ELEMENTARMATHEMATIK

FELIX GÖBLER AND ALEX KÜRONYA

Inhaltsverzeichnis

Die Idee des Lehrtexts / Gebrauchsanweisung

Dieser Lehrtext ist als interaktives Lehrmaterial für das Online- oder Selbststudium gedacht, was gewisse Besonderheiten mit sich bringt. Hier sind die Eckpunkte, die man im Kopf behalten soll.

Aufteilung des Lehrmaterials. Jeder Abschnitt entspricht dem Material für 1-2 Wochen, in unserem konkreten Fall ca. 3-4 Vorlesungsstunden. Die Erwartung ist, dass man außerhalb der Veranstaltungszeiten *mindestens* ca. 1-2 mal so viel, das heißt ungefähr mindestens 6-8 Stunden pro Abschnitt, eingenständig studiert. Im Prinzip sollen Abschnitte greifbare und abgerundete Teile der Mathematik sein.

Wiederholung/Vorbereitung für die Abschnitte. Jeder Abschnitt fängt mit einer kurzen Liste an, die sagt, welches Material aus der Schule welche bisherigen Kapitel als Grundlage dienen. Unser Vorschlag ist, dass man das Material aus der Liste mindestens kurz durchblättern soll, sodass die erwähnten Begriffe und Techniken etwas aufgefrischt werden.

Leitfragen. Zu Beginn jedes Abschnitts finden Sie eine oder wenige Leitfragen, die im Laufe des Abschnittes hoffentlich gründlich erklärt werden. Sie haben das Material des Abschnittes gut verstanden, wenn Sie die Leitfrage(n) selbstständig mit Beweis beantworten können. Diese Fragen dienen auch als Lösung zum Problem 'Was werde ich hier lernen?'

Aktivitätspunkte oder Schnell-Aufgaben. Vielerorts im Text werden Sie kleinere Aufgaben finden, die mit (**A**) gekennzeichnet sind. Diese sollten Sie unbedingt auf der Stelle versuchen zu lösen. Auch wenn man sie vielleicht nicht schafft, der Versuch ist sehr wichtig. Anderseits, wenn man wirklich keine Ahnung von der Aufgabe hat, ist das ein Zeichen davon, dass die Wiederholung der früherer Teile des Abschnittes oder des Vorbereitungsmaterials eine gute Idee ist.

Bonusinhalt. Vielerorts im Text werden Sie das Symbol (*) vorfinden. Dieses kennzeichnet Inhalte, welche nicht klausurrelevant sind und übersprungen werden können. Allerdings handelt es sich dabei meist um wichtige Aussagen oder Anmerkungen, welche Ihr Verständnis vertiefen könnten. Wir empfehlen grundsätzlich diese Punkte zumindest grob zu verstehen.

Übungsaufgaben. Am Ende jedes Abschnittes und teilweise auch mittendrin gibt es einige Aufgaben, die dazu dienen, das Verständnis des Materials des Abschnittes zu überprüfen. Wir empfehlen Ihnen möglichst viele dieser Aufgaben zu bearbeiten. Auch hier gilt, dass jeder Versuch zählt.

Leitfrage: Logik

FEHLT

Leitfrage: Mengentheorie

Es seien $A, B \subseteq G$ Mengen. Mit welchen Methoden kann man beweisen, dass genau dann $A \subseteq B$ gilt, wenn $A \cup B = B$ ist?

Leitfrage: Abbildungen

Seien $A, B \subseteq \mathbb{R}$ und $f\colon A \to B$ mit Abbildungsvorschrift $x \mapsto x^2$. Ist f eine Abbildung? Wie müssen A und B gewählt werden, damit f injektiv, surjektiv oder gar bijektiv ist?

Leitfrage: Mächtigkeit

In einem Tanzverein mit 50 Mitgliedern werden die drei Disziplinen Klassisch, Latin und Rock'n Roll angeboten. Die Disziplinen Klassisch und Rock'n Roll betreiben jeweils 22 Mitglieder. Nur die Latin Disziplin betreiben 10 Tanzende. 38 Mitglieder betreiben Rock'n Roll und/oder Latin. Alle drei Disziplinen betreibt ein Mitglied. Genau in zwei Disziplinen aktiv sind 26 Mitglieder. Gehen Sie davon aus, dass jedes Mitglied mindestens eine Disziplin betreibt. Wie viele Mitglieder betreiben genau eine Disziplin?.

Leitfrage: Induktion

Wie kann man zeigen, dass für jede natürliche Zahl n gilt $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$?

Leitfrage: Kombinatorik

Wie viele Möglichkeiten gibt es, ein Lotterieticket, bei dem man 6 Zahlen aus 49 auswählen muss, auszufüllen?

Leitfrage: Teilbarkeit I

Es seien a und b ganze Zahlen. Gibt es einen Zusammenhang zwischen dem größten gemeinsamen Teiler und dem kleinsten gemeinsamen Vielfachen von a und b? Wir werden sehen, dass folgendes gilt:

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

Leitfrage: Teilbarkeit I Teil 2

Es sei n eine ganze Zahl. Wie kann man beweisen, dass $5|n^5 - n$ immer zutrifft?

Leitfrage: Teilbarkeit II

Gibt es reelle Zahlen, die nicht rational sind? Falls ja, wie kann man zeigen, dass eine reelle Zahl, wie z.B. $\sqrt{2} + \sqrt{3}$, *keine* rationale Zahl ist?

Leitfrage: Zahlensysteme

Gibt es Teilbarkeitsregeln wie z.B. die Quersummenregel bei Teilbarkeit durch 9 oder die alternierende Quersummenregel bei Teilbarkeit durch 11 in anderen Zahlensystemen? Ist es richtig z.B. im Zwölfersystem die gleichen Regeln bei Teilbarkeit mit 11 und 13 zu erwarten?

Leitfrage: Polynome I

Wie viele und welche reellen Nullstellen hat das Polynom $f(X) = 2X^4 + 4X^3 - 24X^2 - 26X + 24$?

Leitfrage: Polynome II

Wie kann man beweisen, dass das Polynom $f(X) = X^7 + 14X^5 + 20 \in \mathbb{Q}[X]$ nicht als Produkt von nicht-konstanten Polynomen kleineren Grades mit Koeffizienten aus $\mathbb{Q}$ geschrieben werden kann?

Leitfrage: Ungleichungen

Für welche reelle Zahlen x gilt die Ungleichung

$$\frac{x-1}{x-2} < \frac{2x-3}{x-4} \; ?$$

Leitfrage: Folgen

Konvergiert die Zahlenfolge

$$\frac{2n^2 + 3n + 5}{3n^2 + n + \pi n} \; ?$$

Falls ja, wie kann man ihren Grenzwert bestimmen?

1. Logik

1.1. **Wiederholung.** Sollten Sie in Ihrer Schulzeit bereits Wahrheitstafeln begegnet sein, so lohnt sich ein kurzer Blick darauf. Andernfalls können Sie auch problemlos ohne Vorwissen starten.

Leitfrage.
- *Wahrheitswert einer zusammengesetzen Aussage mithilfe einer Wahrheitstafel bestimmen.*
- *Logische Rätsel lösen.*

1.2. **Aussagenkalkül.** Mathematische Logik ist im Grunde genommen die Sprache der Mathematik. Diese ist unabdingbar um z.B. einen mathematischen Beweis zu formulieren oder einen Sachverhalt mathematisch Korrekt beschreiben zu können.

Die Grundlage für diese Sprache bildet die sogenannte *Aussagenlogik*:

- Eine *Aussage* im mathematischen Sinn ist ein als Satz formulierter Gedanke, den man auf sinnvollem Wege einen Wahrheitswert zuordnen kann.
- In der Mathematik beschäftigen wir uns mit Aussagen, die entweder „wahr“ oder „falsch“ sind, aber nicht beides.

Beispiel 1.1. Folgendes sind mathematische Aussagen:

- 2 ist eine gerade Zahl.
- Ein Monat hat 30 Tage.
- Wenn es nass ist, regnet es.
- 4 ist eine Quadratzahl.
- $(a+b)^2 = a^2 + 2ab + b^2$.

Folgende Aussagen hingegen sind **keine** mathematischen Aussagen:

- Das Mathegebäude ist schön.
- Ich mag Züge.
- Diese Aussage ist falsch.
- $x + 5$.

Konvention: Wir benutzen w oder 1 für wahr und f oder 0 für falsch.

Aussagen kann man auf verschiedene Art und Weise kombinieren. Das Ziel dieses Abschnittes ist es daher, einen Überblick über die Kombinationsmöglichkeiten zu geben. Mit diesem Handwerkszeug ist es anschließend möglich, einzelne Aussagen zusammenzusetzen und somit neue Aussagen zu generieren. Dabei lässt sich der Wahrheitswert dieser *zusammengesetzen Aussage* mithilfe der Wahrheitswerte der Bausteine ermitteln. Dazu werden meist Wahrheitstafeln verwendet und die zusammengesetzen Aussagen werden in ihre Bestandteile zerlegt.

Bemerkung 1.2. Die im Folgenden definierten Operationen heißen auch *logische Verknüpfungen*.

Definition 1.3. (Konjunktion, und)
Die Konjugation zweier Aussagen A und B ist die Aussage „$\mathbf{A \wedge B}$“, die genau dann wahr ist,

wenn A und B gleichzeitig wahr sind. Das lässt sich durch eine Wahrheitstafel ausdrücken:

A	B	A ∧ B
1	1	1
1	0	0
0	1	0
0	0	0

A **1.4.** *Betrachten Sie die Aussagen $A =$ „24 ist eine gerade Zahl.“ , $B =$ „24 ist durch 3 teilbar.“ und $C =$ „24 ist durch 5 teilbar.“*
Welche der Konjunktionen $A \wedge B, A \wedge C, B \wedge C$ sind wahr, welche falsch?

Definition 1.5. (Disjunktion, oder)
Die Disjunktion zweier Aussagen A und B ist die Aussage „$\mathbf{A} \vee \mathbf{B}$“, die genau dann wahr ist, wenn mindestens eine der Aussagen A oder B wahr ist.

Achtung: In der natürlichen Sprache bedeutet „A oder B“ oft „entweder A oder B“, aber nicht beides. Das ist hier nicht der Fall. Ein mathematisches „oder“ ist **nicht** ausschließend. Die Wahrheitstafel zeigt diesen Sachverhalt in der zweiten und dritten Zeile:

A	B	A ∨ B
1	1	1
1	0	1
0	1	1
0	0	0

A **1.6.** *Seien A, B, C wie in Übungsaufgabe 1. Welche der Aussagen $A \vee B, A \vee C, B \vee C$ sind wahr, welche falsch?*

Definition 1.7. (Negation, nicht)
Die Negation der Aussage A ist „$\neg\mathbf{A}$“, die genau dann wahr ist, wenn A falsch ist.

Die Wahrheitstafel der Negation ist:

A	¬ A
1	0
0	1

Beispiel 1.8.
- Sei $A =$ „5 ist gerade“. Dann ist die Negation gegeben durch $\neg A =$ „5 ist ungerade“.
- Sei $A =$ „Diese Kuh ist schwarz“. Dann ist $\neg A =$ „Diese Kuh ist nicht schwarz“.

A **1.9.** *Seien A, B, C wie in Übungsaufgabe 1. Was sind die Wahrheitswerte der Aussagen $\neg A \vee A, \neg A \wedge B, (B \vee \neg A) \wedge C$?*

Definition 1.10. (Implikation, Folgerung)
Unter „$\mathbf{A} \Rightarrow \mathbf{B}$“ („$A$ impliziert B“, „aus A folgt B“) verstehen wir die Aussage $\neg A \vee B$.

Die Wahrheitstafel der Implikation ist:

A	B	A ⇒ B
1	1	1
1	0	0
0	1	1
0	0	1

Beispiel 1.11. Seien A, B Aussagen. Wir betrachten die Wahrheitstafeln folgender Implikationen:

- $(A \wedge B) \Rightarrow A$.
  Die Strategie ist, wie zuvor erwähnt, die zusammengesetze Aussage $(A \wedge B) \Rightarrow A$ zu zerlegen in die Aussagen $A \wedge B$ und A, für welche zunächst die jeweiligen Wahrheitswerte in die Tafel eingetragen werden. Anschließend wird der Wahrheitswert der Implikation überprüft.

A	B	(A ∧ B)	⇒	A
1	1	1	1	1
1	0	0	1	1
0	1	0	1	0
0	0	0	1	0

  Da die Implikation für jede Kombination wahr ist, ist somit insgesamt die Aussage $(A \wedge B) \Rightarrow A$ wahr.
- $A \Rightarrow (A \wedge B)$:

A	B	A ⇒ (A ∧ B)
1	1	1
1	0	0
0	1	1
0	0	1

- $A \vee B \Rightarrow A$:

A	B	(A ∨ B) ⇒ A
1	1	1
1	0	1
0	1	0
0	0	1

- $A \Rightarrow (A \vee B)$:

A	B	A ⇒ (A ∨ B)
1	1	1
1	0	1
0	1	1
0	0	1

Ⓐ **1.12.** *Füllen Sie die Wahrheitstafeln des vorigen Beispieles aus, indem Sie die Wahrheitswerte der Zwischenschritte eintragen.*

Definition 1.13. (Äquivalenz, $\Leftrightarrow$)
Die logische Äquivalenz „$\mathbf{A} \Leftrightarrow \mathbf{B}$“ der Aussagen A und B („A gilt *genau dann, wenn* B gilt"), ist die zusammengesetzte Aussage $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

Bemerkung 1.14. Achten Sie ab sofort stets auf die Formulierung „genau dann, wenn“. Damit ist immer eine Äquivalenz gemeint. Möchte man zeigen, dass zwei Aussagen äquivalent sind, so muss man stets beide Richtungen (Implikationen) beweisen oder Äquivalenzumformungen durchführen. Ein klassisches Beispiel für eine Äquivalenzumformung kennen Sie aus der Schule:

$$\begin{aligned} 3x - 2 &= 5 \quad | + 2 \\ \Leftrightarrow 3x &= 7. \end{aligned}$$

Dabei handelt es sich um eine Äquivalenzumformung, da man durch Addition von 2 von der ersten Aussage auf die zweite schließen kann und umgekehrt durch Subtraktion von 2 von der zweiten auf die erste Aussage.

(A) 1.15. *Drücken Sie $A \Leftrightarrow B$ mithilfe von $\wedge, \vee$ und $\neg$ aus. Zeigen Sie dazu zunächst, dass tatsächlich $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$ gilt.*

Beispiel 1.16. Seien A, B Aussagen. Dann sind die Wahrheitstafeln von $A \Rightarrow B$, $B \Rightarrow A$ und $A \Leftrightarrow B$ wie folgt gegeben.

A	B	A ⇒ B
1	1	1
1	0	0
0	1	1
0	0	1

A	B	B ⇒ A
1	1	1
1	0	1
0	1	0
0	0	1

A	B	B ⇔ A
1	1	1
1	0	0
0	1	0
0	0	1

Zwei Aussagen heißen *logisch äquivalent*, wenn sie den gleichen Wahrheitswert haben:

Definition 1.17. Eine zusammengesetzte Aussage heißt *Tautologie*, falls sie immer wahr ist, unabhängig davon, welche Wahrheitswerte die verknüpften Einzelaussagen besitzen (also ergibt jede Kombination der Wahrheitswerte der Einzelaussagen eine wahre Aussage).

Satz 1.18. *Seien A, B und C logische Aussagen. Die folgenden Ausdrücke sind Tautologien:*

(1) $\neg(\neg A) \Leftrightarrow A$. *(Doppelte Verneinung)*

(2) *(Verneinungsregeln / De Morgan'schen Regeln)*

$$\begin{aligned} \neg(A \wedge B) &\Leftrightarrow (\neg A) \vee (\neg B), \\ \neg(A \vee B) &\Leftrightarrow (\neg A) \wedge (\neg B). \end{aligned}$$

(3) *(Kommutativgesetze)*

$$A \wedge B \Leftrightarrow B \wedge A \quad \text{und} \quad A \vee B \Leftrightarrow B \wedge A.$$

(4) *(Assoziativgesetze)*

$$\begin{aligned} A \wedge (B \wedge C) &\Leftrightarrow (A \wedge B) \wedge C \\ \text{und } A \vee (B \vee C) &\Leftrightarrow (A \vee B) \vee C. \end{aligned}$$

(5) *Distributivgesetze*

$$\begin{aligned} A \wedge (B \vee C) &\Leftrightarrow (A \wedge B) \vee (A \wedge C), \\ A \vee (B \wedge C) &\Leftrightarrow (A \vee B) \wedge (A \vee C). \end{aligned}$$

Beweis: Alle Aussagen können wir mit Wahrheitstafeln beweisen. Den Beweis für i) und ii) finden Sie im Buch von Klaus Fritzsche auf Seite 26. Für die restlichen Aussagen zeigen wir exemplarisch jeweils eine davon. Notwendigerweise haben wir hier auch schon ersten Kontakt mit Kombinatorik. Wie eingangs erwähnt haben mathematische Aussagen den Wahrheitswert

wahr oder falsch. Das heißt wir müssen, abhängig von der Anzahl der vorkommenden Einzelaussagen $A, B, C, \ldots$, die Anzahl der Kombinationen derselben ermitteln. Da jede Einzelaussage zwei Zustände haben kann, ist für k Einzelaussagen die Anzahl der Kombinationen gegeben durch 2^k. Dementsprechend haben wir in iii) eine Tabelle mit $2^2 = 4$ Zeilen (ohne Kopfzeile) und in iv) und v) eine mit $2^3 = 8$ Zeilen.

iii) Um das Beweisschema zu verdeutlichen, werden die Schritte farblich getrennt. Zuerst werden die blauen Werte ermittelt und damit anschließend die Äquivalenz nachgewiesen.

A	B	$A \wedge B$	$\Leftrightarrow$	$B \wedge A$
1	1	1	1	1
1	0	0	1	0
0	1	0	1	0
0	0	0	1	0

iv) Wir gehen vor wie in (iii), allerdings benötigen wir mehr Zwischenschritte. Die logische Reihenfolge des Beweises ist nun farblich gekennzeichnet durch blau-rot-schwarz.

A	B	C	A	$\wedge$	$(B \wedge C)$	$\Leftrightarrow$	$(A \wedge B)$	$\wedge$	C
1	1	1	1	1	1	1	1	1	1
1	1	0	1	0	0	1	1	0	0
1	0	1	1	0	0	1	0	0	1
1	0	0	1	0	0	1	0	0	0
0	1	1	0	0	1	1	0	0	1
0	1	0	0	0	0	1	0	0	0
0	0	1	0	0	0	1	0	0	1
0	0	0	0	0	0	1	0	0	0

v) Farben wie in iv).

A	B	C	A	$\wedge$	$(B \vee C)$	$\Leftrightarrow$	$(A \wedge B)$	$\vee$	$(A \wedge C)$
1	1	1	1	1	1	1	1	1	1
1	1	0	1	1	1	1	1	1	0
1	0	1	1	1	1	1	0	1	1
1	0	0	1	0	0	1	0	0	0
0	1	1	0	0	1	1	0	0	0
0	1	0	0	0	1	1	0	0	0
0	0	1	0	0	1	1	0	0	0
0	0	0	0	0	0	1	0	0	0

□

A 1.19. *Ergänzen Sie den Beweis von ii) bis v) um die fehlenden Teile. Gehen Sie dabei genauso vor wie oben angegeben.*

A 1.20. *(Äquivalenzprinzip)*
Seien A und B logische Aussagen. Zeigen Sie: Ist A eine Tautologie und $A \Leftrightarrow B$ eine Tautologie, dann ist B ebenfalls eine Tautologie.

Mathematische Argumentation beruht auf dem Begriff der Implikation.

Idee: Wenn A stimmt und B aus A folgt, dann sollte auch B stimmen. Jetzt können wir diese Idee formalisieren und verifizieren:

Satz 1.21. *(Ableitungsregel)*
Seien A, B und C logische Aussagen. Dann ist die zusammengesetzte Aussage

$$\Big(A \wedge (A \Rightarrow B)\Big) \Rightarrow B$$

eine Tautologie.

Beweis: Wie schon in Satz 1.18 genügt eine Wahrheitstafel als Beweis. Es gilt

A	B	A	$\wedge$	$(A \Rightarrow B)$	$\Rightarrow$	B
1	1	1	1	1	1	1
1	0	1	0	0	1	0
0	1	0	0	1	1	1
0	0	0	0	1	1	0

□

Ein weiteres Argumentationsbeispiel: Falls B aus A folgt und C folgt aus B, dann sollte aus A auch C folgen. Auch diese Aussage lässt sich schnell mit einer Wahrheitstafel beweisen. Eine alternative Formulierung für diese Aussage ist: Implikationen sind transitiv.

Satz 1.22. *(Syllogismusregel)*
Seien A, B und C logische Aussagen. Dann gilt

$$\Big((A \Rightarrow B) \wedge (B \Rightarrow C)\Big) \Rightarrow (A \Rightarrow C)$$

Beweis: Die Wahrheitstafel lautet:

A	B	C	$(A \Rightarrow B)$	$\wedge$	$(B \Rightarrow C)$	$\Rightarrow$	$(A \Rightarrow C)$
1	1	1	1	1	1	1	1
1	1	0	1	0	0	1	0
1	0	1	0	0	1	1	1
1	0	0	0	0	1	1	0
0	1	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1

□

(A) 1.23. *(Kontraposition)*
Seien A und B logische Aussagen. Beweisen Sie das wichtige Kontrapositionsprinzip

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A).$$

(A) 1.24. *(Ringschluss)*
Seien A, B und C logische Aussagen. Zeigen Sie: A, B und C sind genau dann paarweise äquivalent (das heißt $A \Leftrightarrow B$, $B \Leftrightarrow C$ und $A \Leftrightarrow C$), wenn $A \Rightarrow B$, $B \Rightarrow C$ und $C \Rightarrow A$ gelten.

1.3. **Prädikatenlogik.** Jetzt gehen wir ein Stück weiter, und machen unsere Logik komplizierter und nützlicher zugleich. Diese Erweiterung der Aussagenlogik wird als *Prädikatenlogik* bezeichnet.

Definition 1.25. Eine *Aussageform* ist ein Satz, der formal wie eine Aussage aussieht, aber eine oder mehrere Variablen enthält. Eine *Variable* ist der Name für eine Leerstelle in einer Aussage. An Stelle der Variablen kann ein konkretes Objekt eingesetzt werden, wobei nur solche Objekte eingesetzt werden sollen, welche zu sinnvollen Aussagen führen. Wir sagen dazu, dass die Objekte aus einem *zulässigen Objektbereich* gewählt werden.

Beispiel 1.26. Die Gleichung

$$2^3 + 25 \cdot 2 - 1 = 0$$

ist eine Aussage, wohingegen

$$x^3 + 25x - 1 = 0 \ , \ x \in \mathbb{R}$$

eine Aussageform $A(x)$ ist für jedes $x \in \mathbb{R}$ (zulässiger Objektbereich). Allerdings ist $A(x = r)$ eine Aussage, die entweder wahr oder falsch ist (in Abhängigkeit vom Wert von $r \in \mathbb{R}$). Zum Beispiel für $x = 1$ ist die Aussage $1^3 + 25 - 1 = 0$ offenbar falsch.

Wichtig: Alles, das wir über Aussagen A gelernt haben, bleibt für Aussageformen $A(x)$ wahr. Diese kann man beispielsweise verknüpfen

$$A(x) \wedge B(x) \ , \ \neg A(x) \text{ usw.}$$

und erhält eine neue Aussageform.

Neuigkeit: *Sollten Sie mit dem folgenden Abschnitt Schwierigkeiten haben, lesen Sie diesen erneut, sobald Sie sich etwas mit Mengen auskennen.*
Es kann sein, dass für die Aussageform $A(x)$ die Aussage $A(a)$ für jedes a aus dem zulässigen Objektbereich O richtig ist. Dann sagen wir: „Für jedes a aus O gilt $A(a)$“, oder äquivalent

$$\forall a \in O : A(a) \, .$$

Gilt die Aussage $A(a)$ für (mindestens) ein a aus dem Objektbereich, so sagen wir: „Es gibt ein a aus O, für das $A(a)$ gilt“, oder äquivalent

$$\exists a \in O : A(a).$$

Wir definieren daher abschließend.

Definition 1.27. (Quantoren)
Sei $A(x)$ eine Aussageform mit zulässigem Objektbereich O. Dann definieren wir die logischen Symbole $\exists$ („Es gibt ein“) und $\forall$ („Für alle“) wie folgt:

$\exists x \in O : A(x)$ bedeutet „Es gibt ein Element x aus dem Objektbereich O, sodass $A(x)$ wahr ist “.

$\forall x \in O : A(x)$ bedeutet „Für alle Elemente x aus dem Objektbereich O ist $A(x)$ wahr “.

Der Quantor $\exists$ heißt *Existenzquantor* und $\forall$ heißt *Allquantor*.

Bemerkung 1.28. (Negation von Quantoren)
Viele mathematische Definitionen sind über Quantoren und logische Aussagen definiert. Möchte man also zeigen, dass eine definierende Eigenschaft **nicht** erfüllt ist, so muss die logische Aussage negiert werden. Die Negation von Quantoren ist dabei besonders leicht: Jeder Existenzquantor wird zu einem Allquantor und umgekehrt. Dies werden wir später in der

Verneinungsregel Satz 2.38 einsehen. Das ist natürlich nur logisch: Wenn Sie behaupten, es gäbe keine Katzen, so würde die Existenz einer einzigen Katze Ihre Aussage widerlegen. Diese Existenz muss natürlich nachgewiesen werden. In der Mathematik geschieht dies in der Regel durch Konstruktion eines geeigneten Beispiels.

1.4. **Übungsaufgaben.**

Hausaufgabe 1.29. *Sei $T(x) =$ „x ist eine Primzahl“ eine Aussageform mit zulässigem Objektbereich $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$. Dann gilt*

$$T(x) \implies T(x^2 - 1).$$

Hausaufgabe 1.30. *Berechnen Sie die Wahrheitstafel zu der logischen Aussage*

$$(A \vee B) \wedge (C \vee A) \wedge (B \vee C) \iff (A \vee B \vee C).$$

Hausaufgabe 1.31. *Betrachten Sie die folgenden Aussageformen:*

$$T(x) = \text{„}x \text{ ist eine gerade Zahl“}.$$
$$S(x) = \text{„}x \text{ ist eine Quadratzahl“}.$$
$$Q(x, y) = \text{„}x \text{ ist durch } y \text{ teilbar“}.$$

Was ist der Wahrheitswert von

$$T(x) \wedge S(x) \implies Q(x, 4)?$$

1.5. **Wiederholungsaufgaben.**

1.6. **Weiterführende Literatur.**

(1) Fritsche: Mathematik für Einsteiger
(2) Junker

2.1. **Wiederholung.** Als Hintergrund brauchen Sie alles was Sie in der Schule über Mengen gelernt haben, und Abschnitt 1.

Leitfrage. *Es seien $A, B \subseteq G$ Mengen. Mit welchen Methoden kann man beweisen, dass genau dann $A \subseteq B$ gilt, wenn $A \cup B = B$ ist?*

2.2. **Was sind Mengen?** Mengentheorie bildet das Fundament der modernen Mathematik. Das Lernziel dieses Kapitels ist es Mengen mithilfe von Prädikatenlogik in der beschreibenden Darstellung darzustellen und Aussagen über Mengen auf Aussagen in der Prädikatenlogik zurückzuführen

Definition 2.1. Eine *Menge* ist eine Zusammenfassung von bestimmten, wohlunterscheidbaren Objekten („Elemente der Menge“) zu einem Ganzen.

Bemerkung 2.2. Wenn es um den Begriff von Mengen geht, ist es am wichtigsten, dass wir immer irgendwie entscheiden können, ob Objekte zu einer gegebenen Menge gehören oder nicht. Ein Objekt gehört entweder zu einer Menge oder nicht (eine andere Möglichkeit gibt es nicht), aber mehrmals kann es nicht dazugehören.

Definition 2.3. Sei M eine Menge und a ein Objekt. Der Ausdruck „$\mathbf{a \in M}$“ bedeutet dann „a ist ein Element von M“. „$\mathbf{a \notin M}$“ bedeutet, dass a kein Element von M ist.

Mengen können beschrieben werden, indem jedes Element einzeln aufgezählt wird. Elemente können dabei alles Mögliche sein, wie zum Beispiel Zahlen, Menschen, Gemüse, Möbel. Mengen können aber auch aus anderen Mengen bestehen:

Beispiel 2.4. Folgendes sind Mengen:

- $\{1, 2, 5, 6\}$ (Menge von Zahlen).
- $\Big\{\{1\}, \{1, 2\}, \{2\}\Big\}$ (Menge von Mengen).
- $\{a, b, d, f, z\}$ (Menge von Buchstaben).
- $\{*, \sim, \square, \cong, \cdot, \circ, +\}$ (Menge bestehend aus irgendwelchen Symbolen).
- $\{Malm, Frihetten, Kallax, Lack, Brimnes, Billy\}$ (Menge bestehend aus IKEA-Möbeln).

Insgesamt kann jede noch so sinnlose Ansammlung von Symbolen eine Menge bilden.

Die aufzählende Darstellung von Mengen führt schnell zu Problemen, wenn die Anzahl der Elemente größer wird. Wir bezeichnen dann zum Beispiel mit $\{1, 2, \ldots, 100\}$ die Menge aller ganzen Zahlen von 1 bis 100.

