a_1 b_1 + a_2 b_2$$

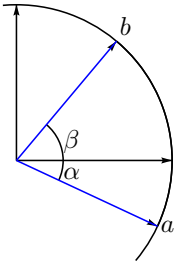
Hieraus können wir die Gegenkathete ausrechnen als $\det(a,b)/\|a\|$ und die Ankathete als $\langle a, b\rangle/\|a\|$, weil $\|a^\perp\| = \|a\|$. Hieraus erhalten wir folgender Satz.

Satz 8.4 Für $a, b \in \mathbb{R}^2$ gelten die Formeln:

$$\begin{aligned} \det(a,b) &= \|a\| \cdot \|b\| \sin(\angle(a,b)) \\ \langle a, b\rangle &= \|a\| \cdot \|b\| \cos(\angle(a,b). \end{aligned}$$

Es seien

$$\begin{aligned} a &= (\cos(\alpha), -\sin(\alpha)) \\ b &= (\cos(\beta), \sin(\beta). \end{aligned}$$



Dann gilt $\|a\| = \|b\| = 1$ und $\angle(a,b) = \alpha + \beta$. Somit folgt durch eine direkte Anwendung von Satz 8.4 folgende Additionstheoreme.

Satz 8.5 (Additionstheoreme für sinus und cosinus)

$$\begin{aligned} \sin(\alpha+\beta) &= \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta) \\ \cos(\alpha+\beta) &= \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta) \end{aligned}$$

Aufgabe 8.20 Rechnen Sie die Gleichung 8.2 nach.

Aufgabe 8.21 Es seien a, b zwei Elemente in $\mathbb{R}^2$, beide ungleich $(0,0)$. Schreiben Sie ein Programm `winkel(a,b,n)` das der Winkel $\angle(a,b)$ zwischen $-180°$ und $180°$ ausrechnet.

Aufgabe 8.22 Zeigen Sie für $a, b \in \mathbb{R}^2$L mit $a \neq (0,0)$:

1. $\|b\|^2 = \frac{\langle a,b\rangle^2 + \det(a,b)^2}{\|a\|^2}$, wenn $a \neq (0,0)$.
2. Die Cauchy-Schwarz Ungleichung $|\langle a, b\rangle| \leq \|a\| \cdot \|b\|$
3. Die Dreiecksungleichung:

$$\|a + b\| \leq \|a\| + \|b\| \text{Dreiecksungleichung}$$

Aufgabe 8.23 Warum gilt $\sin(\angle(b,a)) = -\sin(\angle(a,b))$ und $\cos(\angle(b,a)) = \cos(\angle(a,b))$?

Aufgabe 8.24 Zeigen Sie die nachfolgenden Formeln.

1. $\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha)$
2. $\cos(2\alpha) = \cos^2(\alpha) - \sin^2(\alpha)$
3. $\cos(\alpha/2) = \pm\sqrt{\frac{1}{2}(1 + \cos(\alpha))}$
4. $\sin(\alpha/2) = \pm\sqrt{\frac{1}{2}(1 - \cos(\alpha))}$

Aufgabe 8.25 Geben Sie, nur ausgehend von $\sin(0°) = 0$, $\sin(90°) = 1$ und $\cos(60°) = 1/2$, exakte algebraische Formeln für die nachfolgenden Zahlen. Berechnen Sie diese danach mit dem Taschenrechner und vergleichen Sie Ihr Ergebnis mit der sin- und cos-Taste.

1. $\sin(30°)$
2. $\sin(15°)$
3. $\cos(75°)$
4. $\sin(22,5°)$
5. $\sin(67,5°)$
6. $\sin(7,5°)$

Aufgabe 8.26 (Rechenregeln für das Skalarprodukt) Zeigen Sie:

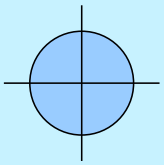
1. $\langle a + b, c\rangle = \langle a, c\rangle + \langle b, c\rangle$
2. $\langle a, b\rangle = \langle b, a\rangle$
3. $\langle \lambda a, b\rangle = \lambda \cdot \langle a, b\rangle$
4. $\langle a, a\rangle = \|a\|^2$.

Aufgabe 8.27 Zeigen Sie die **Cosinusregel**: Es gilt

$$\|v - w\|^2 = \|v\|^2 + \|w\|^2 - 2\|v\| \cdot \|w\| \cdot \cos(\angle(v,w)).$$

8.6 Das Winkelmaß und seine Berechnung

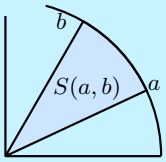
1. Wir definieren die Kreiszahl π als die Fläche des Einheitskreises $\{(x,y) \in \mathbb{R}^2 \colon x^2 + y^2 < 1\}$.



2. Für $(a,b) \in \mathbb{R}^2$, $a, b \neq (0,0)$ mit $\det(a,b) > 0$ definieren wir das Winkelmaß $\angle(a,b)$ als **zweimal** die Fläche des Sektors $S(a,b)$ definiert durch

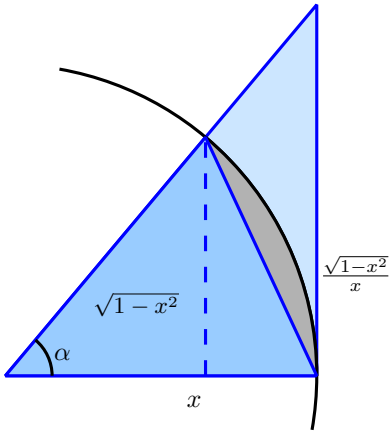
   $$\{\lambda \cdot a + \mu \cdot b \colon \lambda, \mu > 0\} \cap \{(x,y) \in \mathbb{R}^2 \colon x^2 + y^2 < 1\}.$$

   Ist $\det(a,b) < 0$, so definieren wir $\angle(a,b) = -\angle(b,a)$. Weiterhin $\angle(a, \lambda a) = 0$ für $\lambda > 0$ und $\angle(a, \lambda a) = \pi$, für $\lambda < 0$.



Sei $a = (1,0)$, $b = (x, \sqrt{1-x^2})$ und $\alpha = \angle(a,b)$. so möchten wir das Winkelmaß von $\alpha = \angle(a,b)$ berechnen. Dazu betrachten wir $x = \cos(\alpha)$. Ist $0 < x < 1$, so sehen wir mit dem nebenstehende Bild durch Betrachten der Flächen zweier Dreiecke, dass

$$\sqrt{1-x^2} \leq \alpha \leq \frac{\sqrt{1-x^2}}{x}$$



Die Idee ist jetzt, statt α den Winkel $\alpha_n = \alpha/2^n$ zu betrachten. Betrachte $P_0 = (x, \sqrt{1-x^2}) =: (x_0, y_0)$ und Induktiv P_n die Mitte zwischen P_{n-1} und $(1,0)$, also mit $P_n = (x_n, y_n)$ gilt

$$\begin{aligned} x_n &= \frac{x_{n-1}+1}{\sqrt{2+2x_{n-1}}} = \sqrt{(1+x_{n-1})/2} \\ y_n &= \frac{y_{n-1}}{\sqrt{2+2x_{n-1}}} = \frac{y_{n-1}}{2x_n} \end{aligned}$$

Somit gelten die Ungleichung

$$y_n \leq \frac{\alpha}{2^n} \leq y_n/x_n$$

Sei $f_n = 2^n y_n$. Dann gilt

$$\begin{aligned} f_0 &= \sqrt{1-x^2} \\ x_0 &= x \\ x_n &= \sqrt{(1+x_{n-1})/2} \\ f_n &= f_{n-1}/x_n \\ f_n &\leq \arccos(x) \leq f_n/x_n. \end{aligned}$$

Die Zahlen f_n und f_n/x_n nähern sich immer besser den Winkel $\alpha = \arccos(x)$ an, weil die Zahl x_n und somit $1/x_n$ sich die Zahl 1 immer besser annähert, je größer n wird. Wir erhalten folgendes Programm zur Berechnung von α in Bogenmaß, wenn $x = \cos(\alpha)$ gegeben ist. Dies funktioniert für alle x mit $-1 < x \leq 1$.

```
def acos(x,n):
    x = N(x); f = sqrt(1-x**2)
    for i in range(n):
        x = sqrt((1+x)/2)
        f = f/x
    return f
```

Insbesonder erhalten wir für $x = 0$ eine Annäherung der Zahl $\pi/2$.

Aufgaben

Aufgabe 8.28 Nehmen Sie die Bezeichnung x_n der vorherigen Seite und sei $f_n = 2^n\sqrt{1-x_n^2}$.

1. Zeigen Sie, dass $x_{n-1} < x_n < 1$ für jedes n.
2. Folgern Sie, dass $f_{n-1} < f_n$ für jedes $n \geq 1$.
3. Zeigen Sie, dass $\dfrac{f_n}{x_n} < \dfrac{f_{n-1}}{x_{n-1}}$ für jedes $n \geq 1$.

Aufgabe 8.29 1. Sei $a = (3,1)$ und $b = (2,4)$. Zeigen Sie, dass $\cos(\angle(a,b)) = \sin(\angle(a,b)) = \frac{1}{2}\sqrt{2}$, und folgern Sie, dass $\angle(a,b) = 45^{\text{o}}$.

2. Sei $a = (2,1)$ und $b = (-3,4)$. Berechnen Sie $\cos(\alpha)$ und bestimmen Sie danach mithilfe eines Taschenrechners $\angle(a,b)$.

Aufgabe 8.30 Zeigen Sie die Formel von Heron. Ist ein Dreieck mit Seitenlängen a, b, c gegeben, $s = (a+b+c)/2$ und F die Fläche des Dreiecks, so gilt $F^2 = s \cdot (s-a) \cdot (s-b) \cdot (s-c)$.

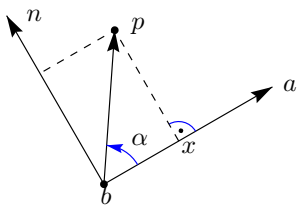
8.7 Abstände

Es gibt zwei Methoden, den Abstand eines Punktes zu einer Geraden zu berechnen: einmal mit der Gleichung und einmal mit der Parameterdarstellung.

Satz 8.6 1. Der Abstand von p zur Gerade $b + \mathbb{R} \cdot a$ ist gleich $\dfrac{|\det(p-b,a)|}{\|a\|}$.

2. Der Abstand von p zur Gerade $\langle n, x\rangle = c$ ist $\dfrac{|\langle n,p\rangle - c|}{\|n\|}$.

Beweis. 1. Für alle $x = b + t \cdot a$ gilt $\det(x - p, a) = \det(b - p, a)$. Es gilt $\det(x - p, a) = \|x - p\| \cdot \|a\| \sin(\angle(x - p, a))$. Deshalb ist die Länge $\|x - p\|$ minimal, wenn $\angle(x - p, a) = \pm 90^0$, also $x - p \perp a$. Sei n senkrecht auf a. Schneide nun die Gerade $p + \mathbb{R} \cdot n$ mit $b + \mathbb{R} \cdot a$, um den Punkt mit minimalem Abstand zu finden. Der Sinus ist dann gleich 1.



2. Die Aussage ist unabhängig von dem gewählten Normalenvektor n. Ist $a = (a_1, a_2)$, so nehmen wir $n = a^\perp = (-a_2, a_1)$. Eine Gleichung der Geraden $b + \mathbb{R} \cdot a$ ist $\langle n, x\rangle = \langle n, b\rangle$. Nun bemerke, dass $\det(a, b) = \langle a^\perp, b\rangle$, und setze in die erste Aussage ein.

Satz 8.7 1. Sind a, b zwei Vektoren in $\mathbb{R}^2$, so haben die Punkte der Winkelhalbierenden $\mathbb{R} \cdot (\|b\| \cdot a + \|a\| \cdot b)$ gleichen Abstand zu $\mathbb{R} \cdot a$ und $\mathbb{R} \cdot b$.

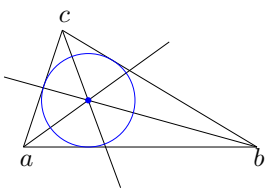
2. Die drei Winkelhalbierenden eines Dreiecks gehen durch einen Punkt.

Beweis. 1. Sei $v = \|b\| \cdot a + \|a\| \cdot b$. Der Abstand von $\lambda \cdot v$ zu $\mathbb{R} \cdot a$ und zu $\mathbb{R} \cdot b$ ist gleich

$$\lambda |\det(a, b)| = |\det(\lambda \cdot v, a)|/\|a\| = |\det(\lambda \cdot v, b)|/\|b\|.$$

2. Sei $C = \|b-a\|$, $B = \|c-a\|$ und $A = \|b-c\|$. Die Winkelhalbierende durch a hat die Parametrisierung $a + \mathbb{R} \cdot (C \cdot (c-a) + B \cdot (b-a))$. Einsetzen von $1/(A + B + C)$ für die Parameter gibt

$$\frac{1}{A+B+C}(A \cdot a + B \cdot b + C \cdot c)$$



auf der Winkelhalbierenden durch a. Genauso zeigt man, dass dieser Punkt auf den anderen Winkelhalbierenden liegt (Symmetrie). ∎

Aufgabe 8.31 Der Punkt $(a, 1)$ habe zu der Geraden ℓ mit der Gleichung $3x-4y = 1$ den Abstand 5. Berechnen Sie a.

Aufgabe 8.32 Die Gerade ℓ habe den Stützvektor $(1, 3)$ und Richtungsvektor $(-2, 1)$. Berechnen Sie den Abstand von P zu ℓ für die nachfolgenden Punkte.

1. $P = (1, 0)$ 2. $P = (0, 1)$ 3. $P = (0, 0)$ 4. $P = (-1, 2)$ 5. $P = (19, 9)$

Aufgabe 8.33 Es sei ℓ die Gerade mit der Gleichung $3x + y = 4$. Bestimmen Sie alle Punkte der Ebene, welche einen Abstand $\sqrt{10}$ zu ℓ haben.

Aufgabe 8.34 Es sei C der Kreis, der gegeben ist durch die Gleichung $x^2 + y^2 + 4x - 9 = 0$. Bestimmen Sie die Punkte von C, welche einen Abstand $\sqrt{2}$ zu der Geraden mit der Gleichung $x + y = 1$ haben.

Aufgabe 8.35 Gegeben ist eine Gerade m durch die Gleichung $3x - y = 6$ und die Gerade ℓ mit Stützvektor $(-2, 3)$ und Richtungsvektor $(2, 1)$. Bestimmen Sie die Punkte von ℓ, welche Abstand $\sqrt{10}$ zu m haben.

Aufgabe 8.36 Gegeben sei die Gerade ℓ mit der Gleichung $2x+y = 3$ und der Punkt $Q = (2, 0)$. Bestimmen Sie alle Punkte P mit der Eigenschaft, dass der Abstand von P zu Q gleich dem Abstand von P zu ℓ ist.

Aufgabe 8.37 Es seien ℓ und m zwei verschiedene Geraden. Zeigen Sie die nachfolgenden Aussagen.

1. Ist ℓ zu m parallel, also $\ell \cap m = \emptyset$, so ist die Menge $\{P\colon d(P, \ell) = d(P, m)\}$ eine Gerade.

2. Ist dagegen der Durchschnitt von ℓ und m ein Punkt, so ist die Menge $\{P\colon d(P, \ell) = d(P, m)\}$ die Vereinigung zweier Geraden.

Aufgabe 8.38 Es sei ℓ eine Gerade, gegeben durch die Gleichung $5x + 12y = 3$. Bestimmen Sie alle Punkte $P \in \mathbb{R}^2$ mit $d(P, \ell) = 1$.

Aufgabe 8.39 Gegeben sind die Punkte $P = (4, -2)$ und $Q = (3, 1)$. Bestimmen Sie die Punkte R, für die gilt: $\angle RPQ = 30°$ und die Fläche des Dreiecks PQR ist gleich 10.

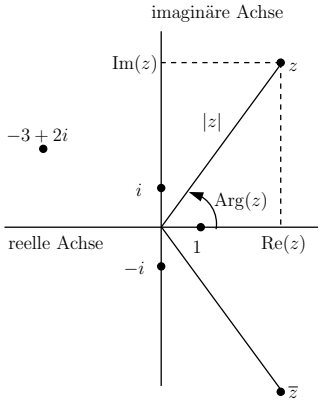
8.8 Komplexe Zahlen

Komplexe Zahlen sind Zahlen z der Gestalt $z = a + b \cdot i$, wobei a und b reelle Zahlen sind und i ein Symbol ist. Ist $z = a + bi$, so nennen wir:

1. $a = \mathrm{Re}(z)$ den Realteil von z und $b = \mathrm{Im}(z)$ den Imaginärteil von z.
2. $|z| := \sqrt{a^2 + b^2}$ den Betrag von z.
3. $\mathrm{Arg}(z) := \angle\big((1,0), z\big) \in (-\pi, \pi]$ das Argument von z
4. $\overline{z} := a - b \cdot i$ die komplex konjugierte von z.

Die Menge der komplexen Zahlen bezeichnen wir mit $\mathbb{C}$.

Eine komplexe Zahl $a + bi$ ist deshalb ein Punkt in der Ebene. Diese Ebene wird in diesem Zusammenhang auch *komplexe Ebene* genannt. Wir schreiben kurz a für $a + 0i$. Jede reelle Zahl werden wir auf diese Weise als komplexe Zahl auffassen. Die reellen Zahlen korrespondieren mit den Punkten auf der Geraden gegeben durch die Gleichung $y = 0$. Die Zahlen der Form $b \cdot i$ nennen wir die rein imaginären Zahlen.
Der Term Zahlen, statt Punkte, für komplexe Zahlen ist dadurch gerechtfertigt, dass wir für komplexe Zahlen eine Addition und Multiplikation definieren.



Es seien $z = a + bi$ und $w = c + di$ komplexe Zahlen. Wir definieren die Summe $z + w = (a + bi) + (c + di)$ und das Produkt $z \cdot w = (a + bi) \cdot (c + di)$ durch

$$(a + bi) + (c + di) := (a + c) + (b + d)i\ , \quad (a + bi) \cdot (c + di) := (ac - bd) + (ad + bc)i\ .$$

Man prüft, dass die Addition und Multiplikation die Assoziativ- und Kommutativgesetze erfüllen. Auch das Distributivgesetz ist gültig.
Die Addition und Multiplikation von komplexen Zahlen ist nicht schwer. Man rechnet mit i wie mit einem Symbol, wobei man jedes Mal, wenn ein i^2 auftritt, dieses durch -1 ersetzen kann. In der Tat ist $i = 0 + 1i$ eine Zahl mit $i^2 = -1$. Bemerke, dass die Dreiecksungleichung gilt: $|z + w| \leq |z| + |w|$. Diese Aussage wurde in Aufgabe **??** behandelt.

Satz 8.8 Für alle $z \in \mathbb{C}$ mit $z \neq 0$ existiert ein $w \in \mathbb{C}$ mit $z \cdot w = 1$.

Beweis. Ist $z = (a + bi)$, so nehme $w = \dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2} i$. Man rechnet nach, dass $z \cdot w = 1$. ∎

Aufgaben

Aufgabe 8.40 Schreiben Sie die nachfolgenden komplexen Zahlen in der Form $a+bi$ mit $a, b \in \mathbb{R}$ und zeichnen Sie diese in der komplexen Ebene.

1. $(1-i)+(3+4i)$
2. $2(3-i)+3(-1-i)$
3. $3(-1+i)-4(2-3i)$
4. $3(1+i)(2-i)$
5. $\dfrac{2+i}{3-i}$
6. $\dfrac{(2+i)(7+5i)}{3-i}$
7. $(1+i)^5$
8. $(-1+2i)^2$
9. $(-1+2i)^{-2}$
10. $\dfrac{3-i}{1+2i}$

Aufgabe 8.41 Es seien z, w komplexe Zahlen. Zeigen Sie:

1. $\overline{z+w} = \overline{z} + \overline{w}$
2. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$
3. Ist $z \neq 0$, so ist $\overline{1/z} = 1/\overline{z}$

Aufgabe 8.42 Gegeben sind folgende komplexe Zahlen:

$$z_1 := -\frac{1-i}{2+i} - \frac{3+i}{4}\,, \quad z_2 := \frac{(1+i)^2}{2} - \frac{6+5i}{i^3}\,.$$

Vervollständigen Sie die nachfolgende Tabelle.