Eleganter lässt sich dieses Problem lösen, indem wir Mengen mithilfe einer Aussageform beschreiben.

Definition 2.5. Sei $A(x)$ eine Aussageform mit zulässigem Objektbereich O. Dann bezeichnet

$$M \stackrel{\text{def}}{=} \{x \in O \mid A(x)\} \text{ oder } \{x \in O : A(x)\}$$

die Menge aller x aus dem zulässigen Objektbereich O, für welche die Aussage $A(x)$ wahr ist.

Mit dieser neuen Darstellung (auch beschreibende Darstellung genannt) können wir die Menge $\{1, 2, \ldots, 100\}$ darstellen als $\{x \in \mathbb{N}_+ \mid x \leq 100\}$. Dabei ist hier $O = \mathbb{N}_+$ und $A(x) =$ „x ist kleiner gleich 100“.

Beispiel 2.6. **Wichtige Symbole:** Es gibt viele wichtige Symbole in der Mathematik. Im Folgenden wollen wir einige Symbole für bestimmte Mengen von Zahlen definieren.

- $\mathbb{N}$: Dieses Symbol bezeichnet die Menge der natürlichen Zahlen. In dieser Vorlesung zählt die Zahl 0 als natürliche Zahl. Daher gilt in aufzählender Darstellung $\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, \ldots\}$.
- $\mathbb{N}_+$: Dieses Symbol bezeichnet die Menge der natürlichen Zahlen ohne 0 (oder auch die Menge der positiven ganzen Zahlen).
- $\mathbb{Z}$: Dieses Symbol bezeichnet die Menge der ganzen Zahlen, in aufzählender Darstellung $\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}$.
- $\mathbb{Q}$: Dieses Symbol bezeichnet die Menge der rationalen Zahlen. Das sind genau die Zahlen, welche eine Darstellung als Bruch haben bzw. eine endliche oder periodische Dezimahlzahldarstellung besitzen. In der beschreibenden Darstellung können wir $\mathbb{Q}$ also wie folgt darstellen:

  $$\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}.$$

  Eine mathematisch korrekte Einführung der rationalen Zahlen können Sie in Bemerkung 11.30 finden.
- $\mathbb{R}$: Dieses Symbol bezeichnet die Menge der reellen Zahlen. Das sind in gewisser Weise alle Zahlen, die Sie kennen.

Definition 2.7. Zwei Mengen A und B heißen *gleich* („$A = B$“), wenn sie die gleichen Elemente besitzen.

Bemerkung 2.8. Seien $A := \{x \mid P(x)\}$ und $B := \{x \mid Q(x)\}$, wobei $P(x)$ und $Q(x)$ Aussageformen mit zulässigem Objektbereich O sind. Dann gilt $A = B$, falls für alle x aus dem zulässigen Objektbereich O die Aussagen $P(x)$ und $Q(x)$ äquivalent sind. Formal:

$$\forall x \in O : P(x) \Leftrightarrow Q(x).$$

Mit diesen Symbolen können wir nun Mengen besser und genauer darstellen, wenn wir die beschreibende Darstellung benutzen wollen.

Beispiel 2.9. Die beschreibende Darstellung ermöglicht präzise und trotzdem kurze Beschreibungen von Mengen:

(1) $\{0, 2, 4, 6, 8, 10, \ldots\} = \{x \in \mathbb{N} \mid x \text{ ist gerade}\} = \{x \in \mathbb{N} \mid \exists k \in \mathbb{N} : x = 2 \cdot k\}$.
(2) $\{\ldots, -6, -4, -2, 0, 2, 4, \ldots\} = \{x \in \mathbb{Z} \mid x \text{ ist gerade}\} = \{x \in \mathbb{N} \mid \exists k \in \mathbb{Z} : x = 2 \cdot k\}$.
(3) $\{1, 3, 5, 7, 9, \ldots\} = \{x \in \mathbb{N} \mid x \text{ ist ungerade}\} = \{x \in \mathbb{N} \mid \exists k \in \mathbb{N} : x = 2 \cdot k + 1\}$.

(A) **2.10.** *Beschreiben Sie die Menge aller ungeraden ganzen Zahlen in beschreibender Darstellung.*

(A) **2.11.** *Bestimmen Sie die beschreibende Darstellung der Menge*

$$M = \{0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \ldots\}.$$

Definition 2.12. (Teilmenge) Wir sagen A ist eine *Teilmenge* von B (Notation „$A \subseteq B$“), falls aus $x \in A$ folgt, dass $x \in B$ ist (d.h. $\forall x : P(x) \Rightarrow Q(x)$). Es folgt insbesondere, dass $A = B$ genau dann gilt, wenn $A \subseteq B \wedge B \subseteq A$ wahr ist. Gelegentlich nennt man eine Teilmengenbeziehung auch *Inklusion*.

Beispiel 2.13. Wir haben die Inklusionskette $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$. In Beispiel 2.9 ist die Menge aus i) in der Menge aus ii) enthalten.

Eine wichtige Frage ist: Wie zeigt man, dass zwei Mengen gleich sind?

Bemerkung 2.14. Wir haben gesehen, dass für zwei Mengen $A, B \subseteq G$ genau dann $A = B$ gilt, wenn

(*) $$\boxed{\forall x \in G : x \in A \Leftrightarrow x \in B.}$$

Es gelten daher die folgenden Eigenschaften:

$$\begin{array}{rcl} A & = & A \quad (= \text{ ist reflexiv}) \\ A & = & B \Rightarrow B = A \quad (= \text{ ist symmetrisch}) \\ ((A & = & B) \wedge (B = C)) \Rightarrow A = C \quad (= \text{ ist transitiv}). \end{array}$$

A **2.15.** *Schreiben Sie die obigen Eigenschaften mittels (*) um.*

Als nächstes werden wir aus gegebenen Mengen neue Mengen konstruieren.

Bemerkung 2.16. **Vorsicht:** Das geht nicht ohne Probleme. Z.B. „Die Menge aller Mengen“ ist leider keine Menge (das ist das Russel'sche Paradoxon).

Die folgenden Konstruktionen sind allerdings ungefährlich:

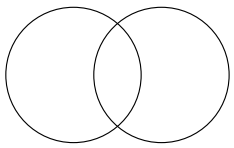
1) Teilmenge:

Es sei G eine bereits bestehende Grundmenge, $A(x)$ eine Aussageform mit einer Variablen x, deren zulässiger Objektbereich G ist. Dann ist $M := \{x \in G \mid A(x)\}$ ebenfalls eine Menge. Nach Definition 2.12 ist M somit eine Teilmenge von G.

Beispiel 2.17. Sei $G = \{1, 2, 3, 4\}$ und $A(x) = x > 2$. Dann ist M gegeben durch $M = \{3, 4\}$.

2) Vereinigung:

Seien $A, B \subseteq G$ Mengen. Die Vereinigung von A und B ist definiert als



$$\mathbf{A \cup B} := \{x \in G \mid (x \in A) \vee (x \in B)\}$$

. Das heißt $A \cup B$ besteht aus den Elementen von A und den Elementen von B.

Beispiel 2.18. Es gelten

- $\{1, 2, 3\} \cup \{4, 5\} = \{1, 2, 3, 4, 5\}$.
- $\{2, 4, 6\} \cup \{4, 6\} = \{2, 4, 6\}$.
- $A \cup \emptyset = A$.
- $\mathbb{N} \cup \mathbb{Z} = \mathbb{Z}$.
- Es gilt $A \subseteq A \cup B$, da $(x \in A) \Rightarrow \Big((x \in A) \vee (x \in B)\Big)$ wahr ist.

Aussage 2.19. *(Leitfrage)*
Es seien $A, B \subseteq G$ Mengen. Dann gilt $A \subseteq B$ genau dann, wenn $A \cup B = B$.

Beweis: Wir müssen eine „genau dann, wenn“ Aussage zeigen. Dazu müssen zwei Implikationen gezeigt werden:

„Falls $A \subseteq B$, dann ist $A \cup B = B$“: Angenommen, $A \subseteq B$, dann ist jedes Element von A sofort ein Element von B. Insbesondere sind Elemente von A oder B einfach Elemente von B.

„Falls $A \cup B = B$, dann ist $A \subseteq B$“: Angenommen $A \not\subseteq B$, d.h. es gibt ein $a \in A$, das nicht in B liegt (Kontraposition). Dann ist $a \in A \subseteq A \cup B$ und $a \notin B$, d.h. $A \cup B$ und B können nicht gleich sein. □

Zweite Lösung mittels Logik:

$$\begin{aligned} A \subseteq B \text{ bedeutet} &: \forall x \in G : (x \in A) \Rightarrow (x \in B) \\ A \cup B = B \text{ bedeutet} &: \forall x \in G : \Big((x \in A) \vee (x \in B)\Big) \Leftrightarrow (x \in B) \end{aligned}$$

Unsere Aussage ist dann äquivalent zu der Behauptung, dass

$$\Big((x \in A) \Rightarrow (x \in B)\Big) \Leftrightarrow \Big((x \in A) \vee (x \in B)\Big) \Leftrightarrow (x \in B)\Big)$$

für alle $x \in G$ eine Tautologie ist. Man schreibt jetzt $P(x)$ für $x \in A$ und $Q(x)$ für $x \in B$, dann erhalten wir die äquivalente Behauptung: Die Aussage

$$\Big(P(x) \Rightarrow Q(x)\Big) \Leftrightarrow \Big((P(x) \vee Q(x)\Big) \Leftrightarrow Q(x)\Big)$$

ist für jedes $x \in G$ eine Tautologie. □

(A) **2.20.** *Schließen Sie den obigen Beweis ab, indem Sie eine Wahrheitstafel erstellen.*

Bemerkung 2.21. Zwar scheint die zweite Lösung komplizierter zu sein, sie hat aber den wesentlichen Vorteil, dass sie das Problem auf die kleinsten Bausteine (in diesem Fall die Aussagenlogik) reduziert. Und mit der Aussagenlogik haben wir schon Erfahrungen gesammelt. Auf diesem Prinzip (ein Problem auf „bekannte“ bzw. leichtere Probleme zu reduzieren) beruht die gesamte Mathematik.

3) Schnitt(Menge):
Seien $A, B \subseteq G$ Mengen. Dann ist der *(Durch)Schnitt von A und B*

$$\mathbf{A \cap B} := \{x \in G \mid x \in A \wedge x \in B\}$$

wegen 1) eine Menge. Insbesondere ist $A \cap B$ sowohl Teilmenge von A als auch von B.

Bemerkung 2.22. Man sieht mit Satz 1.18 leicht ein, dass Durchschnittbildung kommutativ ist:

$$\begin{aligned} A \cap B &= \{x \in G \mid x \in A \wedge x \in B\} \\ &= \{x \in G \mid x \in B \wedge x \in A\} \\ &= \{x \in B \mid x \in A\} = B \cap A. \end{aligned}$$

(A) **2.23.** *Bestimmen Sie*

$$\{x \in \mathbb{N} \mid \exists k \in \mathbb{N} : x = 2k\} \cap \{x \in \mathbb{N} \mid \exists l \in \mathbb{N} : x = 2l + 1\}.$$

4) Komplement:
Wir haben gesehen, dass die logischen Operatoren $\vee$ und $\wedge$ zur Konstruktion von neuen Mengen führen. Was ist mit dem Operator $\neg$? Wir definieren für Mengen A und B die *Differenz von A und B* oder auch das *Komplement von B in A* als

$$\begin{aligned} A \setminus B &:= \{x \in A \mid x \notin B\} \\ &= \{x \in A \mid \neg(x \in B)\}. \end{aligned}$$

Beispiel 2.24.
- $\{1,2,3,4\} \setminus \{3,5,6\} = \{1,2,4\}$.
- $\{3,5,6\} \setminus \{1,2,3,4\} = \{3,6\}$. Somit ist offenbar Komplementbildung **nicht** kommutativ.
- $\mathbb{N} \setminus \{x \in \mathbb{N} \mid x \text{ ist gerade }\} = \{x \in \mathbb{N} \mid x \text{ ist ungerade}\}$.
- $\mathbb{N} \setminus \mathbb{Q} = \emptyset$, denn es gilt $\mathbb{N} \subseteq \mathbb{Q}$.
- $\mathbb{Q} \setminus \mathbb{Z}$ ist die Menge der Brüche, sodass Zähler und Nenner teilerfremd sind (also nicht gekürzt werden können) und der Nenner ungleich 1 ist.

(A) **2.25.** *Bestimmen Sie $\mathbb{Q} \setminus \mathbb{N}$.*

5) Potenzmenge: Sei M eine Menge, dann ist die Menge aller Teilmengen von M

$$\mathcal{P}(\mathbf{M}) := \{T \mid T \subseteq M\}$$

, genannt *Potenzmenge von M*, ebenfalls eine Menge.

Beispiel 2.26.
- $\mathscr{P}(\emptyset) = \{\emptyset\}$.
- $\mathscr{P}(\{a\}) = \{\emptyset, \{a\}\}$.
- $\mathscr{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.

(A) **2.27.** *Bestimmen Sie $\mathscr{P}(\{1,2,3,4\})$.*

2.3. **Mengen-Algebra.** In diesem Abschnitt wollen wir untersuchen, wie mit den Operatoren $\cap, \cup$ und $\setminus$ gerechnet werden kann. Der folgende Satz entspricht im Wesentlichen Satz 1.18, was nicht wirklich verwunderlich ist, da wir Aussagen über Mengen jederzeit in zusammengesetzte Aussagen übersetzen können.

Satz 2.28. *Seien A, B, C beliebige Mengen. Es gelten folgende Regeln*
(1) *(Kommutativgesetze) $A \cup B = B \cup A$ und $A \cap B = B \cap A$.*
(2) *(Assioziativgesetze) $(A \cup B) \cup C = A \cup (B \cup C)$ und $(A \cap B) \cap C = A \cap (B \cap C)$.*
(3) *(Distributivgesetze)*
   (a) $A \cup (B \cap C) = (A \cup B) \cap (B \cup C)$.
   (b) $A \cap (B \cup C) = (A \cap B) \cup (B \cap C)$.

Beweis: Einen Beweis für die Kommutativität von $\cap$ können Sie im Buch von Klaus Fritzsche, Satz 2.8, finden. Für $\cap$ finden Sie den entsprechenden Beweis in Bemerkung 2.9. Die restlichen Aussagen folgen analog (zu Satz 1.18). □

(A) **2.29.** *Zeigen Sie ii) und iii) aus Satz 2.6.*

Satz 2.30. *Sei G eine fest vorgegebene Grundmenge und $A, B \subseteq G$ Teilmengen. A^{C} bezeichne das Komplement von A in G, also $A^{\mathrm{C}} := G \setminus A$. Dann gelten die* De Morgan'schen Regeln*:*
(a) $(A \cap B)^{\mathrm{C}} = A^{\mathrm{C}} \cup B^{\mathrm{C}}$.

(b) $(A \cup B)^{\mathrm{C}} = A^{\mathrm{C}} \cap B^{\mathrm{C}}$.

Beweis: (a) Es gilt

$$x \in (A \cap B)^{\mathrm{C}} \Leftrightarrow \neg(x \in A \cap B) \Leftrightarrow \neg\Big((x \in A) \wedge (x \in B)\Big) \overset{\text{Satz } 1.18}{\Leftrightarrow} \neg(x \in A) \vee \neg(x \in B)$$
$$\Leftrightarrow x \in A^{\mathrm{C}} \vee x \in B^{\mathrm{C}} \Leftrightarrow x \in A^{\mathrm{C}} \cup B^{\mathrm{C}}.$$

Der Beweis für (b) verläuft analog. □

A **2.31.** *Zeigen Sie Teil (b) von Satz 2.30.*

2.4. **Quantoren.** Wir haben die Quantoren bereits am Ende von Abschnitt 1 eingeführt. Das Problem an dieser Stelle war, dass Mengen noch nicht bekannt waren und streng genommen das Symbol „$\in$“ noch nicht erklärt war.

Definition 2.32. (Existenzquantor)
Sei $A(x)$ eine Aussageform und G eine Menge zulässiger Objekte dafür. Ist die Menge $\{x \in G \mid A(x)\} \neq \emptyset$, dann schreibt man „$\exists x \in G : A(x)$“. Ausformuliert bedeutet das „Es gibt / existiert (mindestens) ein $x \in G$ sodass $A(x)$ wahr ist“. Andernfalls schreibt man „$\nexists x \in G : A(x)$“.

Die Aussage „Es gibt / existiert *genau ein* $x \in G$ sodass $A(x)$ wahr ist“ wird in der Quantorenschreibweise durch ein Ausrufezeichen nach dem Existenzquantor fomuliert: „$\exists! x \in G : A(x)$“.

Beispiel 2.33. Die folgenden Aussagen sind wahr

- $\exists m \in \mathbb{N} : 2$ teilt m.
- $\exists \alpha \in \mathbb{R} : \alpha^2 = 2$.
- $\nexists \alpha \in \mathbb{N} : m^2 = 2$.

A **2.34.** *Versuchen Sie, die Existenzquantoren aus Beispiel 2.33 nachzuweisen bzw. zu widerlegen.*

Definition 2.35. (Allquantor)
Sei $A(x)$ eine Aussageform und G eine Menge zulässiger Objekte dafür. Ist $\{x \in G \mid A(x)\} = G$, dann schreiben wir $\forall x \in G : A(x)$. Ausformuliert bedeutet das: „Für jedes/alle $x \in G$ gilt $A(x)$“.

Beispiel 2.36. Die folgenden Aussagen sind wahr

- $\forall \alpha \in \mathbb{R} : \alpha^2 \geq 0$.
- $\forall m \in \mathbb{N} : 4$ teilt $(2m)^2$.

Bemerkung 2.37. Sei $A(x)$ eine Aussageform und G eine Menge zulässiger Objekte dafür. Die Quantoren $\exists$ und $\forall$ können in mengentheoretische Sprache übersetzt werden:

$$\exists x \in G : A(x) \Leftrightarrow \{x \in G \mid A(x)\} \neq \emptyset \text{ und}$$
$$\forall x \in G : A(x) \Leftrightarrow \{x \in G \mid A(x)\} = G.$$

Ist $B(x)$ eine weitere Aussageform mit zulässigem Objektbereich G, dann gilt beispielsweise

$$\begin{aligned} & \exists x \in G : A(x) \vee B(x) \\ \Leftrightarrow\ & \{x \in G \mid A(x) \vee B(x)\} \neq \emptyset \\ \Leftrightarrow\ & \{x \in G \mid A(x)\} \cup \{x \in G \mid B(x)\} \neq 0 \end{aligned}$$

.

Wir folgern damit: $A \cup B \neq \emptyset \Leftrightarrow ((A \neq \emptyset) \vee (B \neq \emptyset))$, wobei $A := \{x \in G \mid A(x)\}, B := \{x \in G \mid B(x)\}$.

2.5. **Verneinungsregel.** Diese Regeln sind auch in unserem Alltag wichtig.

Satz 2.38. *Sei $A(x)$ eine Aussageform und G eine Menge zulässiger Objekte dafür. Dann gelten*

$$\begin{array}{lrcl} (i) & \neg\Big(\forall x : A(x)\Big) & \Leftrightarrow & \exists x \in G : \neg A(x) \\ (ii) & \neg\Big(\exists x : A(x)\Big) & \Leftrightarrow & \forall x \in G : \neg A(x). \end{array}$$

Beweis: (i) Wir wechseln zum Beweis in die Mengenlehre.

Sei $M = \{x \in G \mid A(x)\}$. Dann entspricht $\forall x \in G : A(x)$ (nach Definition) der Gleichung $M = G$, während $\neg\Big(\forall x \in G : A(x)\Big)$ der Ungleichung $M \neq G$ entspricht. In der Sprache der Mengen ist also (i) äquivalent zu $(M \neq G) \Leftrightarrow (M^{\mathrm{C}} \neq \emptyset)$, und das werden wir verifizieren:

Es ist genau dann $M \neq G$, wenn ein Element $g \in G \setminus M$ existiert, daher ist auf jeden Fall $G \setminus M \neq \emptyset$. Also ist auch $M^{\mathrm{C}} = G \setminus M \neq \emptyset$.

(ii) Man geht analog zu (i) vor. □

A **2.39.** *Beweisen Sie den zweiten Teil von Satz 2.38.*

.

2.6. **Das Kartesische Produkt von Mengen.** Wir definieren das sogenannte *kartesische Produkt* der Mengen A und B als

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

wobei (a, b) ein „geordnetes Paar“ ist. Das heißt, anders als bei der Menge $\{a, b\}$, ist die Reihenfolge von a und b wichtig. Ein einfaches Beispiel für ein kartesisches Produkt ist der $\mathbb{R}^2$, welcher in der Schule oft betrachtet wurde (zweidimensionales Koordinatensystem). Er ist das kartesische Produkt von $\mathbb{R}$ mit sich selbst.

Wie kann man (a, b) mit Hilfe unserer mengentheoretischen Operationen aufschreiben?

$$\begin{array}{rcl} (a, b) : & = & \Big\{\{a\}, \{a, b\}\Big\} \\ & & \in \mathcal{P}(A \cup B). \end{array}$$

Damit gilt natürlich $A \times B \subseteq \mathcal{P}(A \cup B)$.

A **2.40.** *Betrachte die folgenden Beispiele von kartesischen Produkten. Wie viele Elemente sind jeweils im Produkt enthalten? Welche der Mengen sind gleich?*

- $\{1, 2\} \times \{a, b, c\}$,
- $\{2, 3\} \times \{1, 2\}$,
- $\emptyset \times \{1, 2\}$,
- $\{1, 2\} \times \{2, 3\}$.

Bemerkung 2.41. (**Relationen**)
Seien A und B Mengen. Eine *Relation* (zwischen A und B) ist eine Teilmenge R des kartesischen Produktes $A \times B$. Relationen können einige wünschenswerte Eigenschaften haben. So heißt eine Relation mit den Eigenschaften aus Bemerkung 2.14 *Äquivalenzrelation*. Relationen

können auch als Aussageform $R(x, y)$ mit zwei Variablen interpretiert werden. Wir können die Eigenschaften aus Bemerkung 2.14 nun wie folgt allgemein definieren. Dabei gelte $A = B$.

$$\begin{aligned} R \text{ heißt } \textbf{reflexiv} &\Leftrightarrow \forall a \in A : (a, a) \in R. \\ R \text{ heißt } \textbf{symmetrisch} &\Leftrightarrow \forall a, b \in A : (a, b) \in R \Rightarrow (b, a) \in R. \\ R \text{ heißt } \textbf{transitiv} &\Leftrightarrow \forall a, b, c \in A : ((a, b) \in R \wedge (b, c) \in R) \Rightarrow (a, c) \in R. \end{aligned}$$

Beispiel 2.42. Relationen sind tatsächlich bereits in der Schulmathematik weit verbreitet. Daher einige Beispiele

- Sei $A = B = \mathbb{R}$ und R sei gegeben durch „<“. Das heißt als Menge $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid a < b\}$. Diese Relation ist weder reflexiv noch symmetrisch, aber transitiv.
- Sei erneut $A = B = \mathbb{R}$. Dann definiert „=“ eine Äquivalenzrelation auf $\mathbb{R}$.
- Teilbarkeit in $\mathbb{Z}$ in ebenfalls eine Relation. Sie ist reflexiv und transitiv, aber nicht symmetrisch (Warum?). Die Eigenschaften von Teilbarkeit werden Sie später genauer untersuchen (ab Lemma 7.5).
- Teilbarkeit in $\mathbb{R}$ ist eine Relation mit den gleichen Eigenschaften wie zuvor. Nehmen wir allerdings die 0 raus, so erhalten wir hier eine Äquivalenzrelation!
- Jede Abbildung $f \colon A \to B$ ist eine Relation. Mehr dazu in Kapitel 3.

(A) **2.43.** *Seien $A = B = \mathbb{R}$ und $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$. Überlegen Sie, welche der Eigenschaften aus Bemerkung 2.41 von der Relation R erfüllt werden und beweisen Sie Ihre Vermutung.*

Bemerkung 2.44. **(Häufige Fehler)**
Nun kennen Sie sowohl die Sprache der Logik als auch die der Mengen. Achten Sie bitte unbedingt darauf, dass Sie die richtigen Symbole in der richtigen Sprache verwenden! So können z.B. Mengen gleich sein, aber **nicht** äquivalent. Umgekehrt können logische Aussagen äquivalent sein, aber **nicht** gleich. Beziehungen zwischen Mengen sind logische Aussagen und können mit Äquivalenzumformungen (anwenden von Tautologien) umformuliert werden. Expliziter: Sind $A, B \subset G$ Mengen, so ist die Gleichung $A = B$ eine logische Aussage. Sie ist logisch äquivalent zur Aussage $\forall x \in G : x \in A \Leftrightarrow x \in B$, aber nicht gleich.

Ebenso sollten Sie auf die Unterschiede von $\in$ und $\subseteq$ achten. Einfaches Beispiel: Sei A eine Menge, $x \in A$. Dann gelten

- $A \in \mathscr{P}(A)$,
- $\{x\} \subset A$,
- $\{x\} \in \mathscr{P}(A)$,
- $\forall B \in \mathscr{P}(A) : B \subset A$.

2.7. Übungsaufgaben.

Hausaufgabe 2.45. *Seien A und B Mengen. Zeigen Sie*

$$A \subseteq B \iff \mathcal{P}(A) \subseteq \mathcal{P}(B).$$

Hausaufgabe 2.46. *Seien A, B Mengen. Zeigen Sie*

$$A \subseteq B \iff \Big(\forall M \subseteq A : M \cup A \subseteq M \cup B\Big).$$

Hausaufgabe 2.47. *Sei $A = \{1, 2, a, b\}$ und $B = \{2, c, d\}$. Dabei stehen a, b, c, d für die untschiedlichen Buchstaben des Alphabets. Bestimmen Sie die Anzahl der Elemente der Menge*

$$\mathcal{P}\Big((A \setminus B) \cup \{3\}\Big).$$

2.8. **Wiederholungsaufgaben.**
Bearbeiten Sie die folgenden Aussagen analog zu Aussage 2.19, indem Sie beide Beweismethoden durchführen.

Hausaufgabe 2.48. *Seien A, B und C beliebige Mengen. Beweisen Sie die folgenden Aussagen:*

a) *Es gilt $A \setminus B = A$ genau dann, wenn $A \cap B = \emptyset$.*
b) *Es gilt $A \setminus (B \setminus C) = A$ genau dann, wenn $A \cap B \subseteq C$.*

Hausaufgabe 2.49. *Zeigen Sie sowohl mit den Methoden der Mengenlehre als auch mit denen der Aussagenlogik die Aussage $A \cup B = B \cup A$.*

Hausaufgabe 2.50. *Übersetzen Sie die folgende Aussage mit Prädikatenlogik und bestimmen Sie deren Wahrheitswert:*

$$A \cap B \neq \emptyset \Rightarrow (A \neq \emptyset) \wedge (B \neq \emptyset).$$

2.9. **Weiterführende Literatur.**

(1) Fritsche: Mathematik für Einsteiger
(2) Junker

3.1. **Wiederholung.** Lineare und quadratische Funktionen aus der Schule, Proportionalität und die bisherige Abschnitte. Außerdem Addition, Multiplikation und Kürzen von Brüchen als auch Potenzgesetze (diese beinhalten auch Wurzelgesetze).

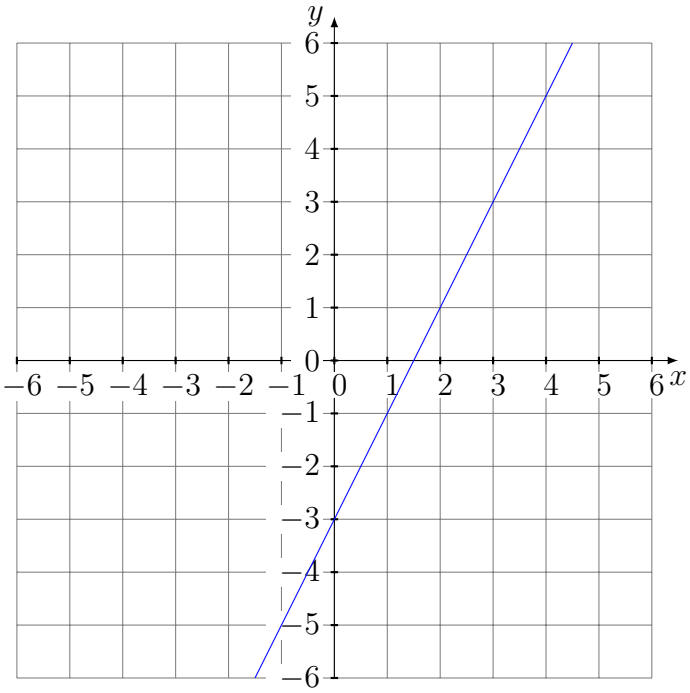
Leitfrage. *Seien $A, B \subseteq \mathbb{R}$ und $f\colon A \to B$ mit Abbildungsvorschrift $x \mapsto x^2$. Ist f eine Abbildung? Wie müssen A und B gewählt werden, damit f injektiv, surjektiv oder gar bijektiv ist?*

3.2. **Die Definition einer Abbildung.** In diesem Abschnitt beschäftigen wir uns mit Abbildungen. Das sind mathematische Objekte, die verschiedene Mengen miteinander verbinden. Mengen zusammen mit deren Abbildungen sind das fundamentale Gerüst der modernen Mathematik.

Wir fangen an mit einer kurzen Wiederholung um zu zeigen, dass es hier um die Verallgemeinerung von bekannten Themen geht. Eine Abbildung besteht aus drei Bestandteilen: *Definitionsbereich, Wertebereich und Abbildungsvorschrift*. In der Schule lernt man verschiedene Formen von Abbildungen kennen, ist aber in der Definition sehr unpräzise. Es wird meistens nur die Abbildungsvorschrift angegeben. Sie werden später sehen, dass Wertebereich und Definitionsbereich wichtig sind um Injektivität oder Surjektivität nachzuweisen. Zunächst einige Beispiele von Funktionen/Abbildungen, die Sie aus der Schule kennen:

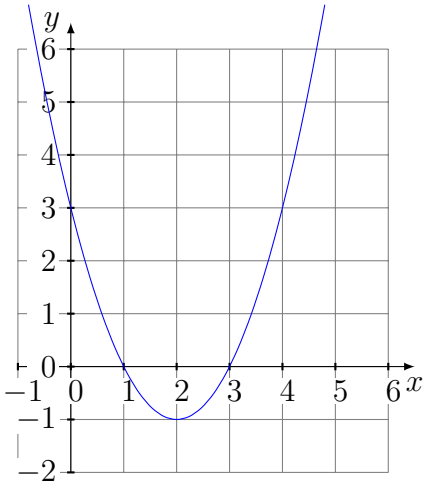
- **Lineare Funktionen** wie z.B. $y = 2x - 3$ $\Big($ oder $f(x) = 2x - 3\Big)$, welche reelle Zahlen zu reellen Zahlen zuordnen. Diese Abbildungen können in einem Koordinatensystem mit zwei Achsen graphisch illustriert werden. Lineare Abbildungen sind durch zwei Punkte der Form $(x_1, f(x_1)), (x_2, f(x_2))$ eindeutig festgelegt.

Graph von $y = 2x - 3$:



- **Quadratische Funktionen** wie z.B. $y = x^2 - 4x + 3$ $\Big($ oder $f(x) = x^2 - 4x + 3\Big)$. Hier werden wieder reelle Zahlen zu reellen Zahlen zugeordnet, wir verwenden dafür die übliche Notation $f\colon \mathbb{R} \to \mathbb{R}$.

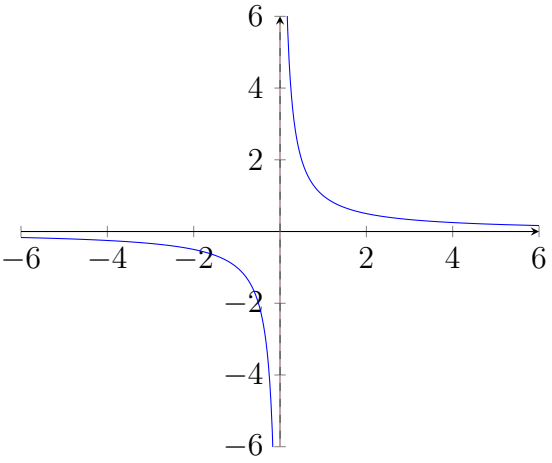
Graph von $y = x^2 - 4x + 3$:



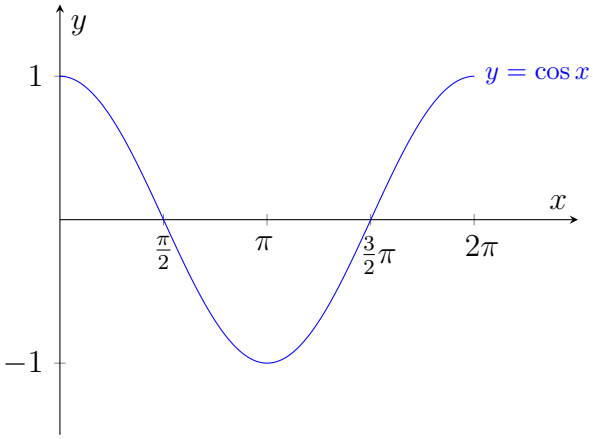
- **Inverse Proportionalität** führt ebenfalls zu einer Funktion, allerdings muss hier der Definitionsbereich angepasst werden.

$f\colon \mathbb{R} \setminus \{0\} \to \mathbb{R} \quad , \quad x \longmapsto \frac{1}{x}$
oder $f(x) := \frac{1}{x}$.

Graph von $y = \frac{1}{x}$:



- **Kosinus-Funktion**: $y = \cos x$ ist auch eine Abbildung von $\mathbb{R}$ nach $\mathbb{R}$, kann aber auch als Funktion $\cos\colon \mathbb{R} \to [-1, 1] := \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ aufgefasst werden.



Unser Ziel ist es, eine gemeinsame, flexible Verallgemeinerung von allen bisherigen Funktionen zu geben. Etwas konkreter, wir möchten den Begriff „Abbildung von einer Menge A in eine Menge B“ zu definieren.

Wiederholung: Seien A, B Mengen. Das kartesische Produkt $A \times B$ ist definiert als

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

wobei (a, b) als *geordnete Paar* oder *Tupel* („zuerst a dann b“) bezeichnet wird. Im Gegensatz zur Menge $\{a, b\}$ zählt hier die Reihenfolge der Elemente.

Das ist aber keine ordentliche Definition, weil wir alles aus Mengen und mathematischen Operationen aufbauen möchten.

Deshalb definieren wir

$$(a, b) := \Big\{\{a\}, \{a, b\}\Big\} \in \mathcal{P}(A \cup B), \text{ und}$$

$$A \times B := \Big\{(a, b) \mid a \in A, b \in B\Big\} \subseteq \mathcal{P}(A \cup B).$$

Wenn $A = \emptyset$ oder $B = \emptyset$ ist, dann *definieren* wir $A \times B := \emptyset$.

Bemerkung 3.1. Da man intuitiv mit Tupeln, also mit der ersten Definition, gut umgehen kann, werden wir die zweite (formal korrekte) Definition in der Praxis nur selten benutzen.

Beispiel 3.2. Das kartesische Produkt $\mathbb{Z} \times \mathbb{Z}$ besteht aus allen Punkten des Koordinatensystems, die auf den „Ecken“ der Kästchen liegen. Deshalb wird es auch Gitter genannt. Die Punkte $(1, 2)$ und $(2, 1)$ sind verschieden!

A **3.3.** *Stellen Sie eine Vermutung auf, wie viele Elemente $A \times B$ hat, falls $|A| = m, |B| = n$ (das heißt, falls A genau m Elemente und B genau n Elemente hat) (erst einmal ohne Beweis). Sie können anschließend Ihre Vermutung überprüfen, indem Sie einen Blick auf Satz 5.12 riskieren.*

$A \times B$ hat wichtige Teilmengen:

$$\begin{aligned} \forall a \in A &: \{a\} \times B \subseteq A \times B \\ \forall b \in B &: A \times \{b\} \subseteq A \times B \end{aligned}$$

und falls $A = B$ gilt, so ist die Menge $\Delta_A := \{(a, a)) \mid a \in A\} \subseteq A \times A$ eine Teilmenge von $A \times B$. Sie heißt *Diagonale* von A.

Definition 3.4. (Abbildung zwischen Mengen)
Seien $A, B \neq \emptyset$ Mengen. Eine *Abbildung* $\mathbf{F}$ *von* $\mathbf{A}$ *nach* $\mathbf{B}$ ist eine Teilmenge $\mathbf{F} \subseteq A \times B$ des kartesischen Produktes von A und B mit folgender Eigenschaft:

$$\forall\, a \in A\ \exists!\, b \in B\ :\ (a, b) \in F.$$

Für eine Abbildung $F \subseteq A \times B$ notiert man $F : A \to B$. Wir nennen die Menge A auch *Definitionsbereich von* $\mathbf{F}$ und B heißt auch *Wertebereich von* $\mathbf{F}$.

Bemerkung 3.5. Wir verwenden für Abbildungen gelegentlich die Bezeichnung Funktion oder Zuordnung.

Bemerkung 3.6. Die in Quantoren beschriebene Eigenschaft einer Funktion aus Definition 3.1 besteht genau genommen aus zwei Teilen. Zum einen muss jedes Element aus dem Definitionsbereich einem Element aus dem Wertebereich zugeordnet werden (jedes Element wird abgebildet). Diese Eigenschaft heißt auch *linkstotal*. Andererseits muss diese Zuordnung eindeutig sein: Es darf kein zweites Element im Wertebereich geben, welches vom selben Element des Definitionsbereichs kommt. Diese Eigenschaft heißt *rechtseindeutig*.

Achtung: Das ist *nicht* die Art und Weise, wie Abbildungen in der Schule (oder oft an der Uni) eingeführt werden, es ist aber die formal korrekte Definition.

A **3.7.** *Welche der folgenden Teilmengen des kartesischen Produktes sind Abbildungen?*

$$\begin{aligned}
\{(x, 2x-3) \mid x \in \mathbb{R}\} &\subseteq \mathbb{R} \times \mathbb{R} \\
\{(x^2, 2x) \mid x \in \mathbb{R}\} &\subseteq \mathbb{R} \times \mathbb{R} \\
\{(2x, \sin x) \mid x \in \mathbb{R}\} &\subseteq \mathbb{R} \times \mathbb{R} \\
\{(x, x^2) \mid x \in \mathbb{R}\} &\subseteq \mathbb{R} \times \mathbb{R}_{>0} \\
\{(x, x^2 - 4x) \mid x \in \mathbb{R}\} &\subseteq \mathbb{R} \times \mathbb{R} \\
\{(x, y) \mid x^2 = y^2\} &\subseteq \mathbb{R} \times \mathbb{R} \\
A \neq \emptyset \text{ beliebig},\ \Delta_A &\subseteq A \times A \\
A, B \neq \emptyset \text{ beliebig}, \{a\} \times B &\subseteq A \times B \\
A \times \{b\} &\subseteq A \times B.
\end{aligned}$$

Definition 3.8. (Halboffiziell, aber in der Praxis benutzt)
Seien $A, B \neq \emptyset$ Mengen. Eine Abbildung $f\colon A \to B$ ist eine Zuordnung mit der Eigenschaft

$$\forall\, a \in A\ \exists!\, b \in B\ :\ f(a) = b.$$

Ausformuliert bedeutet das, dass jedem Element $a \in A$ ein eindeutiger „Wert“ $f(a)$ zugeordnet wird. Es ist somit nicht erlaubt, dass einem Element $a \in A$ verschiedene bzw. mehrere Werte zugewiesen werden. Dies erklärt die Verwendung der Bezeichnung Zuordnung für Abbildungen.

Bemerkung 3.9. Seien $A, B \neq \emptyset$ Mengen. Dann bilden alle Abbildungen von A nach B ebenfalls eine Menge

$$\mathrm{Abb}(A, B) \stackrel{\text{def}}{=} \{f\colon A \to B \mid f \text{ ist eine Abbildung}\}.$$

Gilt $A = B = \mathbb{R}$, so können wir Abbildungen $f, g \in \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ punktweise addieren und multiplizieren

$$(f + g)(x) \stackrel{\text{def}}{=} f(x) + g(x),\ x \in \mathbb{R}$$

$$(f \cdot g)(x) \stackrel{\text{def}}{=} f(x) \cdot g(x),\ x \in \mathbb{R}$$

und mit Zahlen $\alpha \in \mathbb{R}$ multiplizieren

$$(\alpha \cdot f)(x) \stackrel{\text{def}}{=} \alpha \cdot f(x),\ x \in \mathbb{R}$$

und erhalten dabei jeweils wieder eine Funktion. Das heißt, die Menge ist stabil unter diesen Operationen. Zusätzlich gelten Assoziativ-, Kommutativ- und Distributivgesetze. Insgesamt wird $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ damit zu einem sogenannten *Ring*.

Definition 3.10. (Graph einer Abbildung)
Sei $f\colon A \to B$ nach der halboffiziellen Definition gegeben. Daraus lässt sich

$$\Gamma_f := \Big\{\big(a, f(a)\big) \mid a \in A\Big\} \subseteq A \times B,$$

konstruieren. Diese Menge bezeichen wir als *Graph von* f. Dabei entspricht Γ_f gemäß der offiziellen Definition der eigentlichen Abbildung.

Beispiel 3.11. Die Abbildung $f\colon \mathbb{R} \setminus \{0\} \to \mathbb{R}, x \mapsto \frac{1}{x}$ entspricht gemäß Definition der Menge

$$\Gamma_f = \Big\{(x, \frac{1}{x}) \mid x \in \mathbb{R} \setminus \{0\}\Big\} \subseteq (\mathbb{R} \setminus \{0\}) \times \mathbb{R}$$

.

Die Tatsache, dass $\Gamma_f \subseteq A \times B$ eine Abbildung ist (in unserem Sinne), lässt sich graphisch so illustrieren: Jede vertikale Gerade schneidet den Graph Γ_f in **genau einem Punkt**. Gäbe es eine vertikale Gerade, die Δ_f in mehr als einem Punkt schneidet, so würde ein Element $a \in A$ existieren, welches mehr als einem Wert zugeordnet wird.

Bemerkung 3.12. Gemäß Bemerkung 2.41 können wir eine alternative Beschreibung einer Abbildung geben. Seien A und B Mengen. Dann ist eine Abbildung eine linkstotale und rechtseindeutige Relation (zwischen A und B).

Beispiel 3.13. (Identität)
Für $A \neq \emptyset$ beliebig ist $\Delta_A \subseteq A \times A$ eine Abbildung. Diese kann nach Definition 3.8 umformuliert werden zu $f\colon A \to A, a \mapsto a$. In dieser Form nennen wir diese Abbildung *Identität von* A und notieren id_A. Sie macht buchstäblich nichts.

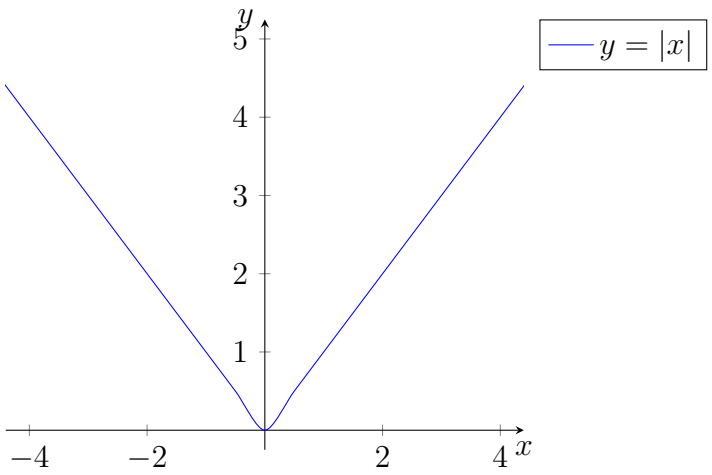
Beispiel 3.14. (Konstante Funktion)
Seien $A, B \neq \emptyset$, $b \in B$. Dann ist $A \times \{b\} \subseteq A \times B$ eine Abbildung. Diese kann als $c_b : A \to B, a \mapsto b$ geschrieben werden.

A **3.15.** *Zeichnen Sie den Graph der konstanten Abbildung* $f\colon \mathbb{R} \to \mathbb{R}, x \mapsto 3$.

Beispiel 3.16. (Betrag)
Sicher kennen Sie den Begriff *Betrag* bereits aus der Schule. Nun können wir den Betrag formal korrekt einführen, nämlich als Abbildung reeller Zahlen:

$$f\colon \mathbb{R} \to \mathbb{R},\ x \mapsto \begin{cases} x, & \text{falls } x \geq 0 \\ -x, & \text{falls } x < 0 \end{cases}.$$

Der Graph dieser Abbildung besteht im ersten Quadrant aus der Identität und im Vierten aus der Spiegelung derselben an der y-Achse:



Hausaufgabe 3.17. *Zeigen Sie mithilfe einer geeigneten Fallunterscheidung, dass der Betrag eine multiplikative Abbildung ist. Das heißt, für $x, y \in \mathbb{R}$ gilt $|x \cdot y| = |x| \cdot |y|$.*

Beispiel 3.18. Eine Folge von rationalen (oder reellen) Zahlen ist eine Abbildung $\mathbb{N} \to \mathbb{Q}$ (oder $\mathbb{N} \to \mathbb{R}$). Wir werden uns damit später genauer beschäftigen (vgl. Definition 10.75).

Definition 3.19. (Einschränkung einer Abbildung)
Es sei $F \subseteq A \times B$ eine Abbildung und $A' \subseteq A$ eine Teilmenge des Definitionsbereiches A von F. Dann definieren wir *die Einschränkung von* $\mathbf{F}$ *auf* $\mathbf{A'}$ als

$$F|_{A'} \stackrel{\text{def}}{=} \{(a, b) \in F \mid a \in A'\} \ .$$

In der üblichen Notation $f \colon A \to B$ schreibt man $f|_{A'} \colon A' \to B$.

Bemerkung 3.20. Es sei A eine Menge, $A' \subseteq A$ eine Teilmenge. Betrachten wir die Identitätsabbildung $\mathrm{id}_A \subseteq A \times A$, so ist die Einschränkung $\mathrm{id}_A|_{A'}$ als eine Teilmenge von $A' \times A$ definiert, und ist formal gesehen nicht gleich $\mathrm{id}_{A'} \subseteq A' \times A'$. Da beide Abbildungen aber das gleiche Bild haben, sprich die Elemente von $A \setminus A'$ werden nicht getroffen, werden sie trotzdem oft nicht unterschieden.

(A) **3.21.** *Betrachte die Abbildung $f \colon \mathbb{Q} \to \mathbb{Q}$ gegeben durch $f(x) = 2x - 3$. Beschreiben Sie die Einschränkungen von f auf $\mathbb{N}$ und $\mathbb{Z}$ und zeichnen Sie den jeweiligen Graph.*

Abbildungen können hilfreiche Eigenschaften besitzen. Diese erkennt man allerdings oft nicht durch bloßes „draufschauen“.

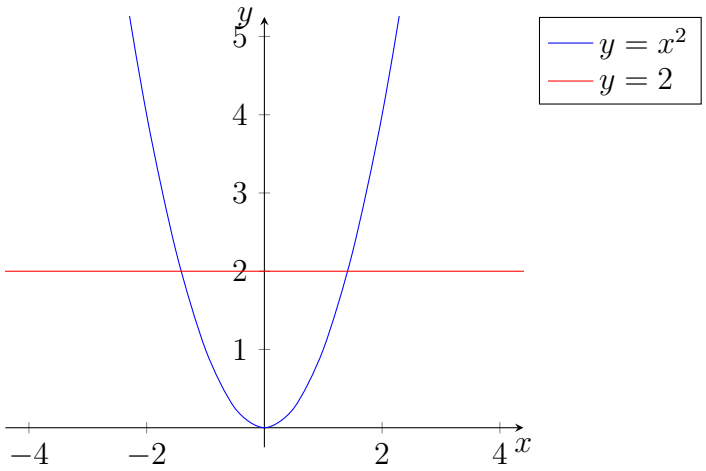
Definition 3.22. Eine Abbildung $f : A \to B$ heißt *injektiv*, falls gilt:

$$\forall\ a_1, a_2 \in A \ : \ f(a_1) = f(a_2) \implies a_1 = a_2.$$

Anschaulich bedeutet das, dass ungleiche Elemente auf ungleiche Elemente abgebildet werden (das ist formal die Kontraposition der obigen Implikation). Alternativ kann man auch sagen, dass jedes Element $b \in B$ höchstens ein Urbild (vgl. Definition 3.58) hat. Das heißt, es gibt höchstens ein $a \in A$ mit $f(a) = b$.

(A) **3.23.** *Formulieren Sie die Kontraposition der Implikation aus Definition 3.22 (als mathematische Aussage).*

Beispiel 3.24. Ein Standardbeispiel für eine Abbildung, die **nicht** injektiv ist, ist die Abbildung $f\colon \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, welche aus der Schule als Normalparabel bekannt ist. Wir wählen z.B. $a_1 = 1$ und $a_2 = -1$. Dann gilt $f(-1) = f(1) = 1$, aber $1 \neq -1$. Damit ist die Implikation aus Definition 3.22 falsch und f kann nicht injektiv sein.



Achtung: Dieses Beispiel zeigt auch sehr anschaulich, weshalb wir für Injektivität dringlichst den Definitionsbereich genau betrachten müssen. Ist dieser nämlich nicht $\mathbb{R}$, sondern $\mathbb{R}_+$, dann ist die Abbildung f durchaus injektiv!

A **3.25.** *Seien A, B beliebige Mengen. Welche von den folgenden Abbildungen ist injektiv? Sollten Sie Probleme mit dem Ansatz haben, so könnte ein Blick auf den Graph der Abbildung hilfreich sein.*

a) $f\colon \mathbb{R} \to \mathbb{R}, f(x) = 3x - 4$.
b) $f\colon \mathbb{R} \to \mathbb{R}, f(x) = x^2 - 2$.
c) $f\colon A \to A, f(x) = \mathrm{id}_A(x)$.
d) $f\colon A \to B, f(x) = c_b$ *für ein* $b \in B$.
e) $f\colon \mathbb{R} \to \mathbb{R}, f(x) = \sin x$.

Bemerkung 3.26. Wie können wir Injektivität für die formale Definition einer Abbildung (als Relation) formulieren? Eine Funktion $f : A \to B$ ist das Gleiche wie $\Gamma_f = \{\big(a, f(a)\big) \mid a \in A\} \subseteq A \times B$. f ist nach Definition injektiv, wenn für jedes $b \in B$ **höchstens** ein $a \in A$ mit $f(a) = b$ existiert.

In anderen Worten: Für jedes Element $b \in B$ besteht der Schnitt $\Gamma_f \cap (A \times \{b\})$ aus höchstens einem Element. Anschaulich heißt das, dass der Graph von f mit jeder horizontalen Gerade (genau das ist nämlich $A \times \{b\}$) höchstens einen Schnittpunkt haben darf. In Beispiel 3.24 kann man gut erkennen, dass dies nicht der Fall ist. Jede positive konstante Abbildung sch

Neben der Injektivität gibt es noch eine weitere Eigenschaft, die wir untersuchen wollen.

Definition 3.27. Eine Abbildung $f\colon A \to B$ heißt *surjektiv*, falls für jedes Element $b \in B$ (mindestens) ein Element $a \in A$ mit $f(a) = b$ existiert. Als Formel:

$$\forall b \in B\ \exists a \in A : f(a) = b.$$

Anschaulich betrachtet bedeutet das, dass jedes Element des Wertebereiches von f „getroffen“ wird.

Beispiel 3.28. Wir betrachten die Abbildung f aus Beispiel 3.16. Da der Graph symmetrisch zur y-Achse ist, sieht man direkt, dass die Betragsfunktion nicht injektiv ist. Da der Betrag stets nicht-negativ ist, folgt ebenso direkt die Surjektivität (keine negative Zahl wird getroffen).

Schließlich gibt es noch einen Begriff für diejenigen Abbildungen, welche beide Eigenschaften zugleich erfüllen.

Definition 3.29. Eine Abbildung $f\colon A \to B$ heißt *bijektiv*, wenn sie sowohl injektiv als auch surjektiv ist.

Beispiel 3.30. Wir betrachten erneut die Normalparabel $f\colon \mathbb{R} \to \mathbb{R}, x \mapsto x^2$. Da Quadrate reeller Zahlen stets nicht-negativ sind, also $x^2 \geq 0$ für alle $x \in \mathbb{R}$, kann f nicht surjektiv sein. Achtung: Das reicht als Beweis nicht aus. Um den Allquantor aus Definition 3.27 zu widerlegen, müssen wir die logische Negation der Aussage zeigen, also einen Existenzquantor nachweisen (wegen 2.38)! Daher nehmen wir z.B. Das Element $-1 \in \mathbb{R}$, welches nicht als $f(x)$ geschrieben werden kann, da sonst $\sqrt{-1} \in \mathbb{R}$ folgen würde.

Auch hier kann durch Manipulation (diesmal des Wertebereiches) die Abbildung surjektiv gemacht werden, indem wir $\mathbb{R}$ ersetzen durch $\mathbb{R}_+$. Insgesamt ist die Normalparabel also als Abbildung von $\mathbb{R}_+ \to \mathbb{R}_+$ sowohl injektiv als auch surjektiv.

A **3.31.** *Welche der Abbildungen aus Aufgabe 3.25 sind surjektiv?*

Bemerkung 3.32. Wir können wie zuvor Surjektivität mit Hilfe von Graphen von Abbildungen beschreiben: $f\colon A \to B$ ist genau dann surjektiv, wenn für jedes $b \in B$

$$\Gamma_f \cap (A \times \{b\}) \neq \emptyset,$$

gilt. Das heißt, der Schnitt besteht aus mindestens einem Element. Anschaulich bedeutet das, dass jede horizontale Gerade vom Graph von f geschnitten wird.

A **3.33.** *Es sei $f\colon \mathbb{R} \to \mathbb{R}$ eine lineare Funktion in der Form $f(x) = ax + b$. Bestimmen Sie die Werte von a und b, falls $f(1) = 1$ und $f(2) = -1$.*

3.3. **Komposition und Invertierbarkeit.** Als nächstes betrachten wir die Komposition von Abbildungen.

Definition 3.34. Es seien $f\colon A \to B$ und $g\colon B \to C$ Abbildungen zwischen Mengen. Wir nennen den Ausdruck

$$g \circ f\colon A \to C, \quad (g \circ f)(a) := g\Big(f(a)\Big)$$

Komposition, Hintereinanderausführung oder Verkettung von f und g.

Lemma 3.35. *Die Komposition $g \circ f\colon A \to C$ von f und g ist eine Abbildung.*

Beweis: Nach Definition des Graphen gilt

$$\Gamma_{g\circ f} := \{(a,c) \in A \times C \mid \exists b \in B \ : \ (a,b) \in \Gamma_f \wedge (b,c) \in \Gamma_g\}$$

Wir müssen also zeigen: $\forall a \in A\ \exists! c \in C : \ (a,c) \in \Gamma_{g\circ f}$. Da f und g Abbildungen sind, gilt $(\forall a \in A\ \exists! b \in B : \ (a,b) \in \Gamma_f) \ \wedge \ (\forall b \in B\ \exists! c \in C : \ (b,c) \in \Gamma_g)$. Das impliziert $\forall a\ \exists! c : \ (a,b) \in \Gamma_f \wedge (b,c) \in \Gamma_g$. Es ist nämlich c eindeutig bestimmt durch b, welches eindeutig bestimmt ist durch a. □

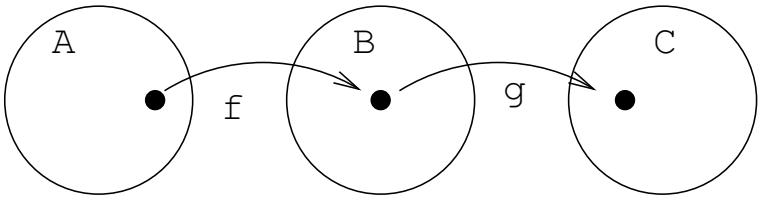
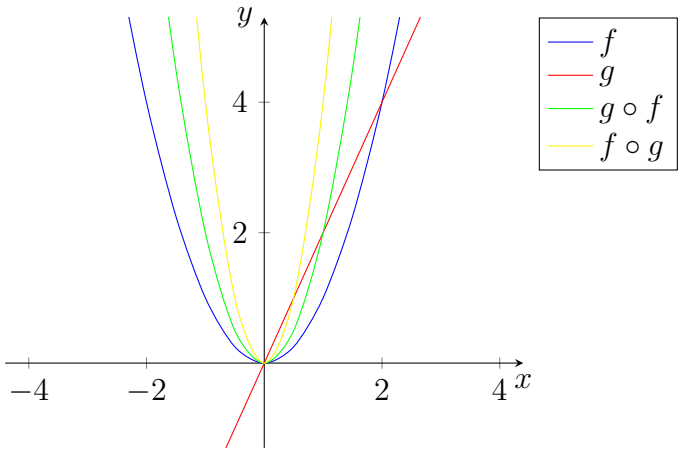


ABBILDUNG 1. Die Verkettung der Abbildungen f und g

Beispiel 3.36. Seien $f, g\colon \mathbb{R} \to \mathbb{R}$ gegeben durch $f(x) = x^2$ und $g(x) = 2x$. Dann ist $(g \circ f)(x) = g(x^2) = 2x^2$ und $(f \circ g)(x) = f(2x) = 4x^2$. Dieses Beispiel zeigt bereits, dass die Verkettung nicht kommutativ ist!



A **3.37.** *Seien $f, g\colon \mathbb{R} \to \mathbb{R}$ gegeben durch $f(x) = x + 1$ und $g(x) = x^2$. Bestimmen Sie $f \circ g$ und $g \circ f$.*

Bemerkung 3.38. Die Verkettung $g \circ f$ ist nur definiert, wenn $f : A \to B$ und $g : B \to C$ ist. Das heißt genauer, dass der Wertebereich von f mit dem Definitionsbereich von g übereinstimmen muss. Ist nämlich zum Beispiel $f\colon \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ und $g\colon \mathbb{R} \setminus \{0\} \to \mathbb{R},\ x \mapsto \frac{1}{x}$, so sind f und g in der Reihenfolge $g \circ f$ **nicht** komponierbar. $f \circ g$ ist aber wolhdefiniert.