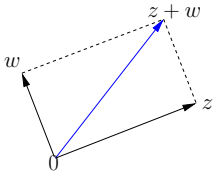
$\mathrm{Re}(z_1)$	$\mathrm{Im}(z_1)$	$\lvert z_1\rvert$	$\mathrm{Re}(z_2)$	$\mathrm{Im}(z_2)$	$\lvert z_2\rvert$	$\mathrm{Re}(z_1+z_2)$	$\mathrm{Im}(z_1+z_2)$	$\lvert z_1+z_2\rvert$

Aufgabe 8.43 Berechnen Sie den Betrag und das Argument der nachfolgenden komplexen Zahlen.

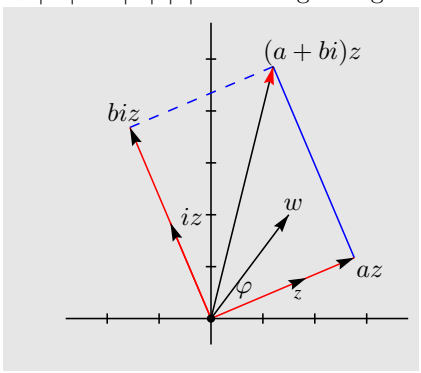
1. $-2+2i$
2. $4-4\sqrt{3}i$
3. $1+i\sqrt{3}$
4. $-5i$
5. -3
6. $3+4i$
7. $-1+i$
8. $(1+i)^{10}$

8.9 Geometrie der Addition und Multiplikation

Die Addition und Multiplikation kann man geometrisch schön interpretieren. Für die Addition $z + w$ ist dies einfach die Vektoraddition, welche Sie aus der Schule kennen, siehe das nebenstehende Bild.

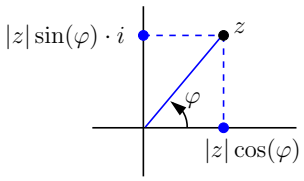


Auch die Multiplikation hat eine schöne Interpretation. Wir schreiben hierzu $w = a + bi$ aus und betrachten die Multiplikation mit w. Zunächst betrachten wir $a \in \mathbb{R}$. Die Multiplikation mit a ist eine Streckung mit dem Faktor a. Ist $z = c + di$, so ist $iz = -d + ci$. Wir können somit iz identifizieren mit $(c, d)^\perp$. Somit ist Multiplikation mit i eine Drehung über 90°. Multiplikation mit bi is somit eine Drehung über 90°, gefolgt durch Streckung mit dem Faktor b.
Somit gilt für den Winkel α zwischen z und wz, dass $\tan(\alpha) = \frac{\sin(\alpha)}{\cos(\alpha)} = b/a = \tan(\mathrm{Arg}(w))$. Somit ist der Winkel zwischen z und wz genau $\mathrm{Arg}(z)$ und mit Pythagoras folgt $|wz|^2 = |az|^2 + |bz|^2 = |w|^2|z|^2$. Somit gilt folgende Aussage.



Satz 8.9 Bei der Multiplikation von komplexen Zahlen werden **die Beträge multipliziert** und **die Argumente addiert**.
Insbesondere gilt **de Moivres Formel**: $(\cos(\varphi)+i\sin(\varphi))^n = \cos(n\varphi)+i\sin(n\varphi)$.

Hierbei wird die Summe der Argumente natürlich modulo 2π gerechnet.
Diese Tatsache kann man auch mit der **Polardarstellung** komplexer Zahlen verstehen. Ist $\varphi = \mathrm{Arg}(z)$, so gilt die Formel



$$z = |z| \cdot (\cos(\varphi) + i \cdot \sin(\varphi)).$$

Ist nun $w = |w| \cdot (\cos(\psi) + i \cdot \sin(\psi))$, so rechnet man mithilfe der Additionstheoreme **??** nach, dass

$$z \cdot w = |z| \cdot |w| \cdot (\cos(\varphi + \psi) + i \cdot \sin(\varphi + \psi)).$$

Natürlich gibt es auch für Punkte $(x, y) \in \mathbb{R}^2$ mit $(x, y) \neq (0, 0)$ eine Polardarstellung $(x, y) = r(\cos(\varphi, \sin(\varphi))$. Man spricht dann von den **Polarkoordinaten** des Punktes $(x, y) \in \mathbb{R}^2$.

Aufgaben

Aufgabe 8.44 In den nachfolgenden Aufgaben zeichnen Sie jeweils z und w in der komplexen Ebene. Konstruieren Sie jeweils mithilfe eines Geodreiecks geometrisch $z + w$ und $z \cdot w$. Rechnen Sie danach $z + w$ und $z \cdot w$ und kontrollieren Sie Ihr Ergebnis.

1. $z = i\,, \quad w = -1$
2. $z = 1 + i\,, \quad w = i$
3. $z = 1 - i\,, \quad w = 1 + i$
4. $z = 2 + i\,, \quad w = 3 - i$
5. $z = 3 + 4i\,, \quad w = 1 + 2i$
6. $z = -1 + 3i\,, \quad z = w$

Aufgabe 8.45 Schreiben Sie die nachfolgenden komplexen Zahlen in Polardarstellung.

1. -2
2. i
3. $-4i$
4. $-1 + i$
5. $\frac{1}{2} + \frac{1}{2}\sqrt{3}i$
6. $-\frac{1}{2} + \frac{1}{2}\sqrt{3}i$
7. $\sqrt{3} + i$
8. $2 - 2i$

Aufgabe 8.46 Beschreiben Sie für eine komplexe Zahl z mit $|z| = 1$ den Kehrwert z^{-1} geometrisch.

Aufgabe 8.47 Berechnen Sie:

1. $(1 + i)^4$
2. $(\sqrt{3} + i)^6$
3. $(1 - i)^{10}$
4. $(1 + i)^{102}$

Aufgabe 8.48

1. Berechnen Sie mithilfe der Formel von de Moivre:

$$\sin(3t) = 3\sin(t) - 4\sin^3(t) \text{ und } \cos(3t) = 4\cos^3(t) - 3\cos(t).$$

2. Sei x, y mit $x^2 + y^2 = 1$. Berechnen Sie, dass $(x + iy)^n$ für n ungerade von der Form $p(x) + iq(y)$, mit p, q Polynome, ist. Was kann man hieraus für $\cos(nx)$ und $\sin(nx)$ schließen?

8.10 Polynomiale Gleichungen

Natürlich hat die Gleichung $z^n = 0$ auch in $\mathbb{C}$ nur $z = 0$ als Lösung.

Satz 8.10 Sei a eine feste komplexe Zahl mit $a \neq 0$. Die Gleichung $z^n = a$ hat n Lösungen in $\mathbb{C}$.

Beweis. Wir setzen dazu $\lambda = \sqrt[n]{|a|}$, welche eine gewöhnliche reelle Zahl ist. Sei $\varphi = \mathrm{Arg}(a)$. Sei $\alpha_1 := \varphi/n$ und $\alpha_k = \alpha_1 + k \cdot \frac{2\pi}{n}$ für $k = 1, \ldots, n-1$. Dann gilt für

$$z_k = \lambda \cdot (\cos(\alpha_k) + \sin(\alpha_k)) \cdot i$$

die Gleichung $z_k^n = \alpha$. Tatsächlich ist nach der geometrischen Interpretation $|z_k|^n = \lambda^n = |a|$ und $\mathrm{Arg}(z_k^n) = n\mathrm{Arg}(z_k) \bmod 2\pi = \varphi = \mathrm{Arg}(a)$, also sind Betrag und Argument gleich, deshalb $z_k^n = a$. ∎

Aus der Schule kennen wir die pq-Formel für quadratische Gleichungen $x^2+px+q = 0$, nämlich

$$x_{1,2} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}.$$

Hierbei sollte das Symbol $\pm\sqrt{p^2 - 4q}$ stehen für eine Lösung der Gleichung $z^2 = p^2 - 4q$, die zwei Lösungen hat, wenn die *Diskriminante* positiv ist. Ist die Diskriminante negativ, so hat die quadratische Gleichung keine reellen Lösungen. Jedoch hat sie Lösungen, wenn man komplexe Zahlen zulässt. Ist $D < 0$, so ist $z = \sqrt{-D} \cdot i$ eine Zahl mit $z^2 = (-D) \cdot i^2 = D$. Wie wir oben gesehen haben, gilt sogar, dass für jede *komplexe Zahl* D ein z existiert mit $z^2 = D$. Folgender Satz folgt.

Satz 8.11 Jede Gleichung $x^2 + px + q = 0$, mit p, q komplexe Zahlen, hat mindestens eine Lösung.

Diese zwei Sätze, welche relativ elementar bewiesen werden können, haben eine wichtige Verallgemeinerung: Jede polynomiale Gleichung in z

$$z^n + a_1 z^{n-1} + \cdots + a_n = 0$$

hat eine Lösung in $\mathbb{C}$. Diese Aussage ist der berühmte **Hauptsatz der Algebra**.

Einen Beweis finden Sie im Buch “Lineare Algebra”, Seite 177.

Aufgaben

Aufgabe 8.49 Zeichnen Sie die komplexen Zahlen z, welche eine der nachfolgenden Gleichungen erfüllen.

1. $z^2 = i$
2. $(z+1)^2 = i$
3. $(z+2-i)^2 = i$
4. $z^2 = -2\sqrt{3} + 2i$
5. $z^3 = 1$
6. $z^4 = 1$
7. $z^6 - 2z^3 + 1 = 0$
8. $(z-i)^4 = 1$
9. $z^6 = 1$

Aufgabe 8.50 Lösen Sie die nachfolgenden Gleichungen.

1. $z^2 - 2z + 2 = 0$
2. $z^2 + 4z + 6 = 0$
3. $z^2 + 4z - 8 = 0$
4. $z^4 + 8 - 8\sqrt{3}i = 0$
5. $z^2 + iz + 2 = 0$
6. $z^2 + (2-2i)z - 2 - 2(1+\sqrt{3})i = 0$

Aufgabe 8.51 Bestimmen Sie die komplexen Zahlen a, sodass die Gleichung

$$iz^2 + (a - 3 + i)z - 12 + 5i = 0$$

genau eine Lösung hat.

Aufgabe 8.52 Bestimmen Sie die reelle Zahl a, sodass die Gleichung

$$(3+4i)z^2 - (a+5)z + (2-4i) = 0$$

eine reelle Lösung hat, und lösen Sie dann diese Gleichung.