A **3.39.** *Zeigen Sie, dass $g \circ f$ in Bemerkung 3.38 nicht wohldefiniert ist.*

A **3.40.** *Betrachten Sie die Abbildungen $f, g\colon \mathbb{R} \to \mathbb{R}, f(x) = 2x - 1$ und $g(x) = \frac{x+1}{2}$. In welcher Reihenfolge sind f und g komponierbar? Was ist die Komposition, falls Sie definiert ist?*

Unter gewissen Umständen ist es möglich Abbildungen umzukehren. Anschaulich bedeutet das, dass wir z.B. den Pfeil, der zu f in Abbildung 1 gehört, umdrehen können.

Definition 3.41. Eine Abbildung $f\colon A \to B$ heißt *invertierbar*, falls eine Abbildung $g\colon B \to A$ existiert, sodass $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$ gelten. In diesem Fall nennen wir g die *Umkehrabbildung* von f.

Beispiel 3.42. Betrachten Sie erneut die Abbildungen $f, g : \mathbb{R} \to \mathbb{R}, f(x) = 2x - 1, g(x) = \frac{x+1}{2}$. f ist eine lineare Abbildung, also insbesondere bijektiv (vgl. Aufgabe 3.86). Die Umkehrabbildung ist genau g.

Satz 3.43. *Eine Abbildung $f\colon A \to B$ ist genau dann invertierbar, wenn sie bijektiv ist.*

Wir werden den Satz in der folgenden stärkeren Form beweisen.

Satz 3.44. *Es sei $f\colon A \to B$ eine Abbildung.*

(a) *f ist injektiv $\iff$ $\exists g\colon B \to A$ mit $g \circ f = \mathrm{id}_A$.*
(b) *f ist surjektiv $\iff$ $\exists g\colon B \to A$ mit $f \circ g = \mathrm{id}_B$.*

Beweis: Wir beweisen beide Äquivalenzen, indem wir jeweils beide Implikationen zeigen.

(a) „$\Rightarrow$“ Wir nehmen an, dass f injektiv ist. Sei ferner $a_0 \in A$ beliebig. Wir setzen

$$g(b) := \begin{cases} a_0 & , \text{ falls } b \notin \text{Bild } (f) \\ a & , \text{ falls } b \in \text{Bild } (f) \text{ mit } f(a) = b. \end{cases}$$

Da f injektiv ist, existiert für jedes $b \in$ Bild (f) (vergleiche Definition 3.48) nur genau ein eindeutiges $a \in A$ mit $f(a) = b$. Also ist $g(b)$ eindeutig bestimmt. Damit ist $g\colon B \to A$ eine wohldefinierte Abbildung. Für $a \in A$ gilt nach Definition der Verkettung:

$$(g \circ f)(a) = g\Big(f(a)\Big) \overset{\text{Def. von } g}{=} a = \mathrm{id}_A(a).$$

„$\Leftarrow$“ Sei f eine beliebige Abbildung und $g\colon B \to A$ eine Abbildung mit der Eigenschaft $g \circ f = \mathrm{id}_A$. Wir machen einen sogenannten Widerspruchsbeweis: Wir nehmen an, dass die Aussage „f ist injektiv“ falsch ist, und zeigen davon ausgehend, dass dann die Aussage „$g \circ f = \mathrm{id}_A$“ ebenfalls falsch ist (logischer Hintergrund: Aufgabe 1.23). Sei also f **nicht** injektiv. Dann existieren $a_1, a_2 \in A$ mit $a_1 \neq a_2$ und $f(a_1) = f(a_2)$. Es folgt

$$\begin{aligned} a_1 = \mathrm{id}_A(a_1) = (g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) \\ = (g \circ f)(a_2) = \mathrm{id}_A(a_2) = a_2, \end{aligned}$$

was der Annahme $a_1 \neq a_2$ widerspricht. Somit ist Teil (a) bewiesen.

(b) „$\Rightarrow$“ Sei f surjektiv, dann gilt: $\forall b \in B\ \exists a \in A:\ f(a) = b$. Setze also $g(b) := a$ für ein solches Urbild a von b unter f. Dann ist $g\colon B \to A$ nach Konstruktion eine Abbildung. Nachrechnen liefert

$$(f \circ g)(b) = f\Big(g(b)\Big) = f(a) = b = \mathrm{id}_B(b).$$

„$\Leftarrow$“ Widerspruchsbeweis: Sei f nicht surjektiv. Dann existiert ein $b \in B$ mit $b \notin$ Bild (f). Damit gilt, unabhängig davon, wie g abbildet:

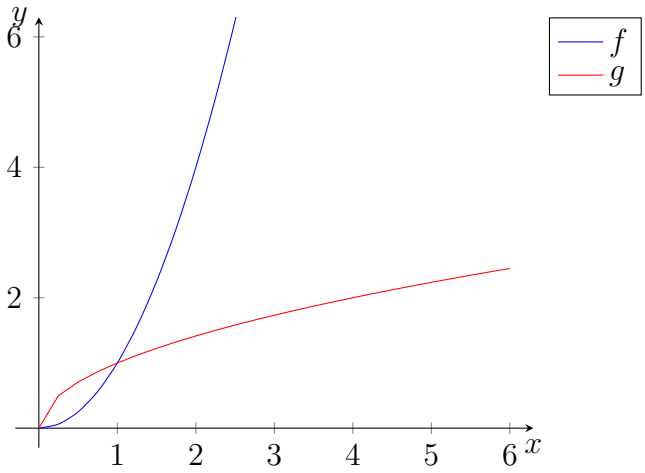
$$(f \circ g)(B) = f\Big(g(B)\Big) \subseteq f(A) = \text{Bild } (f) \not\ni b,$$

insbesondere $f \circ g \neq \mathrm{id}_B$.

□

Bemerkung 3.45. In der Situation von Satz 3.44 nennt man g auch linksinvers btw. rechtsinvers zu f.

Beispiel 3.46. Wir haben in diesem Abschnitt die Normalparabel genau untersucht. Wir wissen bereits, dass $f\colon \mathbb{R}_+ \to \mathbb{R}_+, x \mapsto x^2$ bijektiv ist. Nach Satz 3.43 muss also eine Umkehrabbildung $g\colon \mathbb{R}_+ \to \mathbb{R}_+$ existieren. Diese ist aus der Schule wohlbekannt: Es handelt sich um die Wurzelfunktion $g(x) = \sqrt{x}$. Die Quadratwurzel ist nur für nicht-negative reelle Zahlen definiert. Das ist genau der Grund, warum f auf $\mathbb{R}_{<0}$ keine Umkehrfunktion hat.



(A) **3.47.** *Gegeben seien die Abbildungen $f, g\colon \mathbb{R}_+ \to \mathbb{R}$ mit Abbildungsvorschrift $f(x) = \sqrt{x}$ bzw. $g(x) = ln(x)$. Entscheiden Sie, ob diese Abbildungen injektiv oder surjektiv sind und geben Sie das Links- bzw. Rechtsinverse an. Betrachten Sie nun die Funktion $h\colon \mathbb{R} \to \mathbb{R}, x \mapsto x^3 - 6x^2 + 4x + 12$ und untersuchen Sie diese analog zu f und g.*

3.4. **Bilder und Urbilder.**

Definition 3.48. [Bild einer Abbildung]
Es sei $f\colon A \to B$ eine Abbildung zwischen Mengen, und $X \subseteq A$ eine Teilmenge. Wir setzen

$$f(X) \stackrel{\text{def}}{=} \{f(a) \mid a \in X\} = \{b \in B \mid \text{ Es gibt ein } a \in X \text{ mit } f(a) = b\}$$

und und nennen $f(X)$ das *Bild von* X. Das Bild der Abbildung f ist $f(A)$.

(A) **3.49.** *Zeigen Sie, dass eine Abbildung $f\colon A \to B$ genau dann surjektiv ist, wenn*

$$f(A) = B$$

gilt.

Beispiel 3.50. Es sei A eine nicht-leere Menge und $\mathrm{id}_A\colon A \to A$. Dann ist das Bild von id_A gleich A.

Beispiel 3.51. Es seien A, B Mengen, $b_0 \in B$ ein beliebiges Element. Man betrachte die konstante Abbildung $c_{b_0}\colon A \to B$. Dann ist das Bild von c_{b_0} gleich $\{b_0\}$.

Beispiel 3.52. Sei $f\colon \mathbb{Z} \to \mathbb{Z}$ gegeben durch $x \mapsto x^2$ und $X = \{-3, -1, 2, 3, 4\}$. Dann das das Bild von X genau die Menge $f(X) = \{1, 4, 9, 16\}$.

(A) **3.53.** *Betrachte die Abbildung $f\colon \mathbb{Z} \to \mathbb{Z}$, $m \to m^2 - 2$. Berechnen Sie das Bild der Mengen $\{-5, -2, 1, 2, 5\}$ und $X := \{m^2 \mid m \in \mathbb{Z}\}$.*

Bemerkung 3.54. Es sei $f\colon A \to B$ eine Abbildung. Dann ergibt sich aus f eine natürliche surjektive Abbildung $A \to f(A)$, die wir ebenfalls mit f bezeichnen.

Lemma 3.55. *Es sei $f\colon A \to B$ eine Abbildung, $X \subseteq Y \subseteq A$ Teilmengen. Dann gilt*

$$f(X) \subseteq f(Y)\ .$$

Beweis: Sei $b \in f(X)$. Dann existiert ein $a \in X$ mit $f(a) = b$. Wegen $X \subseteq Y$ gilt sofort $a \in Y$ also $b = f(a) \in f(Y)$. Insgesamt ist somit

$$f(X) \;=\; \{f(a) \mid a \in X\} \subseteq \{f(a) \mid a \in Y\} \;=\; f(Y)\ .$$

□

Im Folgenden betrachten wir die Beziehung zwischen Bildern von Mengen und mengentheoretischen Operationen.

Lemma 3.56. *Es sei $f\colon A \to B$ eine Abbildung, $X, Y \subseteq A$. Dann gelten*

$$\begin{aligned} f(X \cap Y) &\subseteq f(X) \cap f(Y) \\ f(X \cup Y) &= f(X) \cup f(Y)\ . \end{aligned}$$

Beweis: Zunächst behandeln wir die erste Aussage („Das Bild des Schnittes ist enthalten im Schnitt der Bilder“). Bekannterweise gilt $X \cap Y \subseteq X, Y$ und somit

$$f(X \cap Y) \subseteq f(X)\,,\, f(Y)\ .$$

Dann ist aber $f(X \cap Y) \subseteq f(X) \cap f(Y)$, was zu zeigen war.

Als nächstes beschäftigen wir uns mit der Vereinigung(„Das Bild der Vereinigung ist die Vereinigung der Bilder“). Wie vorher folgt aus $X, Y \subseteq X \cup Y$

$$f(X)\,,\, f(Y) \subseteq f(X \cup Y)\ ,$$

dementsprechend $f(X) \cup f(Y) \subseteq f(X \cup Y)$.

Für die andere Inklusion sei $b \in f(X \cup Y)$ ein beliebiges Element. Nach der Definition des Bildes von $X \cup Y$ existiert ein Element $a \in X \cup Y$, so dass $f(a) = b$. Dann ist aber entweder $a \in X$ und daher $b = f(a) \in f(X)$ oder $a \in Y$ und $b = f(a) \in f(Y)$.

Es folgt, dass jedes $b \in f(X \cup Y)$ entweder in $f(X)$ oder in $f(Y)$ enthalten ist, daher $b \in f(X) \cup f(Y)$ und schließlich $f(X \cup Y) \subseteq f(X) \cup f(Y)$. □

Bemerkung 3.57 (Bild und Schnitt). Man sollte im Kopf behalten, dass im Allgemeinen $f(X \cap Y) \neq f(X) \cap f(Y)$ gilt. Hier ist ein konkretes Beispiel: Betrachte die Abbildung $f\colon \mathbb{Z} \to \mathbb{Z}$, die eine ganze Zahl m auf ihren Betrag $|m|$ abbildet. Es seien jetzt $X = \mathbb{N} = \{m \in \mathbb{Z} \mid m \geq 0\}$ und $Y = -\mathbb{N} = \{m \in \mathbb{Z} \mid m \leq 0\}$. Dann gilt $X \cap Y = \{0\}$.

Mit diesen Wahlen haben wir

$$\begin{aligned} f(X) &= X = \mathbb{N}\ , \\ f(Y) &= X = \mathbb{N}\ . \end{aligned}$$

Insbesondere ist $f(X \cap Y) = \{0\}$ und $f(X) \cap f(Y) = \mathbb{N}$. Die hier gewählte Abbildung f ist nicht injektiv, was der tiefere Grund dafür ist, dass der Schnitt der Bilder nicht im Bild der Schnitte enthalten ist.

Definition 3.58. [Urbild einer Teilmenge unter einer Abbildung]
Es sei $f\colon A \to B$ eine Abbildung, $Y \subseteq B$ eine Teilmenge. Das *Urbild von Y unter f* definieren wir als

$$f^{-1}(Y) \stackrel{\text{def}}{=} \{a \in A \mid f(a) \in Y\}\ .$$

Beispiel 3.59. Man betrachte wieder die Identitätsabbildung $\mathrm{id}_A\colon A \to A$ einer Menge A und wähle eine beliebige Teilmenge $Y \subseteq A$. Dann ist

$$f^{-1}(Y) \;=\; Y\ .$$

Beispiel 3.60. Es seien A und B nicht-leere Mengen, $f\colon A \to B$ und $b_0 \in B$ beliebig. Für eine Teilmenge $Y \subseteq B$ gilt

$$f^{-1}(Y) = \begin{cases} A & \text{falls } b_0 \in Y \ , \\ \emptyset & \text{falls } b_0 \notin Y \ . \end{cases}$$

Beispiel 3.61. Sei $f\colon \mathbb{Z} \to \mathbb{Z}$ gegeben durch $x \mapsto x^2$ und $Y = \{-3, -1, 2, 3, 4\}$. Dann das das Urbild von Y genau die Menge $f^{-1}(Y) = \{2\}$.

Bemerkung 3.62. Für eine beliebige Abbildung $f\colon A \to B$ gilt wegen der Linkstotalität von Abbildungen stets $f^{-1}(B) = A$.

(A) **3.63.** *Gegeben sei die Abbildung $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = 3x - 1$. Bestimmen Sie $f^{-1}(-3/2)$ und $f^{-1}(\mathbb{R}_{\geq 2})$.*

(A) **3.64.** *Man betrachte die Abbildung $f\colon \mathbb{Z} \to \mathbb{Z}$, $f(m) = |m|$. Bestimmen Sie die Urbilder der folgenden Teilmengen: $\mathbb{N}$, $\{$gerade ganze Zahlen$\}$, $\{0\}$.*

Lemma 3.65. *Es sei $f\colon A \to B$ eine Abbildung, $X \subseteq Y \subseteq B$ Teilmengen. Dann gilt*

$$f^{-1}(X) \subseteq f^{-1}(Y) \ .$$

Beweis: Es gilt

$$f^{-1}(X) = \{a \in A \mid f(a) \in X\} \subseteq \{a \in A \mid f(a) \in Y\} = f^{-1}(Y) \ .$$

□

Lemma 3.66. *Es sei $f\colon A \to B$ eine Abbildung, $X, Y \subseteq B$ beliebige Teilmengen. Dann ist*

$$\begin{aligned} f^{-1}(X \cap Y) &= f^{-1}(X) \cap f^{-1}(Y) \ , \\ f^{-1}(X \cup Y) &= f^{-1}(X) \cup f^{-1}(Y) \ . \end{aligned}$$

Beweis: Der Beweis dieser Aussagen wird als Übungsaufgabe gestellt. □

Proposition 3.67 (Wechselwirkungen zwischen Bild und Urbild)**.**
Es sei $f\colon A \to B$ eine Abbildung, $X \subseteq A$ und $Y \subseteq B$ Teilmengen. Dann gelten

(1) $X \subseteq f^{-1}(f(X))$,
(2) $f(f^{-1}(Y)) = Y \cap f(A)$.

Beweis:

(1) Die erste Aussage folgt sofort aus der Definition, da $f(a) \in f(X)$ für beliebiges $a \in X$ und $f^{-1}(f(X)) = \{a \in A \mid f(a) \in f(X)\}$.
(2) Die zweite Aussage zeigen wir mit Mengenumformungen:

$$\begin{aligned} f(f^{-1}(Y)) &= \{f(x) \mid x \in f^{-1}(Y)\} \\ &= \{f(x) \mid x \in A \wedge f(x) \in Y\} \\ &= \{b \in Y \mid \exists x \in A : f(x) = b\} \\ &= Y \cap f(A). \end{aligned}$$

□

Bemerkung 3.68. Es sei $f\colon A \to B$ eine Abbildung. Für einelementige Teilmengen von B benutzen wir eine verkürzte Notation: Sei $b \in B$. Statt $f^{-1}(\{b\})$ notieren wir oft nur $f^{-1}(b)$.

Proposition 3.69. *Es sei $f\colon A \to B$. Es gelten die folgenden Äquivalenzen.*

(1) *f ist genau dann injektiv, wenn für alle $b \in B$ die Menge $f^{-1}(b)$ aus höchstens einem Element besteht.*
(2) *f ist genau dann surjektiv, wenn für alle $b \in B$ die Menge $f^{-1}(b)$ aus mindestens einem Element besteht.*
(3) *f ist genau dann bijektiv, wenn für alle $b \in B$ die Menge $f^{-1}(b)$ aus genau einem Element besteht.*

Beweis:

(1) „$\Rightarrow$“ Sei zunächst f injektiv und $x \in f^{-1}(b)$ ein Urbild eines beliebigen Elements $b \in B$. Angenommen, es existiert ein weiteres Urbild $y \in f^{-1}(b)$ mit $x \neq y$. Dann gilt $f(x) = b = f(y)$ und die Injektivität von f impliziert sofort $x = y$. Ein Widerspruch. „$\Leftarrow$“ Sei umgekehrt $f^{-1}(b) = \{x\}$ für ein $x \in A$. Sei nun ein Element $y \in A$ gegeben mit $f(x) = f(y)$. Wir müssen zeigen, dass dann $x = y$ sein muss. Doch das folgt sofort aus $f(y) = b$, denn somit ist y ein Urbild von b, es gibt aber nur genau eines, nämlich x. Also müssen diese gleich sein.
(2) Übungsaufgabe.
(3) Folgt sofort aus i) und ii).

□

A **3.70.** *Beweisen Sie Teil (2) von Proposition 3.69.*

3.5. **Analyse quadratischer Funktionen.** In diesem Abschnitt werden wir quadratische Funktionen, welche bereits aus der Schule bekannt sind, mathematisch untersuchen.

Definition 3.71. Eine *quadratische Funktion* ist eine Abbildung $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = ax^2 + bx + c$, wobei a, b, c reelle Zahlen sind und $a \neq 0$ ist.

Bemerkung 3.72. Das wichtigste Werkzeug, wenn man mit quadratischen Funktionen arbeitet, ist die Lösungsformel, womit man die Nullstellen $f(x) = 0$ (das heißt, das Urbild von $\{0\}$ bezüglich der Abbildung $x \mapsto ax^2 + bx + c$) bestimmt. Die Formel lautet

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} .$$

In dieser Form wird die Formel oft *Mitternachtsformel* oder *abc-Formel* genannt.

A **3.73.** *Leiten Sie die obige Lösungsformel aus der p-q-Formel her.*

Die mengentheoretischen Eigenschaften von quadratischen Abbildungen lassen sich mithilfe von quadratischer Ergänzung (die gleiche Idee, die zur Lösungsformel führt) bestimmen. Man betrachte die folgende Rechnung:

$$ax^2 + bx + c = a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) = a\left(\left(x + \frac{b}{2a}\right)^2 + \left(\frac{c}{a} - \frac{b^2}{4a^2}\right)\right) .$$

A **3.74.** *Führe quadratische Ergänzung in den folgenden konkreten Fällen aus: $x^2 - x - 1$, $2x^2 + 5x - 3$, $-7x^2 - 9x + 2$, $2x^2 + (m-2)x - 1$ (in Abhängigkeit vom Parameter m).*

Satz 3.75 (Mengentheoretische Eigenschaften quadratischer Funktionen)**.**
Es sei $f(x) = ax^2 + bx + c$, $f\colon \mathbb{R} \to \mathbb{R}$ eine quadratische Funktion (insbesondere $a \neq 0$).

(1) *Das Bild von f ist $f(\mathbb{R}) = \left[c - \frac{b^2}{4a},\ +\infty\right)$ bzw. $f(\mathbb{R}) = \left(-\infty,\ c - \frac{b^2}{4a}\right)$.*
(2) *f ist weder surjektiv noch injektiv.*
(3) *$f|_{[-b/2a,+\infty)}\colon \left[-\frac{b}{2a}, +\infty\right) \to \left[c - \frac{b^2}{4a}, +\infty\right)$ ist bijektiv (hier gelte ohne Einschränkung $a > 0$).*
(4) *Der Graph der Funktion f ist eine Parabel mit Scheitelpunkt $\left(-\frac{b}{2a},\ c - \frac{b^2}{4a}\right)$.*

Bemerkung 3.76. Unter einer Parabel verstehen wir eine lineare Transformation der Normalparabel. Das heißt eine Parabel ist eine verschobene und/oder gestreckte bzw. gestauchte Normalparabel.

Beweis:

(1) Wir müssen zeigen, dass die reelle Zahl $c - \frac{b^2}{4a}$ die kleinste bzw. größte Zahl ist, welche im Bild von f liegen kann. Dies hängt davon ab, ob $a < 0$ oder $a > 0$ gilt. Nach obiger Diskussion wissen wir, dass wir f darstellen können wie folgt:

$$f(x) \;=\; a\left(\left(x + \frac{b}{2a}\right)^2 + \left(\frac{c}{a} - \frac{b^2}{4a^2}\right)\right).$$

Wir wissen, dass Quadrate immer positiv sind, daher wird der Ausdruck $f(x)$ minimal bzw. maximal, wenn $x = -\frac{b}{2a}$ ist. Doch dann ist der y-Wert genau $c - \frac{b^2}{4a}$.

Das Ganze lässt sich auch mit Schulmathematik lösen, indem wir eine simple Kurvendiskussion durchführen. Dazu benötigen wir die Ableitungen:

$$\begin{aligned} f(x) &= ax^2 + bx + c \\ f'(x) &= 2ax + b \\ f''(x) &= 2a \end{aligned}$$

Dann berechnen wir die Nullstelle der ersten Ableitung:

$$\begin{aligned} f'(x) &= 0 \\ \Leftrightarrow 2ax + b &= 0 \\ \Leftrightarrow x &= -\frac{b}{2a} \end{aligned}$$

Somit haben wir ein Extremum bei $x = -\frac{b}{2a}$, $y = f(-\frac{b}{2a}) = c - \frac{b^2}{4a}$. In Abhängigkeit von a ist dies nun ein Minimum oder ein Maximum und es folgt die Behauptung.

(2) f ist nicht surjektiv: Ist $a > 0$, so ist $c - \frac{b^2}{4a}$ das Minimum, also liegt z.B. $c - \frac{b^2}{4a} - 1$ nicht im Bild. Für $a < 0$ folgt die Behauptung z.B. mit $c - \frac{b^2}{4a} + 1$.

f ist nicht injektiv: Wir benutzen erneut die Darstellung von f aus i). Dann wählen wir z.B. $x_1 = \frac{b}{2a}$ und $x_2 = -\frac{3b}{2a}$ und erhalten $(x_1 + \frac{b}{2a})^2 = (x_2 + \frac{b}{2a})^2$. Da die übrigen Ausdrücke nicht von x abhängen, haben wir klar $f(x_1) = f(x_2)$ aber $x_1 \neq x_2$.

(3) Wir nutzen erneut die Darstellung

$$f(x) = a\left(\left(x+\frac{b}{2a}\right)^2 + \left(\frac{c}{a} - \frac{b^2}{4a^2}\right)\right).$$

Wie zuvor ist der Wert von $f(x)$ bestimmt durch $\left(x+\frac{b}{2a}\right)^2$, da der restliche Term von x nicht abhängt. Man sieht leicht die Symmetrie

$$\left(x+\frac{b}{2a}\right)^2 = \left(-x-\frac{b}{2a}\right)^2$$

wodurch wir schließen können, dass $f(x) = f(-x-\frac{b}{a})$. Sei nun $x \in \left[-\frac{b}{2a}, +\infty\right)$. Dann ist $-x-\frac{b}{a} \in \left(-\infty, -\frac{b}{2a}\right]$. Es folgt mit i)

$$f(\left[-\frac{b}{2a}, +\infty\right)) = f(\left(-\infty, -\frac{b}{2a}\right]) = f(\mathbf{R}) = \left[c-\frac{b^2}{4a},\ \pm\infty\right)$$

und f ist surjektiv. Sind $x, y \in \left[-\frac{b}{2a}, +\infty\right)$ mit $f(x) = f(y)$, so folgt $(x+\frac{b}{2a})^2 = (y+\frac{b}{2a})^2$, also $x+\frac{b}{2a} = \pm(y+\frac{b}{2a})$. Doch dann gilt entweder $x = y$ oder $x = -y-\frac{b}{a}$. Der zweite Fall ist nicht möglich, da $x \notin \left(-\frac{b}{2a}, +\infty\right)$ folgt. Somit gilt $x = y$ und f ist injektiv.

(4) Wir haben gesehen, dass der Punkt $\left(-\frac{b}{2a},\ c-\frac{b^2}{4a}\right)$ das einzige globale Extremum ist. Außerdem haben wir wegen $f(x) = f(-x-\frac{b}{a})$ gesehen, dass f symmetrisch ist zur (verschobenen y-) Achse $x = -\frac{b}{2a}$. Somit ist der Graph von f eine verschobene Normalparabel mit Scheitelpunkt $\left(-\frac{b}{2a},\ c-\frac{b^2}{4a}\right)$, welche um den Faktor a gestreckt bzw. gestaucht ist.

□

3.6. Übungsufgaben.

Hausaufgabe 3.77. *Entscheiden Sie, welche der folgenden Teilmengen Abbildungen darstellen:*

(1) $\Delta_{\mathbb{R}} \subseteq \mathbb{R} \times \mathbb{R}$
(2) $\{1\} \times \mathbb{N} \subseteq \mathbb{N} \times \mathbb{N}$
(3) $\mathbb{N} \times \{-1\} \subseteq \mathbb{N} \times \mathbb{N}$
(4) $\mathbb{N} \times \{-1\} \subseteq \mathbb{Z} \times \mathbb{Z}$
(5) $\{(\sin\ x, \cos\ x) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$.

Hausaufgabe 3.78. *Seien $f\colon A \to B$ und $g\colon B \to C$ Abbildungen. Zeigen Sie: Sind f und g injektiv, so ist auch $g \circ f$ injektiv.*

Hausaufgabe 3.79. *In der Situation von Lemma 3.56, zeigen Sie: Ist f injektiv, so gilt*

$$f(X) \cap f(Y) = f(X \cap Y).$$

Hausaufgabe 3.80. *Sei $f\colon A \to B$ eine Abbildung. Man beweise, dass $f(A)$ die kleinste Teilmenge (bezüglich Inklusion) von B ist, für welche $f^{-1}(f(A)) = A$ gilt. Nehmen Sie dazu eine beliebige Teilmenge $M \subseteq B$ mit der Eigenschaft $f^{-1}(M) = A$ und folgern Sie, dass M dann bereits $f(A)$ enthalten muss.*

Hausaufgabe 3.81. *Beweisen Sie Lemma 3.66.*

Hausaufgabe 3.82. *Es seien $\alpha, \beta \in \mathbb{R}$ und die Abbildung $f\colon \mathbb{R} \to \mathbb{R}$*

$$f(x) = \alpha x + \beta$$

gegeben. Sei $y_0 \in \mathbb{R}$. Aus wie vielen Elementen besteht das Urbild $f^{-1}(y_0) \subseteq \mathbb{R}$?

Hausaufgabe 3.83. *Wir betrachten die Abbildung $f\colon \mathbb{R} \to \mathbb{R}$, die $x \in \mathbb{R}$ die Zahl $2x^2 - 3x + 1$ zuordnet. Bestimmen Sie die Menge $f^{-1}(2)$. Für welche reelle Zahlen $\alpha \in \mathbb{R}$ besteht das Urbild $f^{-1}(\alpha)$ aus einem Element? Wann aus zwei Elementen? Wann ist $f^{-1}(\alpha)$ leer?*

Hausaufgabe 3.84. *Bestimmen Sie die Nullstellen des quadratischen Polynoms $(m-2)x^2 + (2m+3)x - 2$ in Abhängigkeit von m. Für welche Werte von m gibt es 0,1, 2, oder unendlich viele Lösungen?*

3.7. **Wiederholungsaufgaben.**

Hausaufgabe 3.85. *Bestimmen Sie die größte Teilmenge $M \subseteq \mathbb{R}$, für die die Menge*

$$F := \{(x, \frac{1}{x-1} - \frac{1}{x+1}) \mid x \in M\} \subseteq M \times \mathbb{R}$$

eine Abbildung ist. Ist F injektiv?

Hausaufgabe 3.86 (Analyse linearer Funktionen)**.** *Es seien $a, b \in \mathbb{R}$ und $f\colon \mathbb{R} \to \mathbb{R}$ eine lineare Abbildung, gegeben durch $f(x) = ax + b$. Für welche Werte von a und b ist f injektiv/surjektiv/bijektiv?*

Hausaufgabe 3.87. *Für welche Werte von $a, b \in \mathbb{R}$ ist die Abbildung*

$$f\colon \mathbb{R} \to \mathbb{R},\ x \mapsto \frac{1}{ax+b}$$

injektiv, surjektiv oder bijektiv?

Hausaufgabe 3.88. *Für $a \in \mathbb{R}$ sei die Abbildung*

$$f\colon [a, \infty) \to [1, \infty), \quad f(x) = x^2 - 2x + 2$$

gegeben. Bestimmen Sie den Wert von a, für den f bijektiv ist und bestimmen Sie anschließend die Umkehrabbildung.
Hinweis: Die Berechnung von Urbild und Umkehrabbildung sind identisch.

3.8. **Weiterführende Literatur.**

(1) Fritsche: Mathematik für Einsteiger

4. Mächtigkeit von Mengen

4.1. **Wiederholung.** Alle bisherigen Abschnitte, insbesondere den über Mengentheorie und Abbildungen.

Leitfrage. *In einem Tanzverein mit* 50 *Mitgliedern werden die drei Disziplinen Klassisch, Latin und Rock'n Roll angeboten. Die Disziplinen Klassisch und Rock'n Roll betreiben jeweils* 22 *Mitglieder. Nur die Latin Disziplin betreiben* 10 *Tanzende.* 38 *Mitglieder betreiben Rock'n Roll und/oder Latin. Alle drei Disziplinen betreibt ein Mitglied. Genau in zwei Disziplinen aktiv sind* 26 *Mitglieder. Gehen Sie davon aus, dass jedes Mitglied mindestens eine Disziplin betreibt. Wie viele Mitglieder betreiben genau eine Disziplin?.*

4.2. **Endliche Mengen.** Wir werden hier lernen, wie man darüber sprechen kann, wie viele Elemente eine Menge enthält. Wie es sich herausstellt, ist es deutlich einfacher zu sagen, wann zwei Mengen die gleiche Anzahl an Elementen haben. Das ist genau das, was wir zuerst diskutieren.

Definition 4.1. Zwei Mengen A und B heißen *gleichmächtig*, falls eine bijektive Abbildung $f\colon A \to B$ existiert.

Bemerkung 4.2. Die Gleichmächtigkeit zweier Mengen A und B bedeutet, dass die Mengen A und B die gleiche Anzahl von Elementen haben. Man beachte: Wir müssen dafür nicht wissen, wie viele Elemente A und B haben. Das ist besonders vorteilhaft, wenn die Anzahl der Elemente von A und B unbekannt oder unendlich ist.

Beispiel 4.3. Es sei A eine Menge mit fünf Elementen. Dann sind A und die Menge $B := \{1, 2, 3, 4, 5\}$ gleichmächtig. Um das zu sehen, benötigen wir eine bijektive Abbildung zwischen diesen Mengen. Es seien a_1, a_2, a_3, a_4, a_5 die paarweise verschiedenen Elemente von A in beliebiger aber fixer Reihenfolge. Dann definieren wir die Abbildung

$$1 \mapsto a_1\ ,\ 2 \mapsto a_2\ ,\ 3 \mapsto a_3\ ,\ 4 \mapsto a_4\ ,\ 5 \mapsto a_5\ .$$

Wegen unserer Annahmen ist das wirklich eine Abbildung, und nach Definition sogar bijektiv.

Um zu zeigen, dass zwei Mengen A und B gleichmächtig sind, reicht es, eine Bijektion $f\colon A \to B$ zu konstruieren. Die andere Richtung, also zu zeigen, dass A und B *nicht* gleichmächtig sind, ist normalerweise schwieriger. In diesem Fall muss man beweisen, dass es keine Bijektion von A nach B gibt. Es ist nicht ausreichend dafür zu zeigen, dass eine konkrete Abbildung von A nach B nicht bijektiv ist (denn es könnte eine andere Abbildung existieren, welche bijektiv ist).

A **4.4.** *Beweisen Sie die folgenden Aussagen:*

- *Die Mengen* $\{a, b, c\}$ *und* $\{1, 2, 3\}$ *sind gleichmächtig.*
- *Die Mengen* $\{1, 2\}$ *und* $\{1, 2, 3\}$ *sind nicht gleichmächtig.*
- *Sei* $A \neq \emptyset$*. Dann sind* A *und* $\emptyset$ *nicht gleichmächtig.*

Beispiel 4.5. Hier werden wir zeigen, dass die Mengen $\mathbb{N}$ und $2\mathbb{N} := \{2 \cdot n \mid n \in \mathbb{N}\}$ (das ist die Menge aller nicht-negativen geraden Zahlen) gleichmächtig sind. Das ist besonders interessant, da $2\mathbb{N} \subset \mathbb{N}$ eine echte Teilmenge (mit unendlichem Komplement) ist.

Betrachte die Abbildung $f\colon \mathbb{N} \to 2\mathbb{N}$, $f(m) = 2m$. Diese ist injektiv, da aus $2m = 2m'$ sofort $m = m'$ folgt und auch surjektiv, weil eine beliebige Zahl $m \in 2\mathbb{N}$ durch 2 teilbar ist.

Definition 4.6. Eine Menge A heißt *endlich*, falls eine natürliche Zahl n existiert, so dass A gleichmächtig zu der Menge $\{1, \ldots, n\}$ ist oder falls $A = \emptyset$. Eine Menge, die nicht endlich ist, heißt *unendlich*.

Bemerkung 4.7. Es folgt aus der Definition einer endlichen Menge, dass die leere Menge $\emptyset$ endlich ist und alle nicht-leeren endlichen Mengen positive Mächtigkeit haben.

Bemerkung 4.8. Es sei jetzt A eine endliche Menge. Wir werden es an dieser Stelle noch nicht zeigen, aber es existiert genau *eine* natürliche Zahl n, so dass A gleichmächtig zu $\{1, \ldots, n\}$ ist. Insbesondere hängt diese Zahl n *nur von* A ab.

Definition 4.9. Es sei A eine nicht-leere endliche Menge, die gleichmächtig zu $\{1, \ldots, n\}$ ist. Die *Mächtigkeit* oder *Kardinalität* oder *Anzahl der Elemente* von A ist die natürliche Zahl n. Die leere Menge hat Mächtigkeit 0.

Für die Mächtigkeit von A schreiben wir $|A|$ oder $\#A$.

Lemma 4.10. *Es seien A und B disjunkte endliche Mengen (das heißt ihr Schnitt ist leer). Dann gilt*

$$|A \dot\cup B| \;=\; |A| + |B| \;.$$

Beweis: Zunächst betrachten wir den Fall, wenn A oder B die leere Menge ist. Wenn $A = \emptyset$, dann sind A und B disjunkt (wegen $\emptyset \cap B = \emptyset$), und es gilt

$$|A \cup B| \;=\; |\emptyset \cup B| \;=\; |B| \;=\; 0 + |B| \;=\; |A| + |B| \;,$$

was wir wollten. Der Fall $B = \emptyset$ lässt sich analog erledigen.

Nehmen wir jetzt an, dass weder A noch B leer sind, und es seien $f\colon A \to \{1, \ldots, n\}$ und $g\colon B \to \{1, \ldots, m\}$ bijektive Abbildungen. Wir konstruieren eine bijektive Abbildung $A \cup B \to \{1, \ldots, m + n\}$.

Man betrachte die folgende Abbildung $h\colon A \cup B \to \{1, \ldots, n + m\}$:

$$h(x) \stackrel{\text{def}}{=} \begin{cases} f(x) & \text{falls } x \in A, \\ g(x) + n & \text{falls } x \in B. \end{cases}$$

Da $A \cap B = \emptyset$ ist die Abbildung h wohldefiniert. Sie ist injektiv, weil Elemente von A und B auf die disjunkten Mengen $\{1, \ldots, n\}$ und $\{n + 1, \ldots, n + m\}$ abgebildet werden und f und g per Annahme injektiv sind. Die Abbildung h ist surjektiv, da $h(A) = f(A) = \{1, \ldots, n\}$ und $h(B) = \{n + 1, \ldots, n + m\}$.

Es folgt dann aus Definition 4.9 der Mächtigkeit einer endlichen Menge, dass

$$|A \cup B| \;=\; n + m \;=\; |A| + |B|$$

ist. □

Der folgende Satz liefert eine alternative Beschreibung von endlichen Mengen, die nicht von unserer Kenntnis der natürlichen Zahlen abhängt. In diesem Sinne ist der Satz die „richtige“ Definition von Endlichkeit.

Satz 4.11. *Eine Menge A ist genau dann endlich, wenn keine echte Teilmenge B von A existiert, die gleichmächtig zu A ist.*

Beispiel 4.12. Die Menge $\mathbb{N}$ der natürlichen Zahlen ist unendlich. Wir haben bereits gesehen, dass eine Bijektion zwischen $\mathbb{N}$ und ihrer echten Teilmenge $2\mathbb{N}$ existiert.

Ebenfalls existiert eine Bijektion zwischen $\mathbb{Z}$ und der echten Teilmenge $\mathbb{N}$, daher sind beide Mengen unendlich. Aus dem gleichen Grund sind $\mathbb{Z}$ und $\mathbb{N}$ gleichmächtig.

(A) **4.13.** *Geben Sie eine Bijektion zwischen $\mathbb{N}$ und der Menge der positiven ganzen Zahlen an.*

(A) **4.14.** *Geben Sie eine Bijektion zwischen $\mathbb{N}$ und $\mathbb{N} \times \mathbb{N}$ an.*

Lemma 4.15. *Sei A eine endliche Menge, $B \subseteq A$. Dann ist B ebenfalls endlich.*

Beweis: Wir führen einen Widerspruchsbeweis. Angenommen, B sei unendlich. Dann gibt es eine echte Teilmenge $C \subsetneq B$, und eine Bijektion $f\colon C \to B$. Man betrachte jetzt

$$D \stackrel{\text{def}}{=} (A \setminus B) \cup C \ .$$

Man beachte, dass D eine echte Teilmenge von A ist. Wir konstruieren jetzt eine Bijektion von D nach A. Man definiere die Abbildung $g\colon D \to A$ wie folgt:

$$g(x) \stackrel{\text{def}}{=} \begin{cases} f(x) & \text{falls } x \in C, \\ x & \text{falls } x \in A \setminus B. \end{cases}$$

Dann ist g in der Tat eine wohldefinierte Abbildung von D nach A (weil $C \cap (A \setminus B) = \emptyset$), die eine Bijektion ist. Das bedeutet aber, dass A ebenfalls unendlich ist, ein Widerspruch. □

(A) **4.16.** *Zeigen Sie, dass die Abbildung g aus Lemma 4.15 bijektiv ist.*

Lemma 4.17. *Es seien $B \subseteq A$ endliche Mengen. Dann gilt $|B| \leq |A|$, und sogar $|B| < |A|$, wenn B eine echte Teilmenge von A ist.*

Beweis: Es sei $B \subseteq A$. Wenn $B = A$ ist, dann gilt $|B| = |A|$, daher können wir annehmen, dass $B \subsetneq A$. Man bemerke

$$A \ = \ B \,\dot\cup\, (A \setminus B) \ ,$$

wobei die Vereinigung disjunkt ist, und beide Mengen B und $A \setminus B$ sind endlich und nicht leer. Somit folgt nach Lemma 4.10

$$|A| \ = \ |B| + |A \setminus B| \ ,$$

wobei $|A \setminus B| > 0$ gilt und daher folgt $|B| < |A|$. □

Korollar 4.18. *Es seien $B \subseteq A$ Mengen. Falls B unendlich ist, dann ist auch A unendlich.*

Beweis: Wenn A endlich wäre, dann müsste wegen Lemma 4.15 auch B endlich sein, was unsere Annahme widerspricht. □

Lemma 4.19. *Es seien A und B Mengen.*

(1) *$A \cup B$ ist endlich $\iff$ A und B sind endlich.*
(2) *Falls A oder B endlich ist, dann ist es auch $A \cap B$.*

Beweis: Falls $A \cup B$ endlich ist, dann müssen wegen $A, B \subseteq A \cup B$ und Lemma 4.15 auch A und B endlich sein. Ebenfalls, wenn A oder B endlich sind, dann impliziert $A \cap B \subseteq A, B$ und Lemma 4.15, dass auch $A \cap B$ endlich ist.

Es bleibt zu zeigen, dass aus der Endlichkeit von A und B die Endlichkeit von $A \cup B$ folgt. Für den Fall, dass $A \cap B = \emptyset$ ist, wissen wir das schon nach Lemma 4.10. Sei also der Schnitt von A und B nicht leer. Wir nutzen einen Trick, der uns erlaubt, die Vereinigung von Mengen anders zu beschreiben. Es gilt

$$A \cup B \;=\; (A \setminus (A \cap B)) \,\dot\cup\, B.$$

Wegen $A \setminus (A \cap B) \subset A$ ist auch $A \setminus (A \cap B)$ endlich nach Lemma 4.15. Die Behauptung folgt nun mit Lemma 4.10.

□

Korollar 4.20. *Es seien A und B endliche Mengen. Dann gilt*

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

Beweis: Da A und B endlich sind, ist es auch $A \cup B$. Daher sind beide Seiten der Gleichung sinnvoll. Was die Rechnung betrifft;

$$A \cup B \;=\; A \,\dot\cup\, B \setminus A$$

ist eine disjunkte Zerlegung, somit folgt

$$|A \cup B| \;=\; |A| + |B \setminus A| \;.$$

Weiterhin ist auch

$$B \;=\; (A \cap B) \,\dot\cup\, (B \setminus A)$$

eine disjunkte Zerlegung, daher

$$|B| \;=\; |A \cap B| + |B \setminus A| \;.$$

Es folgt sofort

$$|B \setminus A| \;=\; |B| - |A \cap B| \;.$$

Dann gilt

$$|A \cup B| \;=\; |A| + (=\; |B| - |A \cap B|) \;,$$

wie gewollt. □

Korollar 4.21. *Es seien A und B endliche Mengen. Dann ist auch $A \cup B$ endlich und*

$$|A \cup B| \leq |A| + |B| \;.$$

Beweis: Folgt sofort aus Korollar 4.20, da $|A \cap B| \geq 0$. □

A **4.22.** *Es seien A,B,C endliche Mengen. Zeigen Sie, dass*

(1) *$A \cup B \cup C$ endlich ist, und*
(2) *verifizieren Sie die Formel*

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

Unser nächstes Ergebnis ist eine Besonderheit endlicher Mengen.

Aussage 4.23. *Es sei A eine endliche Menge, $f\colon A \to A$ eine Abbildung. Dann gilt*

$$f \text{ injektiv} \iff f \text{ surjektiv} \iff f \text{ bijektiv.}$$

Beweis: Es reicht zu zeigen, dass die Injektivität und Surjektivität von f äquivalent sind, der Rest folgt sofort. Zunächst nehmen wir an, dass f injektiv ist. Dann ist $f\colon A \to f(A) \subseteq A$ eine Bijektion, insbesondere muss $f(A) = A$ gelten, ansonsten wäre A unendlich.

Umgekehrt nehmen wir an, dass $f\colon A \to A$ surjektiv ist. Betrachten wir eine Abbildung $g\colon A \to A$ so dass für jedes $a \in A$ gilt, dass $g(a) \in f^{-1}(a)$. Dann ist $g\colon A \to A$ injektiv, und surjektiv genau dann, wenn f injektiv war. Wegen des ersten Teiles des Beweises sind wir fertig. □

Mithilfe der in diesem Abschnitt gelernten Formeln und Techniken, um die Anzahl der Elemente von Teilmengen gegebener Mengen zu bestimmen oder um umgekehrt durch Kenntnis der Anzahl der Elemente von Teilmengen die Mächtigkeit derer Vereinigung und Schnitte zu bestimmen, sind wir nun in der Lage mit Venn-Diagrammen zu arbeiten und damit die Leitfrage des Abschnittes zu beantworten. Venn-Diagramme sind im Grunde nur eine Visualisierung der Schnitte und Vereinigungen gegebener Mengen.

Beispiel 4.24. In einem Tanzverein mit 50 Mitgliedern werden die drei Disziplinen Klassisch, Latin und Rock'n Roll angeboten. Die Disziplinen Klassisch und Rock'n Roll betreiben jeweils 22 Mitglieder. Nur die Latin Disziplin betreiben 10 Tanzende. 38 Mitglieder betreiben Rock'n Roll und/oder Latin. Alle drei Disziplinen betreibt ein Mitglied. Genau in zwei Disziplinen aktiv sind 26 Mitglieder. Gehen Sie davon aus, dass jedes Mitglied mindestens eine Disziplin betreibt. Wie viele Mitglieder betreiben genau eine Disziplin?.

Beweis: Wir zeigen zwei Beweise. Beweis 1 beruht auf der Strategie, die gegebenen Mengen in disjunkte Teile zu zerlegen und damit die gesuchten Mengen zu bestimmen. Beweis 2 nutzt eine andere disjunkte Zerlegung aus, über die man bereits volle Kenntnis hat.
Beweis 1: Wir bezeichnen den Tanzverein mit T und die Disziplinen mit K, L und R. Wir wollen die Mächtigkeit der Menge bestimmen, die der Aussage entspricht, genau eine Disziplin zu betreiben. Das heißt, wir suchen genau die Mitglieder, die K betreiben ohne gleichzeitig L oder R zu betreiben etc, also suchen wir

$$| \ K \setminus (L \cup R) \ \bigcup \ L \setminus (K \cup R) \ \bigcup \ R \setminus (L \cup K) \ |.$$

Dazu müssen wir zunächst die Informationen aus dem Text mathematisieren:

- $|T| = 50$, also $|K \cup L \cup R| = 50$.
- Genau ein Mitglied betreibt alle Disziplinen: $|K \cap L \cap R| = 1$.
- $|K| = |R| = 22$.
- $|R \cup L| = 38$.
- Nur Latin betreiben 10: $|L \setminus (K \cup R)| = 10$. Das ist bereits eine der gesuchten Mengen.
- Genau in zwei sind 26 Mitglieder aktiv. Da wir wissen, wie viele in allen drei Disziplinen aktiv sind, können wir das wie folgt formulieren:
  $\Big|\Big((K \cap R) \ \cup \ (K \cap L) \ \cup \ (L \cap R)\Big) \setminus (K \cap L \cap R)| = 26.$

Bisher haben wir nur die Voraussetzungen übersetzt. Erst jetzt müssen wir überlegen, wie die gesuchten Mengen bestimmt werden können. Wenn wir die jeweiligen Schnittmengen kennen, können wir jede der Mengen K, L und R zerlegen in disjunkte Teilmengen. Schauen wir zuerst, was aus $|R \cup L| = 38$ gemacht werden kann.

- $|R \cup L| = 38$ impliziert $|K \setminus (R \cup L)| = 50 - 38 = 12$. Das ist bereits die zweite der gesuchten Mengen.

Die letzte Menge $R \setminus (L \cup K)$ können wir zerlegen (die anderen natürlich auch) in $R \setminus (L \cup K) = R \setminus \Big((R \cap K) \cup (R \cap L)\Big)$, wobei wir hier noch $K \cap L \cap R$ doppelt zählen. Wir wollen also $R \cap K$ und $R \cap L$ bestimmen. Es gilt

- $|L \setminus (K \cup R)| = 10$ impliziert $|R \cup K| = 40$.
- Da zusätzlich $|K| = |R| = 22$, muss $|R \cap K| = 4$.
- Wegen $|\Big((K \cap R) \ \cup \ (K \cap L) \ \cup \ (L \cap R)\Big) \setminus (K \cap L \cap R)| = 26$ müssen wir um $R \cap L$ zu bestimmen $K \cap L$ kennen.
- Wegen $|K| = 22$ und $|R \cap K| = 4$ und $|K \setminus (R \cap L)| = 12$ ist $|(K \cap L) \setminus R| = 22 - 12 - 4 = 6$.
- Es folgt $|(R \cap L) \setminus K| = 26 - 3 - 6 = 17$ wegen $|(K \cap R) \setminus L| = 3$. Also $|R \cap L| = 18$.
- Schließlich ist also $|R \setminus (L \cup K)| = 22 - 18 - 4 + 1 = 1$. Die 1 müssen wir dazu addieren, wir wir $R \cap L \cap K$ zweimal abgezogen haben.

Insgesamt wissen wir jetzt also

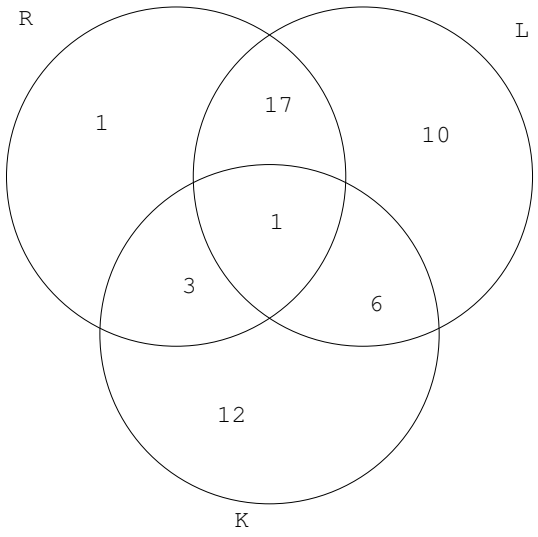
$$| \ K \setminus (L \cup R) \ \bigcup \ L \setminus (K \cup R) \ \bigcup \ R \setminus (L \cup K) \ | = 10 + 12 + 1 = 23.$$

Beweis 2: Liest man den Text aufmerksam, so kann man folgende Fakten entnehmen:

- Jedes der 50 Mitglieder ist mindestens in einer Disziplin.
- Genau ein Mitglied ist in genau 3 Disziplinen.
- Genau 26 Mitglieder sind in genau 2 Disziplinen.
- Da man logischerweise nur enweder genau eine, zwei oder drei Disziplinen machen kann, sind diese Mengen disjunkt.
- Also sind genau $50 - 1 - 26 = 23$ Mitglieder in genau einer Disziplin.

□

Grundsätzlich kann man Aufgaben von dieser Form immer mit einem *Venn-Diagramm* lösen. Das ist im Prinzip nichts anderes als die Visualisierung der Zerlegung von T in disjunkte Teilmengen. Damit kann man dann die Lösung zu den meisten Fragestellungen ablesen. Ein Venn-Diagramm sieht im Fall von Beispiel 4.24 wie folgt aus:



4.3. **Schubfachprinzip.**

Aussage 4.25. *Es seien A und B endliche Mengen, $f\colon A \to B$ eine Abbildung.*

(1) *Falls f injektiv ist, dann ist $|A| \leq |B|$.*
(2) *Falls f surjektiv ist, dann ist $|A| \geq |B|$.*

Beweis: Was die erste Aussage betrifft, für eine injektive Abbildung gilt $|A| = |f(A)|$, und aus $f(A) \subseteq B$ folgt $|f(A)| \leq |B|$. Die zwei Ungleichungen lassen sich kombinieren:

$$|A| \;=\; |f(A)| \leq |B| \;.$$

Für eine beliebige Abbildung gilt $|A| \geq |f(A)|$, wenn f surjektiv ist, dann ist noch dazu $f(A) = B$, daher

$$|A| \geq |f(A)| = |B| \;,$$

wie gewollt. □

Korollar 4.26. *Es seien A und B endliche Mengen und es sei $f\colon A \to B$ eine Abbildung. Falls $|A| > |B|$, dann ist f* nicht *injektiv.*

Beweis: Folgt sofort aus Aussage 4.25 (i). □

Die folgende Umformulierung ist in vielen Fällen sehr nützlich.

Korollar 4.27 (Schubfachprinzip)**.** *Es seien n Objekte in k Kategorien eingeteilt, so dass $n > k$ ist. Dann gibt es mindestens eine Kategorie, die mindestens zwei Objekte enthält.*

Beweis: Es seien

$$A \stackrel{\text{def}}{=} \text{die Menge der Objekte ,}$$
$$B \stackrel{\text{def}}{=} \text{die Menge der Kategorien/Schubfächer ,}$$

und $f\colon A \to B$ die Zuordnung, die von der Einteilung kommt (das heißt: Für ein Objekt $a \in A$ ist $f(a) \in B$ die Kategorie, in welche a eingeteilt wurde). Dann ist

$$|A| \;=\; n \;>\; k \;=\; |B| \;.$$

Wegen Korollar 4.26 ist f nicht injektiv, das heißt, es gibt ein $b \in f(A)$ mit $|f^{-1}(b)| \geq 2$. Das ist genau das, was wir behauptet haben. □

4.4. **Übungsufgaben.**

Hausaufgabe 4.28. *Geben Sie eine Bijektion zwischen $\mathbb{N}$ und $\mathbb{Z}$ an, indem Sie ausnutzen, dass ganze Zahlen gerade oder ungerade sind, aber nie beides zugleich.*

Hausaufgabe 4.29. *Geben Sie eine Bijektion zwischen $\mathbb{N} \times \mathbb{N}$ und $\mathbb{Z}$ an. Zusammen mit Aufgabe 4.14 folgt erneut $|\mathbb{N}| = |\mathbb{Z}|$.*

Hausaufgabe 4.30. *Begründen Sie die folgenden Aussagen mit Hilfe des Schubfachprinzips.*

(1) *Unter je 32 Personen gibt es mindestens zwei, welche am selben Tag des Monats Geburtstag haben.*
(2) *Es gibt zwei Franzosen, die die gleiche Anzahl von Haaren auf dem Kopf haben.*
(3) *Unter je 9 Personen gibt es mindestens zwei, die die gleichen Blutgruppe haben.*

Hausaufgabe 4.31. *In der Sockenschublade befinden sich 10 weiße und 10 schwarze Socken. Wie oft muss man mit geschlossenen Augen aus der Schublade ziehen, bis man*

(1) *mit Sicherheit zwei gleichfarbige Socken hat?*
(2) *mit Sicherheit zwei schwarze Socken hat?*

4.5. **Wiederholungsaufgaben.**

Hausaufgabe 4.32. *Ein Fitnessstudio hat* 420 *Mitglieder. Der Yoga-Kurs wird von* 111 *dieser Mitglieder besucht. Außerdem nehmen* 60 *Mitglieder sowohl am Yoga-Kurs als auch am Zumba-Kurs teil. Ausschließlich den Pilates-Kurs besuchen* 70 *Mitglieder. Schließlich besuchen* 25 *Mitglieder den Pilates-Kurs und den Zumba-Kurs, aber nicht den Yoga-Kurs und* 4 *Mitglieder besuchen alle Kurse. Wie viele Mitglieder des Fitnessstudios besuchen keinen dieser Kurse?*

Hausaufgabe 4.33. *Bei einer Umfrage wurden* 1000 *Zeitschriftenlesende befragt, welche der Zeitschriften A, B oder C sie regelmäßig lesen. Es wurden folgende Angaben gemacht.*
530 *lesen die Zeitschrift A;* 450 *davon nur A.* 150 *lesen nur die Zeitschrift B,* 7 *lesen die Zeitschriften B und C,* 20 *lesen ausschließlich die Zeitschriften A und B. Ferner lesen* 55 *ausschließlich die Zeitschriften A und C.* 195 *lesen keine dieser Zeitschriften.*

a) *Wie viele lesen mindestens eine Zeitschrift?*
b) *Wie viele lesen alle drei Zeitschriften?*
c) *Wie viele lesen die Zeitschrift C?*
d) *Wie viele lesen höchstens eine Zeitschrift?*

Hausaufgabe 4.34. *In einer Schachtel befinden sich farbige Bälle. Jeder Ball enthält mindestens eine der Farben Blau, Grün, Rot und Gelb.*
Es gibt 16 *Bälle, die Blau enthalten,* 25*, die Grün enthalten,* 15*, die Gelb enthalten und* 22*, die Rot enthalten.*
Darüber hinaus gibt es 5*, die Blau und Grün enthalten,* 6*, die Blau und Gelb enthalten,* 0*, die Blau und Rot enthalten,* 4*, die Grün und Gelb enthalten,* 7*, die Grün und Rot enthalten und* 6*, die Rot und Gelb enthalten.*
Weiterhin gibt es 0*, die Rot, Grün und Blau enthalten,* 2*, die Blau, Grün und Gelb enthalten,* 0*, die Grün, Gelb und Rot enthalten und* 0*, die Gelb, Rot und Blau enthalten.*
Außerdem gibt es keine Bälle, die Rot, Grün, Blau und Gelb enthalten.
Wieviele Bälle sind in der Schachtel?

4.6. **Weiterführende Literatur.**

(1) Fritsche: Mathematik für Einsteiger

5.1. **Wiederholung.** Grundlagen zu Mengen und Abbildungen. Außerdem benötigen Sie die Grundlagen im Bruchrechnen und müssen sowohl mit Potenzen, Gleichungen als auch mit Ungleichungen umgehen können.

Leitfrage. *Wie kann man zeigen, dass für jede natürliche Zahl n gilt* $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ *?*

5.2. **Das Prinzip der vollständigen Induktion.** Die natürlichen Zahlen $\mathbb{N}$ haben verschiedene interessante Strukturen:

- $(\mathbb{N}, +, \cdot)$: Wir können natürliche Zahlen Addieren und Multiplizieren. Außerdem können wir das Konzept von Teilbarkeit einführen.
- $(\mathbb{N}, <)$: Wir können natürliche Zahlen nach ihrer Größe ordnen.
- Jede Zahl $m \in \mathbb{N}$ hat einen „Nachfolger“ $m + 1$.