Aufgabe 8.53 (Cardanische Formel) Betrachte die Gleichung $x^3 = px + q$ in x mit p, q in $\mathbb{C}$ und $p \neq 0$. Seien z, u komplexe Zahlen mit

$$z^2 = \left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^2 \text{ und } u^3 = \frac{q}{2} + z\,.$$

Zeigen Sie, dass $x = u + p/(3u)$ eine Lösung der Gleichung $x^3 = px + q$ ist.
Tipp: Berechnen Sie $x^3 - px$ und zeigen Sie, dass $u^6 - qu^3 + p^3/27 = 0$.

Aufgabe 8.54 Finden Sie mithilfe der cardanischen Formel eine Lösung für:

1. $x^3 = 9x + 28$
2. $x^3 = -3x + 4$

Was fällt bei der zweiten Gleichung auf?

Aufgabe 8.55 Es sei p ein Polynom mit reellen Koeffizienten und $a \in \mathbb{C}$ eine Nullstelle von p. Zeigen Sie, dass $\overline{a}$ ebenfalls eine Nullstelle von p ist.

Kapitel 9

Graphentheorie

Motivation
Graph: Graphen sind eine der häufigsten diskreten Strukturen und daher wichtig. Ein Graph wird beschrieben mit Hilfe von zwei verschiedenen Mengen:

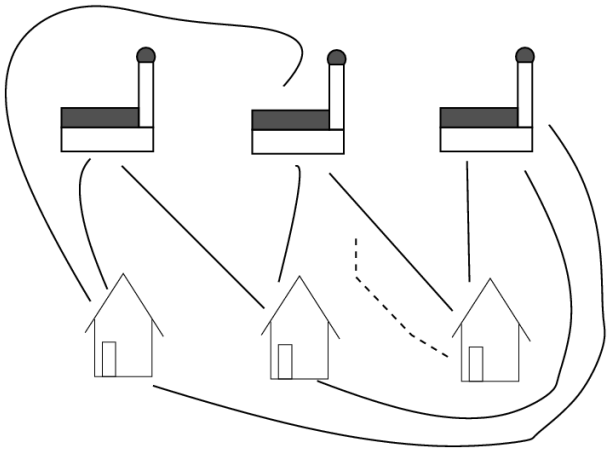
V : Menge der Ecken / Knoten (V für englisch vertices)
E : Menge der Kanten (E für englisch edges).

Kanten können gerichtet oder ungerichtet sein. Dies führt zu den Begriffen gerichteter bzw. ungerichtetet Graph.
Einige Beispiele:

Ecken	Länder	Städte	Mensch	Files	Homepages
Kanten	Grenzen	Autobahnen	Eltern → Kind	enthalten	Links

Einige berühmte Probleme

1. Ist es möglich 3 Häuser mit jeweils drei Leitungen (Wasser/Strom/Elektrizität) an die drei Versorger anzuschließen, ohne, dass sich Leitungen kreuzen?



Wir werden später sehen, dass dies *unmöglich* ist.

2. *Vier-Farben-Satz:* Mit vier Farben ist es möglich eine beliebige Landkarte so zu färben, dass zwei aneinander grenzende Länder unterschiedliche Farben bekommen. Dies ist sehr schwierig zu beweisen; wir werden zeigen, dass fünf Farben ausreichen.

3. Travelling Salesman Problem: Kanten mit Gewichten.

9.1 Definition

1. Ein einfacher gerichteter Graph ist ein Paar (V, E) von Mengen mit $E \subset V \times V \setminus \{(v, v) \colon v \in V\}$. Ist $e = (i, j) \in E$, so sagen wir: e verbindet i und j oder i, j benachbart oder i, j inzident mit e. Ein einfacher Graph hat also keine Schleifen.

2. Ein einfacher ungerichteter Graph ist ein Paar (V, E) von Mengen mit $E \subset \binom{V}{2}$.

3. Ein gerichteter Graph ist ein Tripel (V, E, μ), dabei sind V, E Mengen und $\mu \colon E \to V \times V$ eine Abbildung. Wir können schreiben:

   $$\mu(e) = (\alpha(e), \omega(e)),\ \alpha \colon E \to V,\ \omega \colon E \to V.$$

   Damit meinen wir, dass es in dem Graphen eine Kante e von dem Knoten $\alpha(e)$ zu dem Knoten $\omega(e)$ gibt.

   Ein einfacher gerichteter Graph ist der Spezialfall, indem μ injektiv ist und jedes (v, v) nicht im Bild der Abbildung μ ist.

4. Ein ungerichteter Graph ist ein Tripel (V, E, μ), dabei sind V, E Mengen und $\mu \colon E \to \binom{V}{2}$ eine Abbildung.
   Ein einfacher ungerichteter Graph ist der Spezialfall, indem die Abbildung μ injektiv ist.

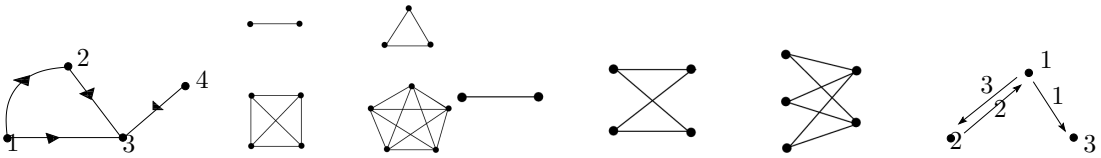
5. Ein gerichteter gewichteter Graph ist ein Paar (V, φ), wobei V eine Menge ist und $\varphi \colon V \times V \to \mathbb{R}$ oder $\mathbb{N}_0$. Für $(i, j) \in V \times V$ nennen wir $\varphi((i, j))$ das Gewicht von (i, j). Es gibt eine Kante zwischen von i nach j genau dann, wenn $\varphi((i, j)) \neq 0$.

6. Ein ungerichteter gewichteter Graph ist ein Paar (V, φ), wobei V eine Menge ist und $\varphi \colon \binom{V}{2} \to \mathbb{R}$ oder $\mathbb{N}_0$. (Alternativ $\varphi \colon V \times V \to \mathbb{R}$.) Für $\{i, j\} \in \binom{V}{2}$ nennen wir $\varphi(\{i, j\})$ das Gewicht von $\{i, j\}$. Es gibt eine Kante zwischen i und j genau dann, wenn $\varphi(\{i, j\}) \neq 0$.

Beispiele.

1. $V = \{1, 2, 3, 4\}$,
   $E = \{(1, 2), (1, 3), (2, 3), (4, 3)\}$
2. $V = \{1, 2, 3, 4\}$, $E = \{\{1, 2\}, \{1, 3\}, \{1, 4\}\}$.

3. $V = \{1, \ldots, n\}$, $E = \binom{V}{2}$. Man nennt diesen Graphen den vollständigen Graphen mit n Knoten und bezeichnet ihn mit K_n.
4. $K_{n,m}$ bipartiter Graph.
5. Beispiel eines gerichteten gewichteten Graphens.



Wir können aus jedem Graphen (gerichtet oder ungerichtet) einen gewichteten Graphen machen, indem wir φ definieren durch

$$\varphi((i,j)) := \#\mu^{-1}(\{(i,j)\}) \text{ bzw. } \varphi(\{i,j\}) := \#\mu^{-1}(\{\{i,j\}\}).$$

Wenn $E \subset V \times V \setminus \{(v,v) \colon v \in V\}$ die Eigenschaft hat, dass

$$(i,j) \in E \;\Rightarrow\; (j,i) \in E,$$

so können wir den einfachen gerichteten Graphen (V,E) als einfachen ungerichteten Graphen auffassen, indem wir die beiden gerichteten Kanten (i,j) und (j,i) als eine ungerichteten Kante $\{i,j\}$ auffassen. Umgekehrt kann man jeden einfachen ungerichteten Graphen als einfachen gerichteten Graphen mit obiger Eigenschaft auffassen.
Auf diese Weise können wir ungerichtete Graphen als spezielle gerichtete Graphen auffassen.
In obiger Definition haben ungerichtete Graphen keine Schleifen, da

$$\mu \colon E \to \binom{V}{2}$$

hat jede Kante nach Definition zwei verschiedene Endpunkte.
Wir können ungerichtete Graphen mit Schleifen ad hoc einführen mit Hilfe einer Abbildung

$$\mu \colon E \to \{A \subset X \mid 1 \leq \#A \leq 2\},$$

oder als Spezialfall von ungerichteten Graphen mit $(i,j) \in E \iff (j,i) \in E$.

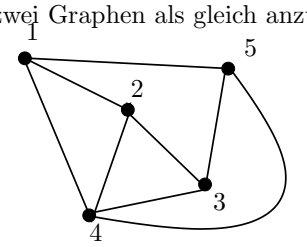
Aufgaben

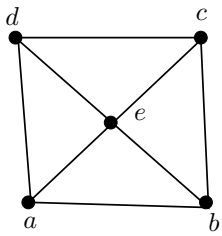
Aufgabe 9.1 Es sei $V = \{7, 19, 10, 43, 26, 82, 27, 94, 6\}$ die Menge der Knoten eines einfachen ungerichteten Graphens $G = (V,E)$. Zwischen i und j in V gibt es eine Kante genau dann, wenn $i = j \bmod 4$. Zeichnen Sie G.

Aufgabe 9.2
1. Es sei $n, k \in \mathbb{N}_+$. Bestimmen Sie die Anzahl der einfachen ungerichteten Graphen mit genau n Knoten und k Kanten.
2. Skizzieren Sie alle einfachen ungerichteten Graphen mit genau 4 Knoten und 3 Kanten.

9.2 Isomorphie von Graphen

Wann sind zwei Graphen als gleich anzusehen?





$f\colon \{1,2,3,4,5\} \to \{a,b,c,d,e\}$, $1 \mapsto a$, $2 \mapsto b$, $3 \mapsto c$, $4 \mapsto e$, $5 \mapsto d$. Dann gilt:

$$\{i,j\} \in E_1 \iff \{f(i),f(j)\} \in E_2.$$

Definition:

1. Für zwei einfache Graphen $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$ ist ein Homomorphismus von G_1 nach G_2 eine Abbildung $f\colon V_1 \to V_2$ mit der Eigenschaft:
   gerichteter Fall: $(i,j) \in E_1 \Rightarrow (f(i),f(j)) \in E_2$.
   ungerichteter Fall: $\{i,j\} \in E_1 \Rightarrow \{f(i),f(j)\} \in E_2$.
   Man schreibt auch $f\colon G_1 \to G_2$ statt $f\colon V_1 \to V_2$, falls die Abbildung f einen Homomorphismus von G_1 nach G_2 liefert.

2. Ein Homomorphismus $f\colon V_1 \to V_2$ von G_1 nach G_2 heißt Isomorphismus, falls es einen Homomorphismus $g\colon V_2 \to V_1$ von G_2 nach G_1 gibt mit

   $$f \circ g = id_{V_2} \text{ und } g \circ f = id_{V_1}.$$

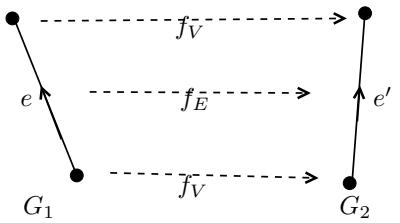
   Dies ist genau dann der Fall, wenn f bijektiv ist und es gilt

   $$\begin{aligned} \text{gerichteter Fall: } (i,j) \in E_1 &\iff (f(i),f(j)) \in E_2, \\ \text{ungerichteter Fall: } \{i,j\} \in E_1 &\iff \{f(i),f(j)\} \in E_2. \end{aligned}$$

3. Für zwei (nicht einfache) Graphen $G_1 = (V_1, E_1, \mu_1), G_2 = (V_2, E_2, \mu_2)$ ist ein Homomorphismus $f\colon G_1 \to G_2$ ein Paar von Abbildungen $f_V\colon V_1 \to V_2$ und $f_E\colon E_1 \to E_2$ so, dass gilt

   $$f_V(\alpha_1(e)) = \alpha_2(f_E(e)) \text{ und } f_V(\omega_1(e)) = \omega_2(f_E(e)) \text{ für alle } e \in E_1.$$

   Im Diagramm:



$$\begin{array}{ccc} E_1 & \stackrel{\mu_1}{\to} & V_1 \times V_1 \\ f_E \downarrow & & \downarrow f_V \times f_V \\ E_2 & \stackrel{\mu_2}{\to} & V_1 \times V_1 \end{array}$$

Aufgaben

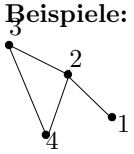
Aufgabe 9.3 Zeichnen Sie 5 einfache Graphen mit jeweils 5 Knoten, die nicht zueinander isomorph.

9.3 Matrizen und Graphen

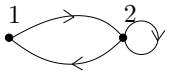
Sei X eine Menge, I und J endliche Indexmengen. Eine Matrix mit Einträgen in X ist eine Abbildung $m\colon I \times J \longrightarrow X, \quad (i,j) \mapsto m_{i,j}$, wobei I und J endliche Indexmengen für die Zeilen bzw. Spalten sind.

Man schreibt auch $M = (m_{i,j})_{i\in I, j\in J}$ oder kurz $M = (m_{i,j})$. Um die Matrix in Rechtecksform aufzuschreiben, muss man zusätzlich noch eine Reihenfolge der Elemente von I und J festlegen. O.E. ist $I = \{1, ..., n\}$ und $J = \{1, ..., m\}$
Ist (V, φ) ein gerichteter gewichteter Graph, so „ist“ $\varphi\colon V \times V \longrightarrow \mathbb{N}_0$ eine Matrix, wenn man $V = \{1, .., n\}$ eine Nummerierung der Knoten wählt. Ist (V, E) ein einfacher ungerichteter graph, so ist $m_{i,j} = 1$ genau dann, wenn $\{i, j\} \in E$ und $m_{i,j} = 0$ sonst. Etcetera.

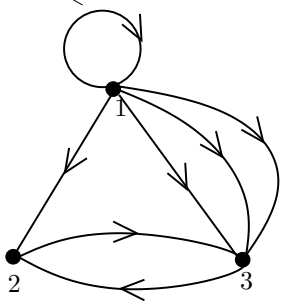
Beispiele:



$$\Phi = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$



$$\Phi = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$



$$\Phi = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Diagonalelemente der Matrix $\Phi_{i,i}$ stehen für Schleifen des Graphen.
Ein Graph ist einfach genau dann, wenn alle Einträge 0 oder 1 sind und alle Diagonalelemente gleich 0.

Ein Graph ist ungerichtet genau dann, wenn Φ symmetrisch ist, d.h. $\Phi^\top = \Phi$, wobei $(\Phi^\top)_{i,j} := \Phi_{j,i}$ und alle Diagonalelemente gleich 0 sind.

Sei $G = (V, E, \mu)$ ein ungerichteter Graph, $v \in V$ ein Knoten. Dann bezeichnet

$$\deg(v) := \#\{e \in E \mid v \in \mu(e)\}$$

die Anzahl der Kanten, die an v grenzen und heißt der Grad von v.

Aufgaben

Aufgabe 9.4 Sei $G = (V, E, \mu)$ ein GRaph. Dann gilt $\sum_{v \in V} \deg(v) = 2 \cdot |E|$. Beweisen Sie diese Aussage.

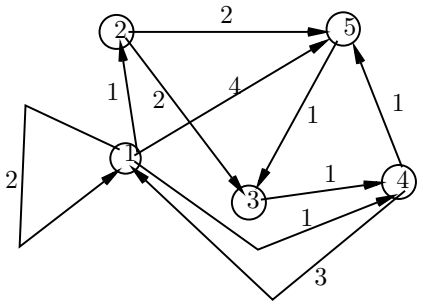
Aufgabe 9.5 Skizzieren Sie die zu den nachfolgend Adjazenzmatrizen gehörigen gewichteten gerichtenten Graphen.

1. $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 0 & 2 & 0 & 1 \\ 4 & 0 & 1 & 0 \end{pmatrix}$

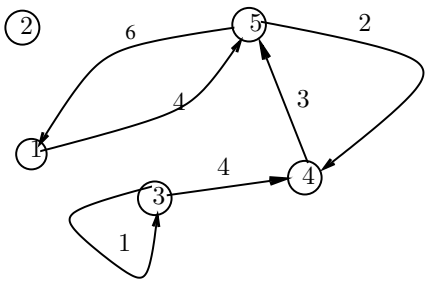
2. $\begin{pmatrix} 0 & 1 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 3 & 9 & 1 & 1 \end{pmatrix}$

Aufgabe 9.6 Bestimmen Sie die zu den nachfolgenden gewichteten gerichtete Graphen gehörigen Adjazenzmatrizen.

1.



2.



9.4 Kantenzüge und Zusammenhang

Sei $G = (V, E, \mu)$ ein gerichteter Graph.

- Ein Kantenzug ist eine Folge von Kanten $(e_1, ..., e_r)$ mit $\alpha(e_{i+1}) = \omega(e_i)$.

$$v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} v_2 \xrightarrow{e_3} \cdots \xrightarrow{e_r} v_r$$

- $v_0 := \alpha(e_1)$ heißt Anfangsknoten , $v_r := \omega(e_r)$ Endknoten. Ein Kantenzug heißt geschlossen, wenn $v_0 = v_r$. Es kann passieren, dass Kanten oder Knoten mehrfach vorkommen.
- Ein Weg ist ein Kantenzug, bei dem die Kanten $e_1, ..., e_r$ paarweise verschieden sind.
- Ein Pfad ist ein Kantenzug, bei dem die Knoten $\alpha(e_1), \omega(e_1) = \alpha(e_2), ..., \omega(e_r)$ paarweise verschieden sind.
- Geschlossenheit ist wie für Kantenzüge definiert. Ein geschlossener Weg heißt Kreis. Eine geschlossener Kantenzug mit $v_0, \ldots, v_{r-1}$ paarweise verschieden heißt Zyklus oder geschlossener Pfad.

Für ungerichtete Graphen definieren wir Kantenzüg, Wege und Kreise auf änliche Weise.

Sei G ein Graph. Ein Knoten v heißt verbindbar mit einem Knoten w, schreibe $v \sim w$, wenn $v = w$ ist oder es einen Kantenzug von v nach w gibt. Es gibt dann automatisch auch einen Pfad von v nach w. G heißt zusammenhängend, wenn je zwei Knoten von G verbindbar sind.

Satz 9.1 Sei G ein einfacher zusammenhängender Graph mit n Knoten und k Kanten. Dann gilt

$$n - 1 \leq k \leq \tfrac{1}{2} n(n-1)\,.$$

Beweis. Die maximale Anzahl der Kanten hat ein vollständiger Graph mit $\frac{1}{2}n(n-1)$ Kanten. Wir brauchen deshalb nur $k \geq n-1$ zu zeigen. Ist $k = 0$, so ist die Anzahl der Knoten höchstens 1. In diesem Fall gilt die Aussage. Sonst is $k \geq 1$ und sei e eine beliebige Kante von G. Nach Streichen der Kante e aus den Graphen G entsteht ein Graphen G'. Ist z ein Knoten in G, dann ist z in G' entweder mit v oder mit w verbunden. Ist nämlich z in G' nicht mit w verbunden, so enthält einen Kantenzug von z nach w in G die Kante $e = \{v, w\}$, welche o.B.d.A. höchstens einmal in diesem Kantenzug vorkommt. Somit ist in G' der Knoten z mit v verbindbar. Es folgt, dass entweder G' zusammenhängend ist $k-1$ Kanten, welche Induktionsgemäß größer oder $n-1$ ist, oder $G' = G_1 \sqcup G_2$ mit G_1 und G_2 zusammenhängend. Hat G_i, für $i = 1, 2$,

n_i Knoten und k_i Kanten, so ist $k = k_1 + k_2 + 1$, $n = n_1 + n_2$ und mit Induktion $k_1 \geq n_1 - 1$, $k_2 \geq n_2 - 1$. ∎

Aufgaben

Aufgabe 9.7 Es sei G ein Graph.