An dieser Stelle werden wir die Nachfolger-Struktur der natürlichen Zahlen weitesgehend ausnutzen. Das führt zu einer Beweismethode (der sogenannten vollständigen Induktion), die dramatische Konsequenzen für die ganze Mathematik hat.

Alles beruht auf der folgenden Aussage, die wir als Axiom betrachten (das heißt wir nehmen an, dass diese Aussage wahr ist).

Aussage 5.1. *(Induktionsprinzip)*
Sei $M \subseteq \mathbb{N}_+$ eine Teilmenge mit den Eigenschaften

(i) $1 \in M$.

(ii) $\forall m \in \mathbb{N}_+ : \Big(\; m \in M \Rightarrow m + 1 \in M \Big)$.

Dann ist bereits $M = \mathbb{N}_+$.

Das ermöglicht ein wichtiges Beweisverfahren: „Beweis durch vollständige Induktion“.

Die Methode: Sei $A(m)$ eine Aussageform, für die $\mathbb{N}_+$ einen zulässigen Objektbereich bildet. Wir wollen die Aussage

$$\forall m \in \mathbb{N}_+ : \; A(m)$$

beweisen. Sei dazu $M := \{m \in \mathbb{N}_+ \mid A(m)\}$. Dann ist $\forall m \in \mathbb{N}_+ : \; A(m)$ äquivalent zu $M = \mathbb{N}_+$.

Der Beweis besteht aus zwei Teilen:

(i) Induktionsanfang: Man zeige, dass $A(1)$ wahr ist (d.h. $1 \in M$).

(ii) Induktionsschluss: Man zeige, dass für beliebige $m \in \mathbb{N}_+$ die Implikation

$$A(m) \Rightarrow A(m + 1)$$

wahr ist (d.h. $m \in M \Rightarrow m + 1 \in M$). Die Annahme „$A(m)$ ist wahr“ heißt auch Induktionsannahme oder Induktionsvoraussetzung. Aus (i) und (ii) folgt wegen des Induktionsprinzips, dass $M = \mathbb{N}_+$ ist, d.h. $A(m)$ stimmt für alle $m \in \mathbb{N}_+$.

Bemerkung 5.2. Das Induktionsprinzip lässt sich auch anwenden, wenn der Induktionsanfang nicht bei $n = 1$ liegt. Ist $M \subseteq \mathbb{N}$ und $m \in M$, sodass jeder Nachfolger von m Element von M ist, dann folgt $M = \mathbb{N}_{\geq m}$.

Im Folgenden werden wir dieses Beweisverfahren an einigen Beispielen veranschaulichen.

Beispiel 5.3. (a) (Kleiner Gauß)

Wir behaupten, dass die folgende Gleichung für alle positiven natürlichen Zahlen $n \in \mathbb{N}_+$ wahr ist

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

Beweis:

(i) **Induktionsanfang:** Für $n = 1$ gilt $1 = \frac{1\cdot(1+1)}{2}$. Somit stimmen, wie gewünscht, die beiden Seiten der Gleichung überein.

(ii) **Induktionsschluss:** Wir gehen nun davon aus, dass $1 + \ldots + n = \frac{n(n+1)}{2}$ gilt (Induktionsannahme, kurz IA). Davon ausgehend wollen wir zeigen, dass

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

ebenfalls gilt. Tatsächlich gilt

$$\begin{aligned} 1 + \ldots + (n+1) &= 1 + \ldots + n + (n+1) \overset{\text{IA}}{=} \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)\Big((n+1)+1\Big)}{2}. \end{aligned}$$

□

(b) $\forall n \in \mathbb{N}_+ : \; n \geq 1$.

Bemerkung: Die Aussage erscheint zunächst trivial, da wir wissen, dass jede positive natürliche Zahl ≥ 1 ist. Aber die meisten dieser Zahlen können wir nicht benennen (es gibt zu viele!). Die Notation $n \to n+1$ verwenden wir gelegentlich als Abkürzung für $A(n) \Rightarrow A(n+1)$.

Beweis:

(i) **Induktionsanfang:** Für $n = 1$ gilt $n \geq 1$.

(ii) **Induktionsschluss:** $(n \to n+1)$ Es sei für eine gegebenes $n \in \mathbb{N}_+$ bewiesen, dass $n \geq 1$ gilt. Dann folgern wir

$$n + 1 \overset{\text{IA}}{\geq} 1 + 1 = 2 > 1$$

□

(c) Für jedes $n \in \mathbb{N}_{>4}$ gilt $2^n > n^2$.

Beweis: Die Aussage soll für alle positiven ganzen Zahlen gelten, welche größer als 4 sind. Daher müssen mir im Induktionsanfang mit $n = 5$ beginnen.

(i) **Induktionsanfang:** Für $n = 5$ gilt $2^5 = 32$ und $5^2 = 25$. Wegen $32 > 25$ ist die Aussage wahr.

(ii) **Induktionsschluss:** $(n \to n+1)$ Es sei für ein gegebenes $n \in \mathbb{N}_{>4}$ bewiesen, dass $2^n > n^2$ gilt. Dann folgern wir zunächst durch Faktorisieren

$$2^{n+1} = 2^n \cdot 2 \overset{\text{IA}}{\geq} 2 \cdot n^2 = n^2 + n^2.$$

Auf der rechten Seite der behaupteten Ungleichung steht $(n+1)^2 = n^2 + 2n + 1$. Das heißt wir müssen noch $2 \cdot n^2 > (n+1)^2$ zeigen, oder äquivalent

$$n^2 > 2n + 1.$$

Dazu verwenden wir erneut Induktion. Für $n = 5$ gilt $n^2 = 25 > 11 = 2n + 1$. Es sei für ein gegebenes $n \in \mathbb{N}_{>4}$ bewiesen, dass $n^2 > 2n + 1$ gilt. Dann folgt

$$(n+1)^2 = n^2 + 2n + 1 \overset{\text{IA2}}{\geq} 4n + 2.$$

Auf der rechten Seite steht $2(n+1) + 1 = 2n + 3$. Da $n > 4$ ist, haben wir

$$2n + 3 < 3n < 4n + 2 < (n+1)^2$$

und die Behauptung folgt.

□

(d) Eine Menge A mit n Elementen hat 2^n Teilmengen. Alternativ formuliert bedeutet das, dass die Potenzmenge von A genau 2^n Elemente besitzt. Beweis siehe Satz 5.10.

(e) Für jede natürliche Zahl $n \geq 1$ gilt

$$\left(\sum_{k=1}^{n} \frac{1}{k(k+1)} =\right) \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \ldots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

Beweis:

(i) **Induktionsanfang:** Für $n = 1$ gilt $\frac{1}{1 \cdot 2} = \frac{n}{n(n+1)}$.

(ii) **Induktionsschluss:** Wir nehmen an, dass für ein festes aber beliebiges $n \in \mathbb{N}_+$

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

gilt und wollen davon ausgehend zeigen, dass dann auch

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

gilt. **Rechnung:**

$$\begin{aligned}
&\frac{1}{1 \cdot 2} + \ldots + \frac{1}{(n+1)(n+2)} \\
&= \left(\frac{1}{1 \cdot 2} + \ldots + \frac{1}{n(n+1)}\right) + \frac{1}{(n+1)(n+2)} \\
&\overset{\text{IA}}{=} \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n(n+2)}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)} = \frac{n(n+2)+1}{(n+1)(n+2)} \\
&= \frac{(n+1)^2}{(n+1)(n+2)} = \frac{n+1}{n+2}.
\end{aligned}$$

□

Die folgende Definition ist eigentlich nur eine verkürzende Notationsweise.

Definition 5.4 (Summe)**.** Es sei k eine positive ganze Zahl, und es seien $a_, \ldots, a_k$ reelle Zahlen. Wir definieren

$$\sum_{i=1}^{k} a_i \stackrel{\text{def}}{=} a_1 + \ldots + a_k \ .$$

Bemerkung 5.5. Wir können die Definition von $\sum$ auch so formulieren, dass keine aufzählende Darstellung der Summanden benötigt wird:

$$\sum_{i=1}^{1} a_i \stackrel{\text{def}}{=} a_1 \ , \ \sum_{i=1}^{j+1} a_i \stackrel{\text{def}}{=} \sum_{i=1}^{j} a_i \ + a_{j+1} \ \text{ für alle } 2 \leq j \leq k.$$

Diese Art von Definition wird *rekursive Definition* genannt, und passt hervorragend zur vollständigen Induktion.

Beispiel 5.6. Mit dem Summenzeichen können wir zum Beispiel die folgende Summation umformulieren:

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

Weitere Beispiele finden Sie in Beispiel 5.3.

Eine typische Anwendung der vollständiger Induktion ist die Erweiterung von Aussagen über zwei Objekte auf mehrere (aber immer noch endlich viele).

Aussage 5.7 (Allgemeines Distributivgesetz)**.**
Es sei $n \geq 2$ eine ganze Zahl, $a, b_1, \ldots, b_n \in \mathbb{R}$. Dann gilt

$$a \cdot \left(\sum_{i=1}^{n} b_i \right) \ = \ \sum_{i=1}^{n} (a \cdot b_i) \ .$$

Beweis: Induktionsanfang: Für $n = 2$ benutzen wir das (aus der Schule bekannte) Distributivgesetz

$$a \cdot \left(\sum_{i=1}^{2} b_i \right) \ = \ a(b_1 + b_2) \ = \ (ab_1) + (ab_2) \ = \ \sum_{i=1}^{n} (a \cdot b_i) \ .$$

Induktionsschritt: Wir nehmen an, dass

$$a \cdot \left(\sum_{i=1}^{n} b_i \right) \ = \ \sum_{i=1}^{n} (a \cdot b_i) \ .$$

gilt, und versuchen die gleiche Aussage für $n + 1$ zu zeigen.

$$\begin{aligned} a \cdot \left(\sum_{i=1}^{n+1} b_i \right) \ &= \ a \cdot \left(\left(\sum_{i=1}^{n} b_i \right) + b_{n+1} \right) \\ &= \ a \cdot \left(\sum_{i=1}^{n} b_i \right) + (a \cdot b_{n+1}) \\ &= \ \sum_{i=1}^{n} (a \cdot b_i) + (a \cdot b_{n+1}) \\ &= \ \sum_{i=1}^{n+1} (a \cdot b_i) \ . \end{aligned}$$

Bei der ersten Gleichung haben wir das Assoziativgesetz für reelle Zahlen verwendet, bei der zweiten den Induktionsanfang (das heisst, das Distributivgesetz für $n = 2$), bei der dritten die Induktionsannahme, und bei der vierten die (rekursive) Definition des Summenzeichen. □

Bemerkung 5.8. Nach dem Muster

$$\sum_{i=1}^{n} a_k \;=\; a_1 + \ldots + a_n$$

schreiben wir

$$\bigcup_{i=1}^{n} A_i \;=\; A_1 \cup \ldots \cup A_n \;,$$

und analog

$$\bigcap_{i=1}^{n} A_i \;=\; A_1 \cap \ldots \cap A_n \;.$$

Aussage 5.9 (Allgemeines Distributivgesetz für Mengen (Schritt über Vereinigung))**.** *Es sei $n \geq 2$ eine ganze Zahl, $A, B_1, \ldots, B_n$ beliebige Mengen. Dann gilt*

$$A \cap \left(\bigcup_{i=1}^{n} B_i \right) \;=\; \bigcup_{i=1}^{n} (A \cap B_i) \;.$$

Beweis: Induktionsanfang: Für $n = 2$ haben wir in Satz 2.28 gesehen, dass

$$A \cap \left(\bigcup_{i=1}^{2} B_i \right) \;=\; A \cap (B_1 \cup B_2) \;=\; (A \cap B_1) \cup (A \cap B_2) \;=\; \bigcup_{i=1}^{2} (A \cap B_i) \;.$$

Induktionsschritt: Wir nehmen an, dass

$$A \cap \left(\bigcup_{i=1}^{n} B_i \right) \;=\; \bigcup_{i=1}^{n} (A \cap B_i) \;.$$

gilt, und versuchen die gleiche Aussage für $n + 1$ zu zeigen.

$$\begin{aligned} A \cap \left(\bigcup_{i=1}^{n+1} B_i \right) \;&=\; A \cap \left(\left(\bigcup_{i=1}^{n} B_i \right) \cup B_{n+1} \right) \\ &=\; A \cap \left(\bigcup_{i=1}^{n} B_i \right) \cup (A \cap B_{n+1}) \\ &=\; \bigcup_{i=1}^{n} (A \cap B_i) \cup (A \cap B_{n+1}) \\ &=\; \bigcup_{i=1}^{n+1} (A \cap B_i) \;. \end{aligned}$$

Bei der ersten Gleichung haben wir das Assoziativgesetz für die Vereinigung von Mengen verwendet, dann bei der zweiten den Induktionsanfang (das heisst, das entsprechende Distributivgesetz für $n = 2$), bei der dritten die Induktionsannahme, und bei der vierten die (rekursive) Definition des Vereinigungszeichens. □

5.3. **Kompliziertere Anwendungen.**

Satz 5.10. *Sei X eine Menge mit $n \in \mathbb{N}$ Elementen. Dann hat $\mathcal{P}(X)$ genau 2^n Elemente.*

$|\mathcal{P}(X)| = 2^n$ heißt, dass X genau 2^n verschiedene Teilmengen hat. Wir werden die Aussage mittels vollständiger Induktion beweisen.

(A) **5.11.** *Überprüfen Sie die Aussage für kleine Werte von n, also $n = 0, 1, 2, 3$.*

Beweis:
INDUKTIONSANFANG: Ist $|X| = 0$, d.h. $X = \emptyset$, dann gilt $|\mathcal{P}(X)| = 1 = 2^0$.
INDUKTIONSSCHRITT: Wir nehmen an, dass aus $|X| = n$ folgt $|\mathcal{P}(X)| = 2^n$ und wollen zeigen: Aus $|X| = n + 1$ folgt

$$|\mathcal{P}(X)| = 2^{n+1} = 2 \cdot 2^n.$$

(„Für jedes neue Element bekommen wir doppelt so viele Teilmengen.“)

Angenommen es gilt $|X| = n + 1$, dann gelte ohne Beschränkung der Allgemeinheit $X = \{1, 2, \ldots, n + 1\}$. Wir definieren

$$\mathcal{M}_0 := \{U \subseteq X \mid n + 1 \notin U\} \text{ und}$$
$$\mathcal{M}_1 := \{V \subseteq X \mid n + 1 \in V\}$$

Dann gilt $\mathcal{M}_0 \cup \mathcal{M}_1 = \mathcal{P}(X)$ und $\mathcal{M}_0 \cap \mathcal{M}_1 = \emptyset$, insbesondere $|\mathcal{M}_0| + |\mathcal{M}_1| = |\mathcal{P}(X)|$ und

$$\mathcal{M}_0 = \mathcal{P}\big(X \setminus \{n + 1\}\big)$$

Wir konstruieren jetzt eine Bijektion $\varphi : \mathcal{P}(X \setminus \{n + 1\}) \longrightarrow \mathcal{M}_1$ und zeigen damit, dass $|\mathcal{M}_1| = |\mathcal{P}(X)|$ ist. Sei

$$\varphi : \mathcal{P}(X \setminus \{n + 1\}) \longrightarrow \mathcal{M}_1, \quad V \longmapsto V \cup \{n + 1\}.$$

- Dies ist eine wohldefinierte Abbildung.
- φ ist injektiv:
  Falls $V_1 \cup \{n + 1\} = V_2 \cup \{n + 1\}$, dann auch $V_1 = V_2$, weil $n + 1 \notin V_1, V_2$.
- φ ist surjektiv:
  Für $W \in \mathcal{M}_1$ ist $W \setminus \{n + 1\} \subseteq X \setminus \{n + 1\}$, daher $\varphi(W \setminus \{n + 1\}) = W$.

Zusammengefasst:

$$\mathcal{P}(X) = \mathcal{M}_0 \,\dot\cup\, \mathcal{M}_1$$
$$\mathcal{M}_0 = \mathcal{P}(X \setminus \{n + 1\})$$
$$\mathcal{M}_1 \xrightarrow{\sim} \mathcal{P}(X \setminus \{n + 1\}) \text{ gleichmächtig.}$$

Nach der Induktionsannahme gilt

$$|\mathcal{P}(X \setminus \{n + 1\})| = 2^n.$$

Insbesondere:

$$\begin{aligned} |\mathcal{P}(X)| &= |\mathcal{M}_0 \,\dot\cup\, \mathcal{M}_1| \\ &= |\mathcal{M}_0| + |\mathcal{M}_1| \\ &= |\mathcal{P}(X \setminus \{n + 1\})| + |\mathcal{P}(X \setminus \{n + 1\})| \\ &= 2^n + 2^n = 2^{n+1}, \end{aligned}$$

wie gewünscht. □

Satz 5.12. *Seien X, Y endliche Mengen mit Mächtigkeit $|X| = n$ und $|Y| = m$ für $m, n \in \mathbb{N}_+$. Dann hat das kartesische Produkt $X \times Y$ genau $n \cdot m$ Elemente.*

Beweis: (Vollständige Induktion über die Anzahl der Elemente m von Y. Wir können nicht zugleich eine Induktion über n und m führen!)
INDUKTIONSANFANG: Ist $|Y| = 1$, sagen wir $Y = \{1\}$, dann ist die Abbildung

$$X \longrightarrow X \times \{1\}, \quad x \longmapsto (x, 1)$$

eine Bijektion. Daher folgt

$$n \cdot 1 = |X \times \{1\}| = |X| = n.$$

INDUKTIONSSCHRITT: Wir nehmen an, dass

$$|X \times \{1, 2, \ldots, m\}| = n \cdot m$$

ist, und wollen zeigen, dass dann gilt

$$|X \times \{1, 2, \ldots, m+1\}| = n(m+1).$$

Rechnung:

$$\begin{aligned}
&|X \times \{1, 2, \ldots, m+1\}| \\
&= |X \times (\{1, 2, \ldots, m\} \cup \{m+1\})| \\
&= |(X \times \{1, \ldots, m\}) \dot{\cup} (X \times \{m+1\})| \\
&= |X \times \{1, \ldots, m\}| + |X \times \{m+1\}| \\
&= n \cdot m + m = n(m+1).
\end{aligned}$$

□

Die folgende Aussage ist eine simple und sehr typische Anwendung der vollständigen Induktion.

Aussage 5.13. *Es sei n eine positive ganze Zahl, und es seien $A_1, \ldots, A_n$ endliche Mengen. Dann ist $A_1 \cup \ldots \cup A_n$ endlich.*

Beweis: INDUKTIONSANFANG: Sei $n = 1$. Dann ist die Vereinigung einfach A_1 selbst, welche per Annahme endlich ist.
INDUKTIONSSCHRITT: Wir nehmen an, dass wir wissen, dass eine Vereinigung von n endlichen Mengen endlich ist, und wollen zeigen, dass die Vereinigung von $n+1$ endlichen Mengen ebenfalls endlich wird. Es seien $A_1, \ldots, A_{n+1}$ endliche Mengen. Es gilt

$$A_1 \cup \ldots \cup A_n \cup A_{n+1} \quad = \quad (A_1 \cup \ldots \cup A_n) \cup A_{n+1} \ .$$

Die Vereinigung $B \stackrel{\text{def}}{=} A_1 \cup \ldots \cup A_n$ ist nach der Induktionsannahme endlich, aber dann können wir die Vereinigung umschreiben:

$$A_1 \cup \ldots \cup A_n \cup A_{n+1} \ = \ B \cup A_{n+1}$$

Nach Lemma 4.19 (1) ist die Vereinigung zweier endlicher Menge erneut endlich und die Behauptung folgt. □

5.4. **Übungsufgaben.**

Hausaufgabe 5.14. *Seien $A_1, A_2, \ldots, A_{n+1}$ Mengen und $f_i \colon A_i \to A_{i+1}, i = 1, \ldots, n$ injektive Abbildungen. Zeigen Sie, dass die Komposition $f_n \circ \ldots \circ f_2 \circ f_1$ injektiv ist (nutzen Sie Aufgabe 3.78).*

Hausaufgabe 5.15. *Beweisen Sie mit vollständiger Induktion folgende Gleichung:*

$$\sum_{k=1}^{n} k \cdot k! \;=\; (n+1)! - 1 \qquad\qquad \forall n \in \mathbb{N}_+ := \{1, 2, 3, \ldots\}.$$

Dabei ist für $n \in \mathbb{N}$ der Ausdruck $n!$ definiert als $n \cdot (n-1) \cdot \ldots \cdot 1$ und $0! := 1$.

Hausaufgabe 5.16. *Beweisen Sie mit vollständiger Induktion folgende Ungleichung:*

$$n! \;\leq\; n^n \quad \forall n \in \mathbb{N}_+.$$

Hausaufgabe 5.17. *Beweisen Sie mit vollständiger Induktion folgende Ungleichung:*

$$2^n \geq n^2.$$

Hausaufgabe 5.18. *Beweisen Sie mit vollständiger Induktion folgende Ungleichung:*

$$2^n \geq n + 1.$$

Hausaufgabe 5.19. *Beweisen Sie mit vollständiger Induktion:*

$$\Big(\prod_{k=2}^{n}\Big(1 - \frac{1}{k}\Big) =\Big)\Big(1 - \frac{1}{2}\Big) \cdot \Big(1 - \frac{1}{3}\Big) \cdot \ldots \cdot \Big(1 - \frac{1}{n}\Big) = \frac{1}{n}.$$

Hausaufgabe 5.20. *Beweisen Sie mit vollständiger Induktion:*

$$\sum_{k=1}^{n} 3k - 2 = \frac{n(3n-1)}{2}.$$

Hausaufgabe 5.21. *Beweisen Sie mit vollständiger Induktion:*

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

Hausaufgabe 5.22. *Sei $q \in \mathbb{R}$ mit $0 < |q| < 1$ gegeben. Beweisen Sie mit vollständiger Induktion, dass die folgende Aussage für alle natürlichen Zahlen $n \geq 1$ erfüllt ist:*

$$\Big(\sum_{k=0}^{n} q^k =\Big) 1 + q + q^2 + \ldots + q^n = \frac{1 - q^{n+1}}{1 - q}.$$

5.5. **Wiederholungsaufgaben.**

Hausaufgabe 5.23. *Beweisen Sie mit vollständiger Induktion:*

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

Hausaufgabe 5.24. *Beweisen Sie mit vollständiger Induktion:*

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

Hausaufgabe 5.25. *Beweisen Sie mit vollständiger Induktion:*

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Hausaufgabe 5.26. *Beweisen Sie mit vollständiger Induktion:*

$$\sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}.$$

Hausaufgabe 5.27. *Beweisen Sie mit vollständiger Induktion:*

$$\sum_{k=1}^{n} 4k - 1 = 2n^2 + n.$$

5.6. **Weiterführende Literatur.**

(1) Fritsche: Mathematik für Einsteiger

6. Kombinatorik

6.1. **Wiederholung.** Die Abschnitte über endliche Mengen und vollständige Induktion aus Elementarmathematik I.

6.2. **Permutationen und Kombinationen.** Kombinatorik ist im Grunde genommen das Studium von endlichen Mengen ohne zusätzliche Struktur. Auch wenn man auf diese Weise nicht viel voraussetzt, kann und wird dieses mathematische Gebiet schnell kompliziert. Hier werden wir die Grundlagen der Kombinatorik kennenlernen; diese sind übrigens auch für Wahrscheinlichkeitstheorie oder Stochastik sehr nützlich.

Unsere Methode des Kennenlernens ist folgende: Wir stellen natürliche Fragen über endliche Mengen und werden sehen, welche Antworten die Mathematik dafür liefern kann.

Leitfrage. *Wie viele Möglichkeiten gibt es, ein Lotterieticket, bei dem man 6 Zahlen aus 49 auswählen muss, auszufüllen?*

Der Weg zur Antwort fängt mit der Frage an:

Frage 6.1. *Auf wie viele verschiedene Arten können wir die Elemente einer Menge mit n Elementen zählen?*

(A) **6.2.** *Betrachte die Mengen $\{a\}$,$\{a,b\}$,$\{a,b,c\}$,$\{1\}$, $\{4,5\}$,$\{5,4,3\}$. Beschreiben Sie die Elemente von diesen Mengen in allen möglichen Reihenfolgen.*

Bemerkung 6.3. Wir haben gesehen, dass in den konkreten Beispielen die Anzahl der möglichen Reihenfolgen nicht wirklich von der Menge selbst, sondern nur von der Mächtigkeit der Menge abhängt. Wenn wir zum Beispiel die Mengen $\{a,b\}$ und $\{4,5\}$ betrachten, dann können wir für jede Reihenfolge der Elemente a,b eine passende Anordnung von $4,5$ finden, wobei wir statt a immer 4 und statt b immer 5 schreiben.

Eine Anordnung der Elemente einer Menge A ist eine Vorschrift, welches Element wir als Erstes nehmen, welches als Zweites, und so weiter. Das lässt sich wie folgt formalisieren:

Definition 6.4. Für eine natürliche Zahl n schreiben wir

$$[n] \stackrel{\text{def}}{=} \{1,\dots,n\} \ .$$

Es sei jetzt A eine endliche Menge mit n Elementen. Eine *Anordnung* oder *Reihenfolge* oder *Permutation* der Elemente von A ist eine Bijektion

$$\pi\colon [n] \;=\; \{1,\dots,n\} \longrightarrow A \ .$$

Bemerkung 6.5. Für $n=0$ folgt aus Definition 1.4, dass $[0]=\emptyset$ ist.

(A) **6.6.** *Schreiben Sie die möglichen Anordnungen der Menge $\{5,4,6\}$ als Bijektionen $[3]\to\{5,4,6\}$. Überzeugen Sie sich, dass die mengentheoretische Definition der Anordnung unserem Alltagskonzept entspricht.*

Bemerkung 6.7. Es folgt aus der Definition einer Permutation, dass die Menge der Anordnungen einer Menge A mit n Elementen genau $\mathrm{Abb}([n],A)$ (siehe Bemerkung 3.9) entspricht. Wenn wir die Anzahl von solchen Permutationen herausfinden möchten, dann interessieren wir uns

nur für die Elemente von $\mathrm{Abb}([n], A)$, die bijektiv sind. Wir müssen also die Mächtigkeit von $\mathrm{Bij}([n], A)$ bestimmen, wobei für zwei Mengen X und Y

$$\mathrm{Bij}(X, Y) \stackrel{\text{def}}{=} \{\phi \in \mathrm{Abb}(X, Y) \mid \phi \text{ bijektiv}\}$$

für die Menge aller Bijektionen von X nach Y steht.

Lemma 6.8. *Es seien A und B nicht-leere Mengen mit n Elementen. Dann ist die Anzahl der Anordnungen der Elemente von A und B gleich. In anderen Worten*

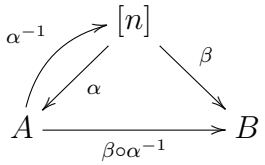
$$|\mathrm{Bij}([n], A)| = |\mathrm{Bij}([n], B)| \ .$$

Für den Anfang reicht es, die Beweisidee in den ersten zwei Sätzen zu verstehen.

Beweis: Wir zeigen, dass eine Bijektion zwischen den Mengen $\mathrm{Bij}([n], A)$ und $\mathrm{Bij}([n], B)$ existiert, weshalb diese die gleiche Anzahl an Elementen haben müssen. Da A und B beide n Elemente besitzen, existieren Bijektionen $\alpha\colon [n] \to A$ und $\beta\colon [n] \to B$. Dann ergibt die Verkettung

$$\beta \circ \alpha^{-1}\colon A \longrightarrow B$$

eine Bijektion von A nach B. Diese Situation können wir im folgenden Diagramm illustrieren:



Sei jetzt eine Bijektion $\phi \in \mathrm{Bij}([n], A)$ gegeben. Die Verkettung mit $\beta \circ \alpha^{-1}$ ergibt eine Bijektion von $[n]$ nach B. Das heißt, wir erhalten eine Abbildung f zwischen den Mengen

$$\begin{array}{rccl} f\colon \mathrm{Bij}([n], A) & \stackrel{(\beta\circ\alpha^{-1})\circ}{\longrightarrow} & \mathrm{Bij}([n], B) \\ \phi & \mapsto & (\beta \circ \alpha^{-1}) \circ \phi \ . \end{array}$$

Man stellt fest, dass

$$\begin{array}{rccl} g\colon \mathrm{Bij}([n], B) & \stackrel{(\alpha\circ\beta^{-1})\circ}{\longrightarrow} & \mathrm{Bij}([n], A) \\ \psi & \mapsto & (\alpha \circ \beta^{-1}) \circ \psi \ . \end{array}$$

die inverse Abbildung liefert, das heißt

$$g \circ f = \mathrm{id}_{\mathrm{Bij}([n]),A} \quad \text{and} \quad f \circ g = \mathrm{id}_{\mathrm{Bij}([n],B)} \ .$$

Damit haben wir gesehen, dass f bijektiv ist. □

Bemerkung 6.9. Eine Konsequenz von Lemma 6.8 ist, dass es für jede positive ganze Zahl n genügt, die Anzahl der Permutationen einer konkreten Menge mit n Elementen auszurechnen. Wir treffen die (willkürliche) Wahl die Anzahl der Permutationen von $[n]$ bestimmen.

Hausaufgabe 6.10. *Es sei A eine endliche Menge. Zeige, dass die Anzahl der Permutationen von A gleich der Mächtigkeit von $\mathrm{Bij}(A, A)$ ist.*

Beispiel 6.11. Zuerst betrachte wir die Menge $[1]$. Es gibt eine Anordnung: 1, die der Indentität $\mathrm{id}_{[1]} \in \mathrm{Bij}([1], [1])$ entspricht. Als Nächstes nehmen wir die Menge $[2] = \{1, 2\}$. Es gibt zwei Anordnungen: $1, 2$ und $2, 1$. Die entsprechen der Bijektionen $1 \mapsto 1, 2 \mapsto 2$ und $1 \mapsto 2, 2 \mapsto 1$.

Der nächte Schritt ist die Menge $[3] = \{1, 2, 3\}$. Wir werden hier rekursiv vorgehen. Auf die erste Stelle können drei Zahlen kommen:1, 2, 3. Sobald die erste Zahl festgelegt wurde, bleiben zwei, die wie oben in zwei verschiedenen Reihenfolgen geschriebene werden können. Das ergibt

$$3 \cdot 2 \ = \ 6$$

Möglichkeiten. Man sollte hier feststellen, dass zwei Anordnungen unterschiedlich sind, wenn sie am Platz Eins verschieden sind, oder wenn sie am Platz Eins übereinstimmen, aber dann die Zahlen an den letzten zwei Stellen umgekehrt stehen.

Definition 6.12. Es sei n eine natürliche Zahl. Man definiert $n!$ (n Fakultät) in der folgenden Art und Weise:

$$0! \stackrel{\text{def}}{=} 1 \ , \ n! \ = \ n \cdot (n-1)! \text{ für alle } n \geq 1.$$

In anderen Worten ist $n! = 1 \cdot 2 \cdot \ldots \cdot n$, wenn $n \geq 1$.

(A) **6.13.** *Berechnen Sie die Werte von $n!$ für $n = 0, 1, 2, 3, 4, 5, 6, 7$ und lernen Sie diese auswendig.*

Aussage 6.14. *Eine endliche Menge mit n Elementen hat $n!$ Permutationen.*

(A) **6.15.** *Bestimmen Sie alle $4! = 24$ Permutationen der Menge $\{q, w, e, r\}$ mit Hilfe der rekursiven Methode aus Beispiel 6.11.*

Beweis: Wir beweisen die Aussage durch vollständige Induktion. Für den Induktionsanfang sehen wir, dass die Aussage für $n = 1$ stimmt, das heißt,

$$|\operatorname{Bij}([1], [1])| \ = \ 1 \ = \ 1! \ .$$

Für den Induktionsschluss nehmen wir an, dass die Anzahl von Permutationen von $[n]$, nämlich $|\operatorname{Bij}([n], [n])|$, gleich $n!$ ist.

Es sei jetzt $\phi \in \operatorname{Bij}([n+1], [n+1])$, in anderen Worten ist $\phi\colon \{1, \ldots, n+1\} \to \{1, \ldots, n+1\}$ eine Bijektion. Für den Wert von $\phi(1)$ haben wir die $n + 1$ Möglichkeiten $1, 2, \ldots, n + 1$. Unterschiedliche Werte von $\phi(1)$ liefern automatisch unterschiedliche Abbildungen, und auf den verbleibenden n Stellen haben wir n Möglichkeiten. Nach der Induktionssannahme ist die Anzahl der Möglichkeiten für $\phi(2), \ldots, \phi(n + 1)$ genau $n!$, und damit ist

$$|\operatorname{Bij}([n + 1], [n + 1])| \ = \ (n + 1) \cdot n! \ = \ (n + 1)! \ .$$

□

Hausaufgabe 6.16. *Im Bücherschrank gibt es 25 Bücher. Wie viele Möglichkeiten gibt es diese aufzustellen, wenn wir wissen, dass das erste Buch 'Das Lied von Feuer und Eis Band 1.' und das letzte Buch 'Das Lied von Feuer und Eis Band 2.' sein muss?*

Jetzt, nachdem wir Permutationen kennengelernt haben, können wir zu unserer Leitfrage zurückkommen. Die Frage, wie viele Möglichkeiten es gibt, um 6 Zahlen aus 49 auszuwählen ist ein Spezialfall von der Folgenden.

Frage 6.17. *Es sei A eine endliche Menge mit n Elementen, und es sei $0 \leq k \leq n$ eine ganze Zahl. Wie viele Teilmengen mit k Elementen hat A?*

(A) **6.18.** *Beantworten Sie die Frage für die Fälle $A = \{a, b\}$ und $k = 0, 1, 2$.*

Ⓐ **6.19.** *Was passiert wenn A eine beliebige endliche Menge ist, und $k = 0$, $k = 1$, oder $k = |A|$ ist?*

Beispiel 6.20. Sei $A = \{d, e, f\}$. Der einzige nicht-triviale Fall ist $k = 2$. Folgende Mengen sind alle 2-elementigen Teilmengen von A:

$$\{d, e\}, \{d, f\}, \{e, f\}$$

Definition 6.21. Es sei A eine endliche Menge, k eine natürliche Zahl. Wir schreiben

$$\binom{A}{k} \stackrel{\text{def}}{=} \{X \subseteq A \mid |X| = k\} ,$$

das heißt, $\binom{A}{k}$ steht für die Menge aller Teilmengen von A mit k Elementen. Eine Untermenge von A mit k Elementen heißt eine *k-elementige Kombination der Elemente von A*.

Wie in Lemma 6.8 werden wir zunächst sehen, dass die Anzahl der k-elementigen Kombinationen einer Menge A nur von $|A|$ und nicht von der Menge A selbst abhängt.

Lemma 6.22. *Es seien A und B endliche Mengen mit $|A| = |B|$, $0 \leq k \leq |A|$ eine ganze Zahl. Dann gilt*

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

Beweis: Folgt aus Lemma 6.22

□

Wegen des Lemmas ist die folgende Definition sinnvoll.

Definition 6.23. Für eine natürliche Zahl n und eine natürliche Zahl $0 \leq k \leq n$ definieren wir

$$\binom{n}{k} \stackrel{\text{def}}{=} \left|\binom{[n]}{k}\right| .$$

Für alle andere ganze Zahlen setzen wir einfach $\binom{n}{k} = 0$. Die Zahlen $\binom{n}{k}$ heißen *Binomialkoeffizienten*.

Ⓐ **6.24.** *Berechnen Sie die folgenden Binomialkoeffizienten*

$$\binom{0}{0} , \binom{1}{0} , \binom{4}{2} , \binom{6}{3} .$$

Hausaufgabe 6.25. *Berechnen Sie alle Binomialkoeffizienten $\binom{n}{k}$ mit $n \leq 5$ und lernen Sie diese auswendig.*

Bemerkung 6.26. Obwohl wir den genauen Wert noch nicht kennen, ist $\binom{n}{k}$ die Anzahl der k-elementigen Teilmengen einer Menge mit n Elementen. In anderen Worten, die Anzahl der Möglichkeiten um k Objekte aus n Objekten zu wählen.

Hausaufgabe 6.27. *Beweisen Sie, dass die Anzahl der Möglichkeiten, um zwei Bälle aus n Bällen auszuwählen $\frac{n(n-1)}{2}$ ist.*

Aussage 6.28. *Es sei n eine positive ganze Zahl, $0 \leq k \leq n$ eine ganze Zahl. Dann gilt*

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

Beweis: Die Frage ist also: Wie viele Teilmengen mit k Elementen gibt es in $[n] = \{1, 2, \ldots, n\}$? Man stellt fest, dass es $n(n-1)\cdot\ldots\cdot(n-k+1)$ Möglichkeiten gibt um k *angeordnete* Elemente aus $[n]$ zu wählen (wir haben n Möglichkeiten für Platz Eins, dann $n-1$ Möglichkeiten für Platz Zwei, und so weiter).

Jede solche Auswahl bestimmt eine Teilmenge mit k Elementen (wir vergessen einfach die Reihenfolge) und jede Teilmenge mit k Elementen wird mindestens einmal auftauchen. Das Problem ist, dass die Teilmengen mehrmals vorkommen werden (zum Beispiel $1, 2, 3$ und $3, 1, 2$ beide führen zur Menge $\{1, 2, 3\}$).

Aber jede Teilmenge mit k Elementen kommt genau $k!$-fach vor, daher die Lösung

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

□

(A) **6.29.** *Berechnen Sie die Binomialkoeffizienten $\binom{100}{3}$ und $\binom{50}{2}$.*

Hausaufgabe 6.30. *Lösen Sie die Leitfrage des Abschnittes, indem Sie die Anzahl der Möglichkeiten für die Auswahl von 6 Zahlen aus 49 bestimmen.*

Hausaufgabe 6.31. *In einem Korb befinden sich 25 Äpfel. Wie viele Möglichkeiten gibt es, 4 Äpfel auszuwählen, wenn wir die 4 verfaulten vermeiden möchten?*

6.3. **Binomialkoeffizienten und Newton's binomische Formel.** Hier werden wir weitere Eigenschaften von Binomialkoeffizienten kennenlernen und eine wichtige Anwendung zeigen, bei welcher diese natürlich auftreten, nämlich Newton's binomische Formel.

Bemerkung 6.32. Wenn man mit Binomialkoeffizienten arbeitet, gibt es zwei verschiedene Arten über diese nachzudenken:

(1) Man kann entweder mit der Formel von Aussage 6.28 arbeiten: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$,
(2) oder man kann ihre definierende Eigenschaft benutzen: $\binom{n}{k}$ ist die Anzahl der Möglichkeiten k Objekte aus n Objekten herauszusuchen.

Beide Denkweisen sind gleich wichtig, manchmal funktioniert die eine besser, manchmal die andere. Um diesen Ansatz zu illustrieren, geben wir oft zwei Beweise.

Lemma 6.33. *Es seien $0 \leq k \leq n$ ganze Zahlen. Dann gelten*

$$\binom{n}{0} = \binom{n}{n} = 1 \quad \textit{und} \quad \binom{n}{1} = \binom{n}{n-1} = n .$$

Beweis:

Erste Methode: Aus der Formel von Aussage 6.28 erhalten wir

$$\binom{n}{0} = \frac{n!}{0!n!} = 1 , \quad \binom{n}{n} = \frac{n!}{n!0!} = 1 ,$$

und

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

wie behauptet.

Zweite Methode: Eine Menge A mit n Elementen hat genau eine Teilmenge mit keinem Element, nämlich die leere Menge. Außerdem hat A genau eine Teilmenge mit n Elementen, nämlich A selbst (hier haben wir ausgenutzt, dass A endlich ist).

Eine Teilmenge mit einem Element entspricht einem Element von A, daher ist ihre Anzahl gleich $|A|$. Teilmengen mit $|A|-1$ Elementen entsprechen bijektiv den Teilmengen mit 1 Element via der Abbildung

$$\begin{array}{ccc} \binom{A}{n-1} & \longrightarrow & \binom{A}{1} \\ X & \mapsto & A \setminus X \ , \end{array}$$

wobei X eine Teilmenge von A ist. Insbesondere muss $\binom{n}{n-1} = \binom{n}{1}$ sein.

□

Bemerkung 6.34. Sei A eine beliebige endliche Menge, $0 \leq k \leq |A|$ eine ganze Zahl. Dann ist die Abbildung

$$\begin{array}{ccc} \binom{A}{k} & \longrightarrow & \binom{A}{n-k} \\ X & \mapsto & A \setminus X \end{array}$$

bijektiv. Die Idee hinter dieser Bijektion ist, dass die Wahl von k Elementen das gleiche ist wie die übrigebliebenen $n-k$ Elemente *nicht* auszuwählen.

Es folgt, dass

$$\binom{n}{k} = \binom{n}{n-k}$$

(A) **6.35.** *Füllen Sie die Details von Bemerkung 6.34 aus, indem Sie explizit die Bijektivität nachweisen. Geben Sie außerdem ein alternatives Argument für die Bijektivität an, indem Sie Aussage 6.28 verwenden.*

Aussage 6.36. *Es sein $n, k \in \mathbb{N}$, $k \leq n$. Dann gilt*

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

Beweis:

Erste Methode: Wir werden die rechte Seite ausrechnen und sehen, dass sie gleich $\binom{n}{k} = \frac{n!}{k!(n-k!)}$ ist:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} + \frac{(n-1)!}{k!((n-1)-k)!} \\
&= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} \\
&= \frac{(n-1)!}{k!(n-k)!}\frac{k}{1} + \frac{(n-1)!}{k!(n-k)!} \cdot \frac{n-k}{1} \\
&= \frac{(n-1)!(k+(n-k))}{k!(n-k)!} \\
&= \frac{n!}{k!(n-k)!} = \binom{n}{k}.
\end{aligned}$$

Zweite Methode: Wir möchten die Anzahl der Möglichkeiten bestimmen, um k Elemente aus der Menge $[n]$ auszuwählen. Dazu wählen wir ein fixes Elemente aus, sagen wir 1. Dann gibt es $\binom{n-1}{k-1}$ Teilmengen, die k Elemente haben, darunter die 1, und es gibt $\binom{n-1}{k}$ Teilmengen mit k Elementen, die die 1 *nicht* enthalten.

□

A **6.37.** *Überprüfen Sie das Ergebnis der Aussage 6.36 für den Fall $n = 5$ und $k = 3$.*

Hausaufgabe 6.38. *In dieser Aufgabe werden Sie den zweiten Beweis von Aussage 6.36 formalisieren. Sei A eine nicht-leere endliche Menge, $1 \leq k \leq |A| = n$ eine ganze Zahl, $a \in A$ ein beliebiges Element.*

(1) *Geben Sie Bijektionen*

$$\begin{aligned}
\binom{[n-1]}{k-1} &\longrightarrow \{X \cup \{a\} \mid a \notin X, X \subseteq A, |X| = k-1\} \quad \textit{und} \\
\binom{[n-1]}{k} &\longrightarrow \{X \subseteq A \mid a \notin X, |X| = k\}
\end{aligned}$$

an, und finden Sie diese Mengen im zweiten Beweis von Aussage 6.36.

(2) *Beweisen Sie, dass*

$$\binom{A}{k} = \{X \cup \{a\} \mid X \subseteq A \setminus \{a\}\, X \subseteq A\,, |X| = k-1\} \coprod \{X \subseteq A \mid a \in X\,, |X| = k\}$$

gilt. Dabei bezeichnet $\coprod$ die disjunkte Vereinigung von Mengen.

(3) *Führen Sie einen vollständigen formalen Beweis von Aussage 6.36.*

Bemerkung 6.39. Es seien a und b beliebige reelle Zahlen. Dann gelten

(1) $(a+b)^2 = (a+b) \cdot (a+b) = a^2 + 2ab + b^2$, und
(2) $(a+b)^3 = (a^2+ab+b^2)(a+b) = a^3 + 3a^2b + 3ab^2 + b^3$.

A **6.40.** *Rechnen Sie aus:* $(3x+7y)^2$,$(2a-b)^3$.

Satz 6.41 (Newton's binomische Formel)**.** *Es sei n eine natürliche Zahl, $a, b \in \mathbb{R}$. Dann gilt*

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

Beweis:

Erste Methode: Wir kombinieren die explizite Rechnung mit vollständiger Induktion.

$$\begin{aligned}
(a+b)^n &= (a+b)^{n-1} \cdot (a+b) \\
&= \left(\sum_{j=0}^{n-1} \binom{n-1}{j} a^j b^{n-j} \right) \cdot (a+b) \\
&= \sum_{j=0}^{n-1} \binom{n-1}{j} a^{j+1} b^{n-j} + \sum_{j=0}^{n-1} \binom{n-1}{j} a^j b^{n-j+1} \\
&\overset{l=j+1}{=} \sum_{l=1}^{n} \binom{n-1}{l-1} a^l b^{n-l+1} + \sum_{j=0}^{n-1} \binom{n-1}{j} a^j b^{n-j+1} \\
&= \left(a^n + \sum_{l=1}^{n-1} \binom{n-1}{l-1} a^l b^{n-l+1} \right) + \left(\sum_{j=1}^{n-1} a^j b^{n-j+1} + b^n \right) \\
&= a^n + \sum_{j=1}^{n-1} \left(\binom{n-1}{k-1} + \binom{n-1}{k} \right) a^k b^{n-k} + b^n \\
&= a^n + \sum_{j=1}^{n-1} \binom{n}{k} a^k b^{n-k} + b^n \\
&= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} ,
\end{aligned}$$

wie gewünscht.

Zweite Methode: Das Produkt

$$(a+b)^n = (a+b) \cdot \ldots \cdot (a+b)$$

ergibt eine Summe von Termen der Form $a^k b^{n-k}$. Die Frage ist, wie die Koeffizienten dieser Terme aussehen. Negative Koeffizienten gibt es keine, da wir lediglich aufzählen müssen, wie oft ein Term $a^k b^{n-k}$ auftaucht. Jeder solcher Term kommt genau so oft vor, wie man k Faktoren (aus welchen wir a wählen) aus n Faktoren auswählen kann. Das ist $\binom{n}{k}$.

□

A 6.42. *Gehen Sie den induktiven Beweis für $n = 4$ durch.*

Das nachfolgende Korollar liefert einen weiteren Beweis für Satz 5.10.

Korollar 6.43. *Sei n eine natürliche Zahl. Dann ist*

$$\sum_{i=0}^{n} \binom{n}{i} = \binom{n}{0} + \ldots + \binom{n}{n} = 2^n .$$

Insbesondere hat eine endliche Menge A mit n Elementen genau 2^n Teilmengen.

Beweis:

Erste Methode: Das ist eine schnelle Konsequenz des binomischen Satzes mit einem Trick. Der Beweis beruht darauf, in der binomischer Formel a und b clever zu wählen. In unserem Fall setzen wir $a = 1$ und $b = 1$ ein, dann folgt

$$2^n \;=\; (1+1)^n \;=\; \sum_{k=0}^{n} \binom{n}{k} 1^k \cdot 1^{n-k} \;=\; \sum_{k=0}^{n} \binom{n}{k} \;,$$

wie gewünscht.

Die zweite Aussage folgt aus der folgenden Bemerkung: Jede Teilmenge von A ist eine Teilmenge mit k Elementen für genau ein $0 \leq k \leq n$. Es folgt, dass

$$\mathscr{P}(A) \;=\; \coprod_{k=0}^{n} \binom{A}{k} \tag{6.1}$$

und somit

$$|\mathscr{P}(A)| \;=\; \left|\coprod_{k=0}^{n} \binom{A}{k}\right| \;=\; \sum_{k=0}^{n} \left|\binom{A}{k}\right| \;=\; \sum_{k=0}^{n} \binom{n}{k} \;=\; 2^n \;. \tag{6.2}$$

Zweite Methode: Hier argumentieren wir umgekehrt, und benuten, dass wir schon wissen, dass $|\mathscr{P}(A)| = 2^{|A|} = 2^n$ ist. Dann ist laut (6.1) und (6.2)

$$2^n \;=\; |\mathscr{P}(A)| \;=\; \sum_{k=0}^{n} \left|\binom{A}{k}\right| \;=\; \sum_{k=0}^{n} \binom{n}{k} \;.$$

□

Hausaufgabe 6.44. *Beweisen Sie (mit dem Trick aus Korollar 6.43), dass für jede natürliche Zahl n*

$$\sum_{k=0}^{n} 2^k \binom{n}{k} \;=\; 3^n$$

gilt.

6.4. Übungsaufgaben.

Hausaufgabe 6.45. *Im Obstladen gibt es 25 Orangen, von denen 5 in keinem guten Zustand sind. Wie viele Möglichkeiten gibt es 5 Orangen auszuwählen, so dass höchstens 1 davon schlecht ist?*

Hausaufgabe 6.46. *Lösen Sie die Gleichung*

$$\frac{(n+1)!}{(n-1)!} \;=\; 90$$

für $n \in \mathbb{N}$.

Hausaufgabe 6.47. *Wie viele Hände gibt es in Bridge, wenn eine Hand aus 13 Karten besteht, die aus 52 Karten gewählt werden?*

Hausaufgabe 6.48. *Beweisen Sie die folgenden Identitäten (mit beiden Methoden):*

(1)
$$n \cdot \binom{n-1}{k-1} \;=\; k \cdot \binom{n}{k} \;=\; (n-k+1) \cdot \binom{n}{k-1}$$

(2)
$$\binom{n+k}{2} \;=\; \binom{n}{2} + nk + \binom{k}{2} \;.$$

6.5. **Wiederholungsaufgaben.**

Hausaufgabe 6.49. *Man betrachte zwei Lotterievarianten: Bei der Ersten werden 5 Zahlen aus 90 gezogen, bei der Zweiten 7 Zahlen aus 36. Bei welchem Spiel hat man bessere Chancen?*

Hausaufgabe 6.50. *Sei n eine natürliche Zahl. Zeigen Sie, dass*

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k} = \binom{n}{0} - \binom{n}{1} \pm \ldots + (-1)^n\binom{n}{n} = 0 \ .$$

(Rechnen Sie zunächst die Fälle $n = 2, 3, 4$ aus.) Wenn es geht, machen Sie Beweise mit beiden Methoden.

Hausaufgabe 6.51. *Beweisen Sie die Gleichung*

$$\sum_{k=0}^{m}\binom{n+k}{k} = \binom{n+m+1}{m} \ ,$$

wobei $m, n \in \mathbb{N}$.

Hausaufgabe 6.52. *Seien m, n positive natürliche Zahlen. Bestimmen Sie die Anzahl der injektiven Abbildungen $[m] \to [n]$.*

6.6. **Weiterführende Literatur.**

(1) Fritsche: Mathematik für Einsteiger

7. Teilbarkeit I. (Division mit Rest und Modulo Arithmetik)

7.1. **Wiederholung.** Alles, was Sie über Teilbarkeit in der Schule gelernt haben, Newton's binomische Formel, vollständige Induktion.

7.2. **Definition und einfache Eigenschaften von Teilbarkeit.** Für diesen Abschnitt gilt: Wenn wir „Zahl" sagen, meinen wir immer eine ganze Zahl. Ansonsten sagen wir „rationale Zahl" oder „reelle Zahl", je nachdem, was wir meinen.

Leitfrage. *Es seien a und b ganze Zahlen. Gibt es einen Zusammenhang zwischen dem größten gemeinsamen Teiler und dem kleinsten gemeinsamen Vielfachen von a und b? Wir werden sehen, dass gilt:*

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

Leitfrage. *Es sei n eine ganze Zahl. Wie kann man beweisen, dass $5|n^5-n$ immer zutrifft?*

(A) **7.1.** *Welche der folgenden Zahlen sind durch* 2,3, *oder* 5 *teilbar:* 64, 128, 96, 111, 576, 1000, 1001 *?*

Der Begriff der Teilbarkeit beruht auf der multiplikativen Struktur der natürlichen oder ganzen Zahlen.

Definition 7.2 (Teilbarkeit)**.** Es seien $a,b\in\mathbb{Z}$. Man sagt '*a teilt b*' oder '*b ist durch a teilbar*', falls es eine ganze Zahl c gibt, für welche $b=ac$ ist. In diesem Fall schreiben wir $a|b$.

(A) **7.3.** *Finden Sie eine geeignete Zahl c in den Beispielen von 7.1.*

Bemerkung 7.4. Es seien a und b ganze Zahlen. Dann gilt $a|b$ genau dann, wenn $(-a)|b$, weil aus $b=ca$ sofort $b=(-c)(-a)$ folgt. Aus diesem Grund studieren wir oft nur die positiven Teiler.

Lemma 7.5. *Es seien $a,b,c\in\mathbb{Z}$. Es gelten die folgenden Eigenschaften.*

(1) *Falls $a|b$ und $b|c$, dann $a|c$.*
(2) *Aus $a|b$ und $a|c$ folgt $a|(b+c)$.*
(3) *Aus $a|b$ und c beliebig folgt $a|bc$.*
(4) *Aus $a|b$ und $c|d$ folgt $ac|bd$.*

Beweis:

(1) Per Definition folgt aus $a|b$ die Existenz einer ganzen Zahl d mit $b=ad$. Analog folgt aus $b|c$ die Existenz einer ganzen Zahl e mit $c=eb$. Dann gilt aber
$$c \;=\; eb \;=\; e(da) \;=\; (ed)a\ ,$$
daher $a|c$.
(2) Nach der Definition der Teilbarkeit existieren Zahlen d,e mit $b=da$ und $c=ea$. Dann folgt
$$b+c \;=\; da+ea \;=\; (d+e)a$$
und somit $a|b+c$.

(3) Nach der Definition der Teilbarkeit gibt es eine Zahl d, sodass $b = da$. Dann gilt
$$bc \;=\; (da)\cdot c \;=\; (dc)a \;,$$
in anderen Worten, $a|bc$.
(4) Unser Argument ist sehr ähnlich zu (3): Es gibt Zahlen e, f so dass $b = ea$ und $d = fc$. Dann
$$bd \;=\; (ea)\cdot(fc) \;=\; (ef)\cdot(ac)$$
und somit $ac|bd$.

□

Korollar 7.6. *Es seien d, a, b ganze Zahlen, so dass $d|a$ und $d|b$. Dann gilt auch $d|a-b$.*

Beweis: Aus $d|b$ folgt $d|-b$. Dann können wir Teil (ii) von Lemma 7.5 benutzen, welches ergibt
$$d|a+(-b) \;=\; a-b \;.$$

□

Bemerkung 7.7. Nach unserer Definition ist 0 durch jede Zahl teilbar, aber 0 selbst teilt keine andere Zahl außer sich selbst.

Bemerkung 7.8. Jede Zahl n ist wegen $n = 1\cdot n$ durch ± 1 und $\pm$ sich selbst teilbar.

Hausaufgabe 7.9. *Es seien $a, b_1, \ldots, b_m, c_1, \ldots, c_m \in \mathbb{N}$. Falls $a|b_1, \ldots, b_m$, dann gilt*
$$a \,|\, \sum_{i=1}^{m} b_i c_i \;.$$

(A) **7.10.** *Wie viele* 0*-en hat die Zahl 10! am Ende?*

Hausaufgabe 7.11. *Welche zweistelligen Zahlen haben die*
(1) *meisten*
(2) *wenigsten*
Teiler?

Hausaufgabe 7.12. *Wie viele* 0*-en stehen am Ende der Zahl* 20!*?*

Beispiel 7.13. In diesem Beispiel zeigen wir, das $3|n^2-1$, falls n nicht durch 3 teilbar ist. Eine solche Zahl lässt sich in der Form $n = 3k \pm 1$ schreiben. Dann gilt
$$n^2 - 1 \;=\; (3k\pm 1)^2 - 1 \;=\; (9k^2 \pm 6k + 1) - 1 \;=\; 3(3k^2 \pm 2k) \;,$$
was offensichtlich durch 3 teilbar ist.

Wenn $3|n$, dann gilt natürlich $3|n^2$, sogar $9|n^2$. Eine interessante Konsequenz ist, dass n^2-2 nie durch 3 teilbar sein kann.

Hausaufgabe 7.14. *Führen Sie die obige Analyse für Teilbarkeit durch* 5 *aus und stellen Sie fest, dass* $5 \not| n^2 \pm 2$.

Beispiel 7.15. Wir werden zeigen, dass sogar $8|n^2-1$ für jede ungerade Zahl n gilt. Es sei also n eine ungerade Zahl, das heißt, wir können n in der Form $n = 2k+1$ schreiben für eine ganze Zahl k. Dann ist
$$n^2 \;=\; (2k+1)^2 \;=\; 4k^2 + 4k + 1 \;=\; 4k(k+1) + 1$$

und somit

$$n^2 - 1 \;=\; 4k(k+1)\ .$$

Man stellt fest, dass entweder k oder $k+1$ gerade ist, und daher $2|k(k+1)$. Dann folgt mit

$$8 \,|\, 4 \cdot k(k+1) \;=\; n^2 - 1\ ,$$

wie versprochen.

A 7.16. *Welche Eigenschaft(en) der Teilbarkeit haben wir in Beispiel 7.15 benutzt?*

Die Anzahl der Teiler einer Zahl n verrät viel über die Zahl selbst. Es gibt genau eine Zahl, die nur einen positiven Teiler hat, nämlich die 1. Von Zahlen, die genau zwei positiven Teiler haben, gibt es schon jede Menge (zum Beispiel $2, 3, 5, 97$). Diese spielen eine besondere Rolle in der Mathematik.

Definition 7.17 (Primzahlen)**.** Eine Zahl $p \in \mathbb{Z}$ heißt *Primzahl*, wenn sie genau zwei positive Teiler (nämlich 1 und p) hat.

Bemerkung 7.18. Wie in der obigen Definition ersichtlich, ist die Zahl 1 *keine* Primzahl.