9.5 Zusammenhangskomponenten

- $v \sim v$
- $v \sim w \Rightarrow w \sim v$
- $v \sim w$ und $w \sim u \Rightarrow v \sim u$

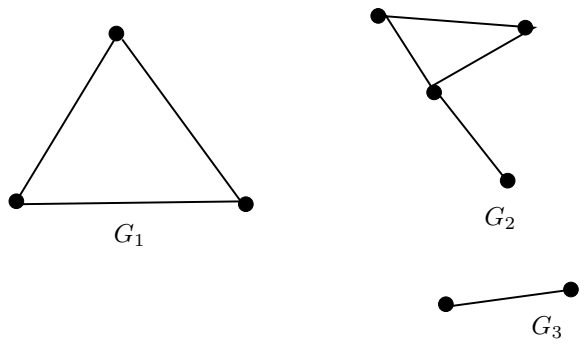
d.h. $\sim$ ist eine sogenannte Äquivalenzrelation. Ist

$$V_v := \{w \colon v \sim w\}$$

so gilt $V_v = V_w$ oder $V_w \cap V_w = \emptyset$. V ist dann die disjunkte Vereinigung von Mengen $V_1, ..., V_s$, $V = V_1 \sqcup V_2 \sqcup ... \sqcup V_s$, so dass $u, v \in V_i \Leftrightarrow u \sim v$.
Die Kanten E zerfallen gleichermaßen in Teilmengen $E_i \subset \binom{V_i}{2}$, und G in Teilgraphen $G_i = (V_i, E_i)$. Schreibe:

$$G = G_1 \sqcup G_2 \sqcup ... \sqcup G_s$$

Die G_i heißen Zusammenhangskomponenten von G und ein Graph heißt *zusammenhängend*, wenn er nur einen Zusammenhangskomponent hat.



Satz 9.2 Sei G ein einfacher Graph mit n Knoten, s Komponenten und k Kanten. Dann gilt

$$n - s \leq k \leq \frac{1}{2}(n-s)(n-s+1)\,.$$

Beweis. Wir zeigen zuerst $k \geq n - s$ mit Induktion nach k. Falls $k = 0$ ist, so hat k keine Kanten. Jeder Knoten ist isoliert, also haben wir genauso viele Komponenten wie Knoten. Also ist $n = s$.
Hat jetzt G $k+1$ Kanten, dann können wir in G einen Kanten entfernen. Wir erhalten einen Graphen G' H mit $k-1$ Kanten, n Knoten und $s' \leq s+1$ Komponenten. Nach Induktion gilt $k - 1 \geq n - s' \geq n - s - 1$, also $k \geq n - s$.

$$\boxed{k \leq \tfrac{1}{2}(n-s)(n-s+1)}$$

Gegeben n und s. Versuchen wir, einen Graphen mit der maximalen Anzahl von Kanten zu konstruieren. Es ist klar, dass dieser Graph Zusammenhangskomponenten $G_1, \ldots, G_s$ hat, wobei die G_i vollständige Graphen sind. Seien n_i die Anzahl der Kanten von G_i, $n_1 + \ldots + n_s = n$. Ohne Einschränkung haben wir $n_1 \geq n_2 \geq \ldots \geq n_s$. Wir behaupten, dass die maximale Anzahl von Kanten auftritt für $n_1 = n - s + 1$, $n_2 = n_3 = \ldots = n_s = 1$.

Sei nämlich G_i und G_j zwei Komponenten mit n_i und n_j Knoten und $n_i \geq n_j > 1$. Betrachten wir jetzt die vollständigen Graphen mit $n_j + 1$ und $n_j - 1$ Knoten, dann bleibt die Gesamtanzahl von Knoten und Zusammenhangskomponenten gleich. Aber die Anzahl von Kanten wird größer:

$$\binom{n_i+1}{2} + \binom{n_i-1}{2} - \left(\binom{n_i}{2} + \binom{n_j}{2}\right) = n_i - n_j + 1$$

(Rechnen Sie dies nach!), was positiv ist.

Die maximale Anzahl von Kanten bei s Komponenten kriegen wir also bei einem vollständigen Graph mit $n_1 = n - s + 1$ Knoten und $s - 1$ isolierten Knoten. Dieser Graph hat $\binom{n-s+1}{2}$ Kanten. Also ist $k \leq \binom{n-s+1}{2}$, was zu zeigen war.

Für $s = 1$ ergibt sich $n-1 \leq k \leq \frac{1}{2}(n-s)(n-s+1)$. Ein zusammenhängender Graph hat also mindestens $n - 1$ Kanten.
Ein Graph mit $s = 2$ Zusammenhangskomponenten hat maximal $k \leq \frac{1}{2}(n-1)(n-2)$ Kanten.

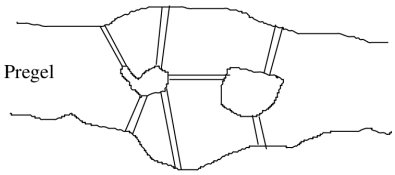
Aufgaben

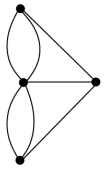
Aufgabe 9.8 Sei $G = (V, E)$ ein einfacher ungerichteter Graph. Den zu G komplementäre Graph $\overline{G}$ ist definier durch

$$\overline{G} = \left(V, \binom{V}{2} \setminus E\right).$$

1. Zeigen Sie: Ist G nicht zusammenhängend, so ist $\overline{G}$ zusammenhängend.
2. Zeigen oder widerlegen Sie: Ist G zusammenhängend, so ist $\overline{G}$ nicht zusammenhängend.

9.6 Eulersche Graphen





Königsberger Brückenproblem(1736)
Gibt es einen Weg, der jede Brücke genau einmal überquert und zum Anfang zurückkehrt? Oder anders gesagt, ist folgender Graph eulersch?

Sei G ein ungerichteter Graph.

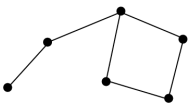
1. Ein Eulerkreis ist ein Kreis, welcher alle Kanten von G genau einmal durchläuft.
2. G heißt eulersch, wenn ein Eulerkreis in G existiert.

Satz 9.3 Ein zusammenhängender Graph G ist eulersch genau dann, wenn der Grad jedes Knotens von G gerade ist.

Beweis. Sei C ein Eulerkreis. Jedes Mal, wenn wir entlang C einen Knoten v passieren, gibt dies eine Beitrag 2 für den Grad des Knotens. Die erste Kante gibt ein Beitrag eins für den ersten Knoten, die letzte Kante auch. Nach Definition ist $\deg(v)$ die Anzahl von Kanten die mit v inzident sind. Da jede Kante von G in C vorkommt, ist der Grad jedes Knotens also gerade.
Für die Umkehrung zeigen wir zunächst, dass ein Kreis existierten, wenn $\text{Grad}(v) \geq 2$ für alle $v \in V$. Sei v_0 ein beliebiger Knoten. Wir können jetzt einen Weg

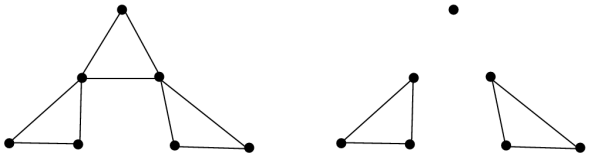
$$v_0, v_1, v_2, \ldots$$

wählen mit $v_{i+1} \neq v_i$. Hier benutzen wir, dass der Grad jedes Knotens mindestens 2 ist. Da G nur endlich viele Knoten hat, müssen wir nach endlich vielen Schritten einen Knoten v_i wählen, der schon vorgekommen ist. Der Weg von v_i nach v_i ist ein Kreis.

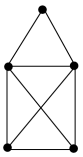


Den Beweis, dass G einen Eulerkreis besitzt, erhalten wir durch Induktion nach der Anzahl der Kanten von G. Da G zusammenhängend ist, hat jeder Knoten mindestens Grad 2. Nach dem Lemma besitzt G einen Kreis C. Falls C schon alle Kanten von C enthält, so sind wir fertig. Falls C nicht alle Kanten enthält, so lassen wir alle Kanten von C weg. Der Graph H, der übrig bleibt, hat weniger Kanten als G. Der Grad jedes Knotens von H ist wieder gerade. H braucht nicht mehr zusammenhängend zu sein, aber die Komponenten von H sind es selbstverständlich. Nach Induktion besitzt jede Komponente von H einen Eulerkreis. Da G zusammenhängend ist, hat jede Komponente von H mindestens einen Knoten mit C gemeinsam. (Warum?) Wir erhalten

jetzt einen Eulerkreis in G, indem wir an den Kanten von C entlang laufen bis ein Knoten von H erreicht wird. Wir durchlaufen jetzt den Eulerkreis in der Komponente von H, wozu dieser Knoten gehört. Danach setzen wir unseren Weg auf C fort, bis wieder ein Knoten von H erreicht wird und so weiter. ∎

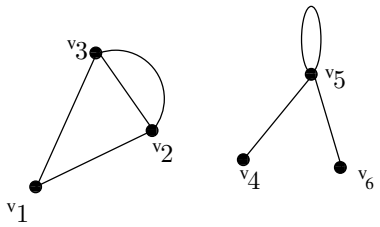


Aufgabe 9.9
G heißt semieulersch, wenn ein weg in G existiert, der alle Kanten einmal durchläuft. Zeigen Sie, dass das Haus von Nikolaus ein semi-Eulerscher, nicht Eulerscher Graph ist das Haus von Nikolaus.



Zeigen Sie, dass ein Graph G genau dann semieulersch ist, wenn er höchstens zwei Knoten mit ungeradem Grad enthält.

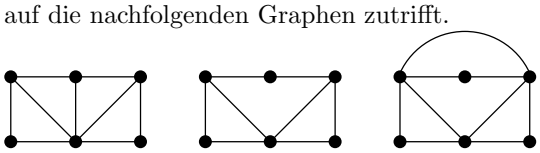
Aufgabe 9.10 Prüfen Sie, ob der nachfolgende Graph eulersch ist.



Aufgabe 9.11 Zeichnen Sie 2 eulerschen Graphen mit 5 Knoten, die nicht zueinander isomorph sind

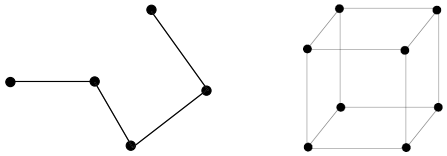
Aufgabe 9.12 Zeichne den Graph (V, E) mit $V = \{1, 2, 4, 7, 8, 14, 15\}$. Zwischen zwei verschiedene Zahlen n und m verlaufe eine Kante wenn $\text{ggT}(n, m) = 1$ oder $n = 2m$. Ist der Graph eulersch?

Aufgabe 9.13 Entscheiden Sie, welche der Eigenschaften eulers und semieulersch auf die nachfolgenden Graphen zutrifft.



9.7 Hamiltonkreise und Hamiltonsche Graphen

Sei G ein einfacher ungerichteter Graph. Ein Hamiltonkreis ist ein Kreis welcher alle Knoten von G genau einmal durchläuft. Enthält G einen Hamiltonkreis, so heißt G Hamiltonsch.



Satz 9.4 Sei $G = (V, E)$ ein einfacher ungerichteter Graph. Gilt für je zwei nicht benachbarte Knoten v und w

$$\deg(v) + \deg(w) \geq n := \#V, \qquad (*)$$

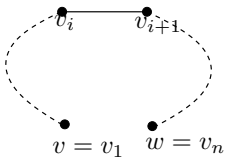
so ist G Hamiltonsch. Gilt insbesondere, dass $\deg(v) \geq n/2$ for alle Knoten v, so ist G Hamiltonsch.

Beweis. Der vollständige Graph K_n ist offensichtlich Hamiltonsch. Wir nehmen nach und nach Kanten weg und zeigen, dass wir immer einen Hamiltonkreis finden können, solange noch $(*)$ gilt.
Sei dazu C ein Hamiltonkreis in G, und G' der Graph der aus G durch wegnehmen der Kante $e = \{v, w\}$ entsteht.

1. Enthält C die Kante e nicht, so ist C auch ein Hamiltonkreis in G'.
2. Falls aber e zu dem Hamiltonschen Kreis C gehört, so müssen wir C abändern. Wir nummerieren die Knoten in C, so dass C gleich

   $$v = v_1 \longrightarrow v_2 \longrightarrow \cdots \longrightarrow v_n = w \longrightarrow v$$

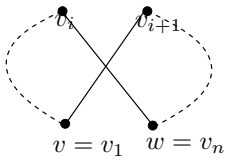
   ist.



Wir suchen nun ein i, $1 \leq i \leq n-1$, sodass $\{v, v_{i+1}\}$ und $\{v_i, w\}$ Kanten in G' sind. Haben wir so ein i, dann ist

$$v = v_1 \to v_2 \to \cdots \; v_i \to v_n = w \to v_{n-1} \to \cdots \to v_{i+1} \to v$$

ein Hamiltonscher Kreis in G'.



Um die Existenz dieses i zu zeigen, betrachten wir die Mengen

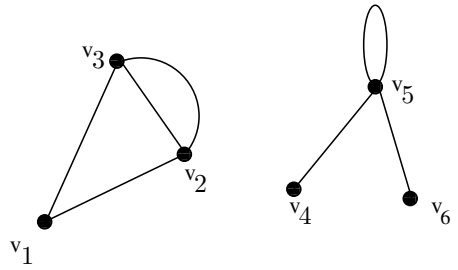
$$A := \{i \mid 1 \leq i \leq n-1,\ \{v_1, v_{i+1}\} \in E\}$$
$$B := \{i \mid 1 \leq i \leq n-1,\ \{v_i, w\} \in E\}.$$

Offensichtlich ist $\#(A \cup B) \leq n-1$. Klar ist auch, dass $\#A = \deg(v)$, $\#B = \deg(w)$. Nach der Voraussetzung dieses Satzes gilt:

$$\#(A \cap B) = \#A + \#B - \#(A \cup B) \geq \deg(v) + \deg(w) - (n-1) \geq 1,$$

Also existiert das gesuchte i. ∎

Aufgabe 9.14 Prüfen Sie, ob der nachfolgende Graph hamiltonsch ist.



Aufgabe 9.15 Zeichnen Sie 2 hamiltonschen Graphen mit 5 Knoten, die nicht zueinander isomorph sind.

Aufgabe 9.16 Zeichne den Graph (V, E) mit $V = \{1, 2, 4, 7, 8, 14, 15\}$. Zwischen zwei verschiedene Zahlen n und m verlaufe eine Kante wenn $\mathrm{ggT}(n, m) = 1$ oder $n = 2m$. Ist der Graph Hamiltonsch.

9.8 Bäume

- Ein Baum ist ein zusammenhängender ungerichteter Graph ohne Kreise.
- Ist $G = (V, E)$ und $v \in V$ ein Knoten mit $\deg(v) = 1$, so nennen wir v ein Blatt.
- Ein Wurzelbaum ist ein Baum mit einem ausgezeichnetem Blatt.
- Ein Wald ist ein Graph, dessen Zusammenhangskomponenten Bäume sind.

Satz 9.5 (Charakterisierung von Bäumen) Sei G ein einfacher ungerichteter Graph mit n Knoten. Dann sind äquivalent:

1. G ist ein Baum.
2. G enthält keinen Zyklus und hat $n - 1$ Kanten.
3. G ist zusammenhängend und hat $n - 1$ Kanten.
4. G ist zusammenhängend und wird durch weglassen einer beliebigen Kante unzusammenhängend.
5. Je zwei Knoten von G werden durch genau einen Pfad verbunden.
6. G enthält keinen Zyklus und durch hinzufügen einer beliebigen Kante entsteht genau ein Zyklus.

Beweis. 1. $\Rightarrow$ 2.: G besitzt keine Zyklen. Durch Weglassen einer Kante $\{v, w\}$ von G entsteht ein Graph H mit 2 Komponenten. Denn sonst wäre G zusammenhängend, und ein Pfad von v nach w zusammen mit $\{v, w\}$ würde ein Zyklus in G liefern.) Die Komponenten seien H_1 und H_2 mit n_1 bzw. n_2 Knoten. Dann gilt $n_1 + n_2 = n$, H_1 und H_2 sind dann auch Bäume, also hat H nach Induktionsannahme

$$n_1 - 1 + n_2 - 1 = n - 2$$

Kanten. Zusammen mit $\{v, w\}$ hat G also $n - 1$ Kanten.
2. $\Rightarrow$ 3.: Nimm an, G habe s Zusammenhangskomponenten. Die Zusammenhangskomponenten haben nach Voraussetzung keine Zyklen und sind deshalb Bäume. Wegen 1) $\Rightarrow$ 2) besitzt jede Komponente eine Kante weniger als Knoten. Bei s Komponenten, also $n - s$ Kanten. G hat aber $n - 1$ Kanten, also $s = 1$ und G ist zusammenhängend.
3. $\Rightarrow$ 4.: Sei H der Graph, der aus G durch Entfernen einer Kante entsteht. H hat dann $n - 2$ Kanten, also nach Satz aus 7.7 mindestens 2 Komponenten.
4. $\Rightarrow$ 5.: Da G zusammenhängend ist, sind je zwei Knoten durch einen Pfad verbindbar. Falls ein gewisses Paar Knoten v, w durch verschiedene Pfaden zu verbinden wäre, können wir, ohne den Zusammenhang zu zerstören, von genau einem der Pfade eine Kante weglassen. Dies ist ein Widerspruch zur Annahme.

5. $\Rightarrow$ 6.: Hätte G einen Zyklus , dann kann man je zwei Knoten in diesem Zyklus durch mindestens 2 Pfade zu verbinden, im Widerspruch zur Annahme. Also hat G keinen Zyklus.
Falls eine Kante $\{v, w\}$ an G zugefügt wird, dann entsteht ein Zyklus, denn v und w sind schon durch einen Pfad verbunden.
Würden 2 Zyklen entstehen, dann müssten die beiden die Kante $\{v, w\}$ enthalten. Dann gäbe es aber auch einen Zyklus, der $\{v, w\}$ nicht enthält, im Widerspruch zum eben gezeigten.
6. $\Rightarrow$ 1.: Wir brauchen nur zu zeigen, dass G zusammenhängend ist. Nehme an, G wäre nicht zusammenhängend. Würden wir eine Kante hinzufügen, die einen Knoten einer Komponente mit einem Knoten einer anderen Komponente verbindet, so entsteht kein Zyklus, (warum nicht?) Widerspruch zur Annahme. ---

Aufgaben

Aufgabe 9.17 Finde mit Hilfe einer Skizze die Anzahl $T(n)$ der nicht-isomorphen Bäume mit n Ecken für $n = 1, 2, 3, 4, 5, 6$.

9.9 Der Algorithmus von Dijkstra

Sei G ein gewichteter und zusammenhängender Graph und v ein Knoten von G. Der Algorithmus von Dijkstra bestimmt einen kürzesten Weg in G von v zu einem beliebigen Knoten von G.

Satz 9.6 Algorithmus von Dijkstra
Initialisierung: $\widetilde{V} = \{v\}$, $K = \emptyset$, $\ell(v) = 0$.
Sei induktiv $\widetilde{V}$ und K gegeben, sowie $\ell\colon \widetilde{V} \to \mathbb{N}$.

- Stopp, wenn $\widetilde{V} = V$.
- Sonst, wähle eine Kante uw, sodass:
  - $u \in \widetilde{V}$
  - $w \in V \setminus \widetilde{V}$
  - $\varphi(uw) + \ell(u)$ minimal.

  Setze $\widetilde{V} := \widetilde{V} \cup \{w\}$, $K := K \cup \{(u,w)\}$ und $\ell(w) := \varphi(u,w) + \ell(u)$.

Dann ist $(\widetilde{V}, K)$ ein Baum mit Wurzel v und $\ell(w)$ ist die Länge des kürzesten Weges in G von v nach w.

Beweis. Wir definieren $\ell\colon V \times V \to \mathbb{R}$ mit $\ell(v,w)$ ist die (gewichtete) Länge des kürzesten Weges von v von w im Graph G. Somit ist $\ell(w) = \ell(v,w)$ als Abkürzung.

In jedem Schritt der Algorithmus ist $(\widetilde{V}, K)$ ein Baum mit Induktionsgemäß der Eigenschaft, dass für alle $u \in \widetilde{V}$ der Weg von v nach u in $(\widetilde{V}, K)$ auch der kürzeste Weg in G ist. Sei u und w wie im Algorithmus und ein Weg W von v nach w in G mit minimaler Länge. Sei $u' \in \widetilde{V}$ so gewählt, sodass der Teilweg von W welche von u nach u' nach ganz in K liegt und w' der nachfolgende Knoten von u' in W. Die Teilwege von W von u nach u' und von u' nach w sind ebenfalls kürzeste Wege in G. Es folgt, dass die Länge $\ell(v,w)$ des kürzesten Weges W gleich

$$\begin{aligned} \ell(v,w) &= \ell(vu') + \varphi(u',w') + \ell(w',w) \\ &= \ell(u') + \varphi(u',w') + \ell(w',w) \end{aligned}$$

ist. Nun ist im Algorithmus $\ell(u') + \varphi(u',w') \geq \ell(u) + \varphi(u,w) = \ell(v,u) + \varphi(u,w)$ und diese ist die Länge eines Weges von v nach w. Somit ist $\ell(w',w) = 0$ und $w' = w$ und $\ell(u') + \varphi(u',w) = \ell(u) + \varphi(u,w)$. ∎

Aufgaben

Aufgabe 9.18 1. Skizzieren Sie den zur nachstehenen Adjazenzmatrix gehörigen

ungerichten gewichteten Graphen.

$$\begin{pmatrix} 0 & 13 & 6 & 9 & 0 & 0 & 0 & 0 & 0 & 0 \\ 13 & 0 & 4 & 0 & 14 & 0 & 3 & 0 & 0 & 0 \\ 6 & 4 & 0 & 10 & 5 & 9 & 0 & 1 & 0 & 0 \\ 9 & 0 & 10 & 0 & 0 & 15 & 0 & 0 & 17 & 0 \\ 0 & 14 & 5 & 0 & 0 & 0 & 4 & 7 & 0 & 0 \\ 0 & 0 & 9 & 15 & 0 & 0 & 0 & 11 & 8 & 0 \\ 0 & 3 & 0 & 0 & 4 & 0 & 0 & 6 & 0 & 8 \\ 0 & 0 & 1 & 0 & 7 & 11 & 6 & 0 & 1 & 12 \\ 0 & 0 & 0 & 17 & 0 & 8 & 0 & 1 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & 12 & 5 & 0 \end{pmatrix}$$

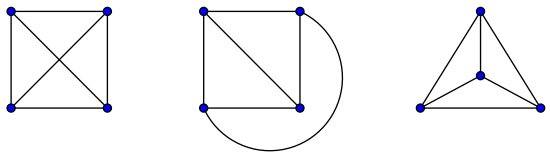
2. Bestimmen Sie mithilfe des Dijkstra-Algorithmus einem Baum kürzest Wege mit Knoten 3 als Wurzel. Ergänzen Sie Ihre Skizze aus dem ersten Teil.

9.10 Planare Graphen

Einen Graphen kann man durch Punkte und Linien in der Ebene veranschaulichen.

Definition: Ein Graph heißt plättbar oder planar, wenn man ihn so in die Ebene zeichnen kann, dass sich seine Kanten nicht schneiden. Den so in die Ebene gezeichneten Graphen nennen wir dann ebenen Graph.

Links sehen Sie einen planaren (aber nicht ebenen) Graphen, daneben zwei ebene Darstellungen von ihm:



Ein ebener Graph teilt die Ebene in verschiedene Flächen auf. Dabei wird die äußere, unbegrenzte stets mitgezählt. Im obigen Beispiel sind dies also 4 Flächen, der Graph hat 6 Kanten und 4 Knoten. Es gilt $4 - 6 + 4 = 2$. Dies gilt allgemein:

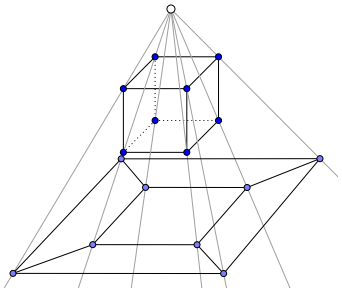
Satz 9.7 (Eulersche Polyederformel) Sei G ein ebener zusammenhängender Graph mit e Knoten und k Kanten, der die Ebene in f Flächen unterteilt. Dann gilt:

$$e - k + f = 2$$

Beweis. Da G zusammenhängend ist, gilt $k \geq e - 1$. Wir führen den Beweis durch Induktion nach der Anzahl k der Kanten durch. Ist $k = e - 1$, so ist G ein Baum, die Ebene besteht also noch aus $f = 1$ zusammenhängendem Gebiet. Somit gilt: $e - k + f = e - (e - 1) + 1 = 2$.

Sei nun G ein Graph mit $k' = k + 1 > e - 1$ Kanten, der die Ebene in f' Flächen zerlegt. Dann ist G kein Baum, enthält also einen Zyklus. Entfernen wir eine Kante aus diesem Zyklus, so erhalten wir einen neuen Graphen mit k Kanten und nach wie vor e Knoten, der die Ebene in $f = f' - 1$ Flächen zerlegt. Nach Induktion gilt für diesen die Eulersche Polyederformel und es folgt: $e - k' + f' = e - (k - 1) + (f - 1) = e - k + f = 2$.

Warum Polyederformel? Euler hat seine Formel ursprünglich nicht für Graphen, sondern für konvexe Polyeder (d.h. Polyeder ohne Dellen oder Löcher) formuliert. Jeder konvexe Polyeder liefert uns einen ebenen Graphen, wenn wir ihn über einer Ebene platzieren, eine Lampe über eine seiner Flächen halten, und damit seine Ecken und Kanten auf die Ebene projizieren.



Nach obiger Zählung gilt dann $e = \#\text{Ecken}$, $k = \#\text{Kanten}$ und $f = \#\text{Flächen}$ des Polyeders. Aus dem Beweis der eulerschen Polyederformel für Graphen, folgt somit automatisch die für Polyeder.

Satz 9.8 Sei G ein einfacher ebener Graph mit e Knoten und k Kanten, der die Ebene in f Flächen zerlegt. Dann ist $3f \leq 2k$. Enthält G keine Dreiecke, so gilt sogar $4f \leq 2k$.

Beweis. Sei dazu f_i die Anzahl der i-Ecke in G, d.h. die Anzahl der Flächen, die von genau i Kanten begrenzt werden. Dann gilt

$$3f = 3(f_3 + f_4 + f_5 + \cdots) \leq 3f_3 + 4f_4 + 5f_5 + \cdots = 2k,$$

da jede Kante an genau zwei Gebiete grenzt.
Gibt es keine Dreiecke, d.h. ist $f_3 = 0$, so folgt

$$4f = 4(f_4 + f_5 + \cdots) \leq 4f_4 + 5f_5 + \cdots = 2k.$$

Satz 9.9 Der vollständige Graph K_5 und der bipartite Graph $K_{3,3}$ sind nicht plättbar.

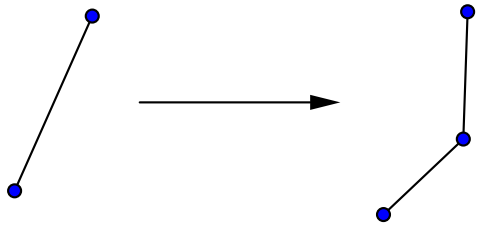
Beweis.

1. K_5 hat $e = 5$ Knoten uns $k = \binom{5}{2} = 10$ Kanten. Angenommen K_5 wäre plättbar, dann müsste er die Ebene in $f = 2 + k - e = 7$ Flächen zerlegen. Daraus folgt:
$$3f = 21 > 20 = 2k$$
im Widerspruch zum Lemma.

2. $K_{3,3}$ hat $e = 3 + 3 = 6$ Knoten uns $k = 3 \cdot 3 = 9$ Kanten. Angenommen $K_{3,3}$ wäre plättbar, dann müsste er die Ebene in $f = 2 + k - e = 5$ Flächen zerlegen. Daraus folgt:
$$4f = 20 > 18 = 2k,$$
was wieder im Widerspruch zum Lemma steht, da ein bipartiter Graph keine Dreiecke enthält.

Gibt es noch mehr nicht plättbare Graphen? Ja, aber „keine interessanten“.
Wie erzeugt man weitere „uninteressante“ nicht planare Graphen?

1. Entsteht G' aus G durch unterteilen ei
Kante durch einen Knoten, so ist G' ge
dann planar, wenn auch G planar ist.



2. Ist G plättbar, so natürlich auch jeder Teilgraph $G' \subseteq G$. Oder umgekehrt: Ist G' nicht plättbar, dann auch nicht G. Die jeweils andere Implikation gilt natürlich nicht.

Satz: (Kuratowski, 1930) Ein Graph ist genau dann nicht planar, wenn er einen Teilgraphen enthält, der durch unterteilen von Kanten aus K_5 oder $K_{3,3}$ entsteht.
Die Richtung $\Leftarrow$ haben wir eben erklärt. Die Rückrichtung $\Rightarrow$ ist schwierig.

Aufgaben

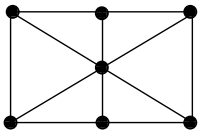
Aufgabe 9.19 Sei $G = (V, E)$ ein zusammenhängender einfacher ungerichteter Graph. Zeigen Sie:

1. Ist G eben und wird jede der Flächen in die G die Ebene unterteilt, von genau 3 Kanten begrenzt, so ist $|E| = 3|V| - 6$.

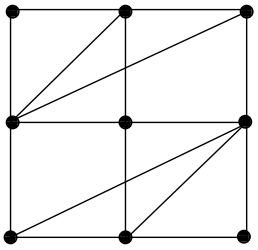
2. Is $|V| \geq 11$, so kann höchstens einer der Graphen G oder $\overline{G}$ planar sein. Hierbei ist $\overline{G}$ der zu G kompementären Graphen.

Aufgabe 9.20 Welche der folgenden Graphen sind plättbar? Begründe Deine Antwort.

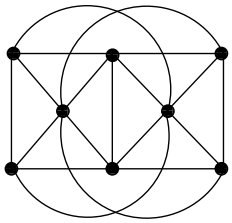
a)



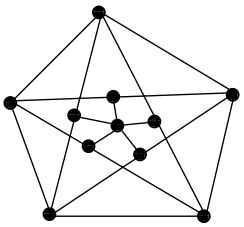
b)



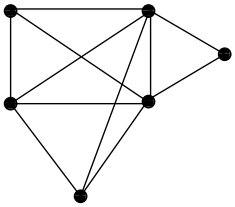
c)



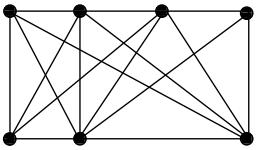
d)



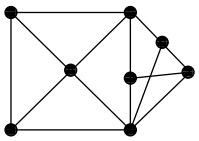
e)



f)



g)



h)