A 7.19. *Stellen Sie eine Liste aller Primzahlen unter* 100 *auf. Ist* 91 *prim?*

A 7.20. *Welche zweistellige Zahl hat die meisten Primteiler (das heißt Teiler, die Primzahlen sind)?*

A 7.21. *Finden Sie Zahlen, die genau* 3,4, *oder* 5 *Teiler haben!*

Lemma 7.22. *Es seien $a, b \in \mathbb{Z}$ mit $a|b$. Dann ist entweder $b = 0$ oder $|a| \leq |b|$.*

Beweis: Falls $b = 0$, dann gibt es nichts zu tun. Wir können daher in aller Ruhe annehmen, dass $b \neq 0$. Wegen $a|b$ existiert $c \in \mathbb{Z}$ mit $b = ac$ so, dass $a, c \neq 0$ sind. Es gilt dann

$$|b| \;=\; |ac| \overset{3.17}{=} |a| \cdot |c| \geq |a|\ ,$$

da $|c| \geq 1$ ist. □

Korollar 7.23. *Eine Zahl $n \neq 0$ hat nur endlich viele Teiler.*

Beweis: In der Tat muss jeder Teiler k von n wegen Lemma 7.22 betragsmäßig zwischen 0 und n liegen. □

Definition 7.24 (Größter gemeinsamer Teiler)**.** Es seien $a, b \in \mathbb{Z}$. Der *größte gemeinsame Teiler* oder $\mathrm{ggT}(a, b)$ von a und b ist wie folgt definiert: Falls $a = b = 0$, dann setzen wir

$$(a, b) \overset{\text{def}}{=} \mathrm{ggT}(a, b) \overset{\text{def}}{=} 0.$$

Falls $a \neq 0$ oder $b \neq 0$, dann

$$(a, b) \overset{\text{def}}{=} \mathrm{ggT}(a, b) \overset{\text{def}}{=} \max\{d \mid d|a \text{ und } d|b\}\ .$$

A 7.25. *Berechnen Sie die folgenden größten gemeinsamen Teiler:* $(24, 0)$,$(0, 24)$,$(7, 11)$,$(34, 35)$, $(24, 25)$,$(24, 36)$, $(80, 100)$.

(A) **7.26.** *Es sei m eine ganze Zahl. Berechne Sie die folgenden größten gemeinsamen Teiler:* $(m, 2m)$,$(m, 3m)$.

Lemma 7.27. *Es sei m eine beliebige ganze Zahl. Dann gilt $(m, m+1) = 1$.*

Beweis: Betrachten wir einen beliebigen gemeinsamen Teiler d von m und $m+1$. Damit wissen wir, dass $d|m$ und $d|m+1$. Es folgt aus Korollar 7.6 (mit der Wahl $a \stackrel{\text{def}}{=} m+1$ und $b \stackrel{\text{def}}{=} m$), dass dann auch $d|(m+1) - m = 1$ gilt.

Insbesondere sind die einzigen gemeinsamen Teiler von m und $m+1$ genau ± 1, daher die Aussage. □

Lemma 7.28. *Es seien $a, b \in \mathbb{Z}$ und n eine positive ganze Zahl. Es gelten die folgenden Eigenschaften:*

(1) $(a, b) = (b, a)$,
(2) $(a, 0) = |a|$,
(3) $(a, b) = (a, -b)$.

Beweis:

(1) Diese Aussage folgt sofort aus der Symmetrie der Definition des größten gemeinsamen Teilers.
(2) Da 0 von allen Zahlen geteilt wird, sind die gemeinsamen Teiler von 0 und a einfach die Teiler von a. Unter diesen ist $|a|$ der Größte.
(3) Die gemeinsamen Teiler von a und b sind genau die gemeinsamen Teiler von a und $-b$.

□

Lemma 7.29. *Es seien $a, b \neq 0$ positive ganze Zahlen mit $a|b$. Dann gilt $(a, b) = a$.*

Beweis: Da jeder Teiler d von a die Eigenschaft $|d| \leq a$ hat, stimmt das auch für alle gemeinsame Teiler von a und b. Insbesondere gilt

$$\text{ggT}(a, b) \leq a \ .$$

Anderseits ist a per Annahme ein gemeinsamer Teiler von a und b, daher

$$a \leq \text{ggT}(a, b) \ .$$

Es muss also $a = \text{ggT}(a, b)$ sein. □

(A) **7.30.** *Was passiert im obigen Lemma, wenn a oder b gleich 0 sind?*

Lemma 7.31. *Es seien $a, b \in Z$ und n sei eine natürliche Zahl. Dann gilt*

$$(a - nb, b) = (a, b) \ .$$

Beispiel 7.32. Wir bestimmen jetzt $\text{ggT}(60, 72)$ mit der Hilfe von Lemma 7.31:

$$(60, 72) = (72, 60) = (72{-}1{\cdot}60, 60) = (12, 60) = (60, 12) = (60{-}5{\cdot}12, 12) = (0, 12) = 12 \, .$$

Beweis: Im Fall $n = 0$ ist die Aussage wegen

$$(a - nb, b) = (a - 0 \cdot b, b) = (a, b)$$

schnell zu beweisen. Für $n \geq 1$ benutzen wir vollständige Induktion als Beweismethode. Induktionsanfang: Sei $n = 1$. Wir werden zeigen, dass die Mengen der gemeinsamen Teiler

von a, b und $a - b, b$ gleich sind. Daraus folgt sofort, dass die größten Elemente dieser Mengen automatisch gleich sein müssen.

Nehmen wir an, dass $d|a$ und $d|b$, dann $d|a - b$ wegen Lemma 7.5. Das bedeutet, dass alle gemeinsame Teiler von a und b gemeinsame Teiler von $a - b$ und b sind.

Umgekehrt, wenn $d|a - b$ und $d|b$, dann $d|a$ wegen Lemma 7.5. Insbesondere sind alle gemeinsamen Teiler von $a - b$ und b zwangsweise gemeinsame Teiler von a und b.

INDUKTIONSSCHLUSS: Unsere Induktionsannahme ist, dass $(a - nb, b) = (a, b)$. Jetzt wollen wir zeigen, dass $(a - (n + 1)b, b) = (a, b)$ ebenfalls stimmt. Es gilt

$$(a - (n + 1)b, b) \;=\; ((a - nb) - b, b) \;=\; (a - nb, b) \;=\; (a, b)\ ,$$

wobei wir bei der zweiten Gleichung den Induktionsanfang mit den Rollen $a' = a - nb$ und $b' = b$ benutzt haben und bei der Dritten die Induktionsannahme. Damit sind wir fertig. □

Hausaufgabe 7.33. *Im Beweis von Lemma 7.31 können wir auch die Anwendung der vollständigen Induktion umgehen.*

Zeigen Sie, dass für eine beliebige ganze Zahl n gilt:

$$\{\textit{gemeinsame Teiler von } a - nb \textit{ und } b\} \;=\; \{\textit{gemeinsame Teiler von } a \textit{ und } b\}.$$

Beispiel 7.34. Mit dem gleichen Trick bestimmen wir jetzt $\mathrm{ggT}(144, 112)$. In diesem Fall werden wir außerdem die Regel $(a, b) = (b, a)$ benutzen, ohne sie explizit hinzuschreiben. Es gilt also

$$\begin{aligned}(144, 112) \;&=\; (144 - 112, 112) \;=\; (112, 32) \;=\; (112 - 3 \cdot 32, 32) \;=\; (32, 16)\\ &=\; 16.\end{aligned}$$

Beispiel 7.35. Im folgenden Beispiel berechnen wir $(99, 27)$. Hier werden wir nur die einzelne Schritte ohne Erklärung hinschreiben:

$$(99, 27) \;=\; (27, 18) \;=\; (18, 9) \;=\; (9, 0) \;=\; 9\ .$$

(A) **7.36.** *Geben Sie alle Details in der Rechnung von Beispiel 7.35 an, wie es in Beispiel 7.32 gemacht wurde.*

Hausaufgabe 7.37. *Berechnen Sie die folgenden größten gemeinsamen Teiler:* $(1024, 768)$, $(500, 395)$, $(128, 144)$, $(1024, 512)$.

Bemerkung 7.38. Die Methode aus Lemma 7.31 ist relativ schnell und am Wichtigsten ist: Um $\mathrm{ggT}(a, b)$ zu bestimmen, brauchen wir die Primfaktorzerlegung (siehe Satz 8.12) von a und b gar nicht zu kennen.

Definition 7.39. Es seien a, b ganze Zahlen. Das *kleinste gemeinsame Vielfache* von a und b oder $\mathrm{kgV}(a, b)$ ist

$$[a, b] \stackrel{\text{def}}{=} \mathrm{kgV}(a, b) \stackrel{\text{def}}{=} \min\{d \in \mathbb{N} \mid a|d \text{ und } b|d\}\ .$$

(A) **7.40.** *Bestimmen Sie* $\mathrm{kgV}(a, b)$ *für die folgenden Paare:* $a = 2, b = 3$*;* $a = 5, b = 7$ *und* $a = 12, b = 18$.

Definition 7.41. Zwei ganze Zahlen a und b heißen *teilerfremd*, wenn $(a, b) = 1$ ist.

Ⓐ **7.42.** *Bestimmen Sie, welche der folgenden Paare teilerfremd sind:*
$\{1,2\}$,$\{2,3\}$,$\{6,8\}$,$\{3,10\}$,$\{24,91\}$, $\{13,91\}$.

Beispiel 7.43. Es sei m eine ganze Zahl, die nicht durch 3 teilbar ist. Dann sind 3 und m teilerfremd. Ein Beweis für diese Aussage ist wie folgt: Wir müssen feststellen, dass $\mathrm{ggT}(3,m) = 1$. Die Zahl 3 hat nur zwei positive Teiler: 1 und 3, der größte gemeinsame Teiler muss also eine von diesen sein.

Die 3 kann es nicht sein, weil $3 \not| m$ nach unserer Annahme, es muss also $\mathrm{ggT}(3,m) = 1$ sein.

7.3. **Wie berechnet man** $\mathrm{ggT}(a,b)$ **(der Euklidische Algorithmus).** Die Methode, die wir in Beispielen 7.32–7.35 kennengelernt haben, lässt sich zu einer der wichtigsten Aussagen in der Zahlentheorie verallgemeinern.

Satz 7.44 (Division mit Rest)**.** *Es seien a und b ganze Zahlen mit $a \neq 0$. Dann existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ so dass*

(1) $b = qa + r$, *und*
(2) $0 \leq r \leq |a|$.

Man sagt, dass q das Ergebnis der Division mit Rest *(oder Ganzzahldivision) von b durch a ist, und r ist der* Rest *dieser Division.*

Beweis: An dieser Stelle werden wir die Aussage einfach ohne Beweis akzeptieren. Einen vollständigen Beweis findet man zum Beispiel in [?StixEZ, Satz 3.6]. □

Bemerkung 7.45. Die Idee des Beweises ist bemerkenswert einfach: Gegeben a und b subtrahieren wir einfach a von b so oft es geht, das heißt, solange der Unterschied $b - ka$ immer noch nichtnegativ ist. Dann ist der Unterschied der Rest der Division und $q = k$. Der Beweis ist die Formalisierung dieses Verfahrens mit der Feststellung der gewünschten Eigenschaften.

Beispiel 7.46. Es sei jetzt $a = 5$ und $b = 17$, wir möchten Division mit Rest durchführen.

$$\begin{aligned} 17 - \mathbf{1}\cdot 5 &= 12 > 0 \\ 12 - 5 &= 17 - \mathbf{2}\cdot 5 = 7 > 0 \\ 7 - 5 &= 17 - \mathbf{3}\cdot 5 = \mathbf{2} > 0 \\ 2 - 5 &= 17 - 4\cdot 5 = -3 < 0 \text{ zu viel abgezogen!} \end{aligned}$$

Zusammengefasst ergibt sich aus der obigen Rechnung

$$17 = 3\cdot 5 + 2\ ,$$

das heißt:

$$\begin{aligned} \text{Ergebnis der Division} &: q = 3 \\ \text{Rest der Division} &: r = 2\ . \end{aligned}$$

Ⓐ **7.47.** *Überprüfen Sie durch iterierte Subtraktion, dass*

$$79 = 11\cdot 7 + 2\ .$$

Das ist der Fall $a = 7$, $b = 79$ von Satz 7.44.

Ⓐ **7.48.** *Üben Sie Division mit Rest in den folgenden Fällen: $a = 198$, $b = 17$ und $a = 392$, $b = 19$.*

Hausaufgabe 7.49. *Es seien a und b natürliche Zahlen und es gelte $a|b$. Bestimmen Sie den Rest der Division von b durch a.*

Hausaufgabe 7.50. *Nehmen Sie drei Würfel und würfeln Sie mit diesen auf einmal. Das Produkt der drei Zahlen wird b. Jetzt würfeln Sie erneut und die Summe der drei Zahlen wird a. Machen Sie Division mit Rest für das Paar a und b.*

Bemerkung 7.51 (Modulo-Arithmetik). Sei m eine positive ganze Zahl, $a, b \in \mathbb{Z}$. Man sagt, a und b seien *kongruent modulo* m, in Zeichen

$$a \equiv b \,(\mathrm{mod}\, m),$$

falls a und b den gleichen Rest haben bei Division mit m. In anderen Worten,

$$a \equiv b \,(\mathrm{mod}\, m) \;\text{ genau dann, wenn }\; m|a-b\ .$$

Es ist interessant zu beobachten, dass für $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, aus

$$a_1 \equiv b_1 \,(\mathrm{mod}\, m) \text{ und } a_2 \equiv b_2 \,(\mathrm{mod}\, m)$$

folgt, dass

$$\begin{aligned} a_1 + a_2 &\equiv b_1 + b_2 \,(\mathrm{mod} m) \;\text{ und} \\ a_1 \cdot a_2 &\equiv b_1 \cdot b_2 \,(\mathrm{mod} m)\ . \end{aligned}$$

Hausaufgabe 7.52. *Welche der folgenden Aussagen ist richtig?*

$$17 \equiv 13 \,(\mathrm{mod}\, 4)\ ,\ 100 \equiv 19 (\mathrm{mod}\, 9)\ ,\ 99 \equiv 88 \,(\mathrm{mod}\, 7)\ .$$

Hausaufgabe 7.53. *Beweisen Sie alle Behauptungen in Bemerkung 7.51.*

Die Formalisierung der Methode von Beispielen 7.32 – 7.35 liefert den sogenannten Euklidischen Algorithmus für die Berechnung des größten gemeinsamen Teilers.

Satz 7.54 (Euklidischer Algorithmus)**.** *Es seien $0 \le a \le b$ natürliche Zahlen. Wir setzen voraus, dass $b \neq 0$ ist. Der folgende Algorithmus berechnet dann* $\mathrm{ggT}(a, b)$.

(1) *Falls $a = 0$, dann ist $(a, b) = b$, und wir sind fertig. Ansonsten weiter nach (2).*
(2) *Wir machen Division mit Rest $b = q \cdot a + r$, ersetzen*

$$b \stackrel{def}{=} a\ ,\ a \stackrel{def}{=} r$$

und gehen zurück nach (1).

Beweis: Das ist ganz konkret die Methode aus Beispielen 7.32 – 7.35. Für einen formalen Beweis siehe [?StixEZ, Satz 3.8]. □

A **7.55.** *Benutzen Sie den Euklidischen Algorithmus zur Berechnung von* $\mathrm{ggT}(768, 524)$ *und* $\mathrm{ggT}(729, 243)$.

Eine nützliche Konsequenz des Euklidischen Algorithmus ist das Lemma von Bézout. Es sagt aus, dass $\mathrm{ggT}(a, b)$ immer als Linearkombination von a und b geschrieben werden kann. Geläufiger ist die Bezeichnung *Erweiterter Euklidischer Algorithmus.*

Lemma 7.56 (Lemma von Bézout)**.** *Es seien a, b ganze Zahlen und $d = \mathrm{ggT}(a, b)$. Dann existieren ganze Zahlen x, y so dass*

$$d \;=\; ax + by\ .$$

Beweis: Siehe [?StixEZ, Lemma 3.10] □

(A) **7.57.** *Finden Sie geeignete x und y im Fall $a = 4$ und $b = 5$. Gibt es nur eine Lösung? Können wir annehmen, dass $x, y \geq 0$?*

(A) **7.58.** *Finden Sie geeignete x und y wenn $a = 6$ und $b = 4$ ist.*

Proposition 7.59. *Es seien a, b, t ganze Zahlen, man schreibe $d \stackrel{def}{=} \mathrm{ggT}(a, b)$. Es gilt dann*

$$t|d \quad \text{genau dann, wenn} \quad t|a \text{ und } t|b \ .$$

Beweis: Zunächst nehmen wir an, dass $t|d$. Wegen $d = \mathrm{ggT}(a, b)$ gilt $d|a$ und $d|b$, und die Transitivität von Teilbarkeit ergibt $t|a$ und $t|b$, wie gewollt.

Umgekehrt nehmen wir an, dass $t|a$ und $t|b$. Man benutze Lemma 7.56 um ganze Zahlen x und y zu finden, für welche

$$d \ = \ ax + by$$

gilt. Aus Lemma 7.5 (oder noch präziser, aus Hausaufgabe 7.9) folgt, dass $t|ax + by = d$, was wir behauptet haben. □

Hausaufgabe 7.60. *Es seien a, b, m ganze Zahlen mit $m \neq 0$. Beweisen Sie, dass*

$$\mathrm{ggT}(ma, mb) \ = \ |m| \cdot \mathrm{ggT}(a, b) \ .$$

Hausaufgabe 7.61. *Es seien a, b, c ganze Zahlen. Beweisen Sie, dass*

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

Damit kann man den größten gemeinsamen Teiler der drei Zahlen a, b, c als

$$\mathrm{ggT}(a, b, c) \stackrel{def}{=} \mathrm{ggT}(\mathrm{ggT}(a, b), c)$$

definieren.

(A) **7.62.** *Bestimmen Sie* $\mathrm{ggT}(36, 90, 128)$.

In Analogie zum größten gemeinsamen Teiler haben wir die folgende Eigenschaft.

Aussage 7.63. *Es seien $a, b \neq 0$ ganze Zahlen. Dann ist jedes gemeinsame Vielfache von a und b ein Vielfaches von* $\mathrm{kgV}(a, b)$.

Beweis: Wir schreiben $m \stackrel{\text{def}}{=} \mathrm{kgV}(a, b)$, wegen $a, b \neq 0$ ist ebenfalls $m \neq 0$. Weiterhin sei c ein gemeinsames Vielfaches von a und b. Die Beweisidee ist, Division mit Rest zu benutzen. Dementsprechen teilen wir c durch m mit Rest:

$$c \ = \ k \cdot m + r \ ,$$

wobei $0 \leq r < m$ gilt. Wir werden jetzt zeigen, dass $r = 0$, und somit $m|c$, wie gewollt. Aus $a|c$ und $a|m$ folgt

$$a \,|\, c - km \ = \ r \ ,$$

und aus $b|c$ und $b|m$ erhalten wir

$$b \,|\, c - km \ = \ r \ .$$

Es folgt, dass die Zahl $0 \leq r < m = \mathrm{kgV}(a, b)$ ein gemeinsames Vielfaches von a und b ist. Wir haben aber vorausgesetzt, dass $m = \mathrm{kgV}(a, b)$ das kleinste (positive) gemeinsame Vielfache von a und b ist, damit muss $r = 0$ sein und wir sind fertig. □

Proposition 7.64. *Es seien a, b, m ganze Zahlen, $m \neq 0$. Dann gilt*

$$\mathrm{kgV}(am, bm) \;=\; |m| \cdot \mathrm{kgV}(a, b) \;.$$

(A) **7.65.** *Zeigen Sie, wie man aus dem Fall $m > 0$ den allgemeinen Fall herleiten kann.*

(A) **7.66.** *Verifizieren Sie Proposition 7.64 im konkreten Fall $a = 24$,$b = 36$, $m = 5$.*

Beweis: Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $m > 0$ ist. Zunächst zeigen wir, dass $m \cdot \mathrm{kgV}(a, b)$ ein gemeinsames Vielfaches von am und bm ist. Das folgt daraus, dass $a | \mathrm{kgV}(a, b)$ und somit $am | \mathrm{kgV}(a, b) \cdot m$ und analog für b.

Jetzt müssen wir noch beweisen, dass $m \cdot \mathrm{kgV}(a, b)$ wirklich das kleinste gemeinsame Vielfache von am und bm ist. Es sei $d > 0$ ein beliebiges gemeinsames Vielfaches von am und bm. Aus $m|am|d$ folgt, dass ein $s \in \mathbb{Z}$ mit $d = sm$ existiert. Wegen $am|d = sm$ folgt $a|s$ und analog lässt sich schließen, dass $b|s$. Es folgt, dass s ein gemeinsames Vielfaches von a und b ist, insbesondere $\mathrm{kgV}(a, b) \leq s$. Aber dann gilt

$$\mathrm{kgV}(a, b) \cdot m \;\leq\; sm \;=\; d \;,$$

und weil d ein beliebiges gemeinsames Vielfaches von am und bm war, gilt auch

$$\mathrm{kgV}(a, b) \cdot m \;\leq\; \mathrm{kgV}(am, bm) \;.$$

Da auf der rechten Seite das *kleinste* gemeinsame Vielfache von am und bm steht, erhalten wir

$$\mathrm{kgV}(a, b) \cdot m \;=\; \mathrm{kgV}(am, bm) \;,$$

wie gewünscht. □

Lemma 7.67. *Es seien $a, b \neq 0$ ganze Zahlen, $d \stackrel{def}{=} \mathrm{ggT}(a, b)$. Dann existieren Zahlen $c, d \in \mathbb{Z}$ so dass $a = de$, $b = df$, und e, f teilerfremd sind.*

(A) **7.68.** *Finde geeignete Zahlen e und f wenn $a = 96$ und $b = 144$ ist. Wie viele verschieden Möglichkeiten gibt es?*

Beweis: Da $\mathrm{ggT}(a, b)|a, b$, existieren (bis auf Vorzeichen eindeutig bestimmte) Zahlen e, f so dass $a = de$ und $b = df$ gilt (insbesondere haben wir keine Freiheit in der Wahl von e und f). Wir müssen jetzt zeigen, dass $(e, f) = 1$.

Zu diesem Punkt merken wir, dass wegen $a = de$ und $b = df$ und Hausaufgabe 2.57 gilt

$$d \stackrel{\mathrm{def}}{=} \mathrm{ggT}(a, b) \;=\; \mathrm{ggT}(de, df) \;=\; d \cdot \mathrm{ggT}(e, f) \;,$$

und somit $(e, f) = 1$. □

Proposition 7.69. *Es seien a und b teilerfremde ganze Zahlen. Dann gelten die folgenden Aussagen.*

(1) *Für eine beliebige Zahl c gilt: aus $a|bc$ folgt $a|c$.*
(2) *Sei m ein gemeinsames Vielfaches von a und b. Dann gilt $ab|m$.*

Beweis: Beide Aussagen beruhen auf der selbe Beobachtung: Wenn a und b teilerfremd sind, dann existieren nach dem Lemma von Bézout $x, y \in \mathbb{Z}$ so dass

$$ax + by \;=\; 1 \;.$$

(1) Da $a|bc$, existiert $d \in \mathbb{Z}$ so dass $bc = ad$. Es folgt

$$a|a \cdot (cx + dy) \;=\; acx + ady \;=\; acx + bcy \;=\; c(ax + by) \;=\; c \;.$$

(2) Wegen $a|m$ und $b|m$ gibt es ganze Zahlen e, f so dass $m = ae$ und $m = bf$. Dann folgt

$$m \;=\; m \cdot 1 \;=\; m(ax + by) \;=\; max + mby \;=\; (bf)ax + (ae)by \;=\; ab(fx + ey) \;,$$

insbesondere $ab|m$.

□

Als Korollar werden wir sehen, dass sich das kgV von teilerfremden Zahlen ganz einfach berechnen lässt.

Korollar 7.70. *Für teilerfremde Zahlen a, b gilt*

$$\mathrm{kgV}(a, b) \;=\; |ab| \;.$$

Beweis: Aus Proposition 7.69 folgt, dass $ab|\,\mathrm{kgV}(a, b)$, insbesondere $|ab| \leq \mathrm{kgV}(a, b)$. Andererseits ist $|ab|$ ein gemeinsamer Teiler von a und b, somit $|ab| = \mathrm{kgV}(a, b)$. □

Satz 7.71. *Es seien a und b von 0 verschiedene ganze Zahlen. Dann gilt*

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) \;=\; |ab| \;.$$

Beweis: Es sei d eine gemeinsame Teiler von a und b. Dann gilt

$$\mathrm{ggT}(a, b) \;=\; \mathrm{ggT}(d \cdot a/d, d \cdot b/d) \;=\; d \cdot \mathrm{ggT}(a/d, b/d) \;,$$

und analog

$$\mathrm{kgV}(a, b) \;=\; \mathrm{kgV}(d \cdot a/d, d \cdot b/d) \;=\; d \cdot \mathrm{kgV}(a/d, b/d) \;.$$

Da

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) \;=\; d^2\,\mathrm{ggT}(a/d, b/d) \cdot \mathrm{kgV}(a/d, b/d)$$

und

$$|ab| \;=\; d^2 \cdot |a/d \cdot b/d| \;,$$

reicht es, wenn wir die Aussage für a/d und b/d beweisen (anstelle von a und b).

Diese Beobachtung gilt für jeden gemeinsamen Teiler von a und b, wir dürfen insbesondere $d \stackrel{\text{def}}{=} \mathrm{ggT}(a, b)$ einsetzen. Dann gilt

$$\mathrm{ggT}(a/d, b/d) \;=\; 1 \quad \text{und} \quad \mathrm{kgV}(a/d, b/d) \;=\; |a/d \cdot b/d| \;,$$

und daher

$$\mathrm{ggT}(a/d, b/d) \cdot \mathrm{kgV}(a/d, b/d) \;=\; 1 \cdot |a/d \cdot b/d| \;=\; |a/d \cdot b/d| \;,$$

wie gewollt. □

(A) **7.72.** *Finden Sie bei jedem Schritt des obigen Beweises, welche bereits bekannte Aussage/Aufgabe benutzt wurde.*

7.4. **Teilbarkeit und vollständige Induktion.** Teilbarkeitsfragen sind oft durch vollständige Induktion zu lösen. In diesem kurzen Abschnitt illustrieren wir diese Beweistechnik mit einer Reihe von Beispielen.

Aussage 7.73. *Es sei n eine positive ganze Zahl. Dann gilt $7|5^{2n} - 2^{2n}$.*

Beweis: INDUKTIONSANFANG: Betrachte den fall $n = 1$. Dann ist

$$5^{2\cdot 1} - 2^{2\cdot 1} \;=\; 5^2 - 2^2 \;=\; 25 - 4 \;=\; 21$$

was in der Tat durch 7 teilbar ist.
INDUKTIONSSCHLUSS: Wir nehmen an, dass wir die Aussage $7|5^{2n} - 2^{2n}$ für die Zahlen $1, \ldots, n$ bewiesen haben und untersuchen den Fall für $n + 1$. Es gilt:

$$\begin{aligned} 5^{2(n+1)} - 2^{2(n+1)} &= 5^{2n+2} - 2^{2n+2} \\ &= 25 \cdot 5^{2n} - 4 \cdot 2^{2n} \\ &= 25 \cdot 5^{2n} + 0 - 4 \cdot 2^{2n} \\ &= 25 \cdot 5^{2n} + (-25 \cdot 2^{2n} + 25 \cdot 2^{2n}) - 4 \cdot 2^{2n} \\ &= 25 \cdot (5^{2n} - 2^{2n}) + (25 - 4) \cdot 2^{2n} \; . \end{aligned}$$

Der erste Summand ist nach der Induktionsannahme durch 7 teilbar, die Zweite wegen $7|25-4 = 21$. Daher ist auch die ganze Summe durch 7 teilbar und somit auch $5^{2(n+1)} - 4^{2(n+1)}$, wie gewünscht. Damit ist die Induktion fertig. □

Ⓐ **7.74.** *Zeigen Sie mit dem Beweisschema von Aussage 7.73, dass $11|6^{2n} - 5^{2n}$.*

Hausaufgabe 7.75. *Seien a und b beliebige ganze Zahlen. Beweisen Sie, dass $a + b|a^{2n} - b^{2n}$ für jede natürliche Zahl n.*

Aussage 7.76. *Es seien a und b ganze Zahlen, n eine natürliche Zahl. Dann gilt $a - b|a^n - b^n$.*

Bemerkung 7.77. Ein kurzen Beweis erhält man mit der Identität

$$a^n - b^n \;=\; (a - b) \cdot (a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}) \; ,$$

die wir aber ebenfalls nicht bewiesen haben.

Beweis: INDUKTIONSANFANG: Wenn $n = 0$ ist gilt $a^0 - b^0 = 1 - 1 = 0$ und 0 ist durch jede ganze Zahl teilbar.
INDUKTIONSSCHLUSS: Unsere Induktionssannahme ist, dass $a - b|a^n - b^n$. Wir versuchen jetzt zu überprüfen, ob $a - b|a^{n+1} - b^{n+1}$ gilt. Hier ist unsere Rechnung:

$$\begin{aligned} a^{n+1} - b^{n+1} &= a \cdot a^n - b \cdot b^n \\ &= a \cdot a^n + 0 - b \cdot b^n \\ &= a \cdot a^n + (-a \cdot b^n + a \cdot b^n) - b \cdot b^n \\ &= a(a^n - b^n) + (a - b)b^n \; . \end{aligned}$$

Der erste Summand ist per Induktionsannahme durch $a - b$ teilbar, der zweite Summand ist offensichtlich durch $a - b$ teilbar, und somit auch die Summe. Damit sind wir fertig. □

Ⓐ **7.78.** *Beweisen Sie, dass $7|8^n - 1$ für jede positive ganze Zahl n.*

Hausaufgabe 7.79. *Beweisen Sie, dass $11|12^n + 21$.*

Aussage 7.80. *Für jede natürliche Zahl n gilt $3|n^3+2n$.*

Beweis: INDUKTIONSANFANG: Wenn $n=0$ ist, gilt

$$n^3+2n \;=\; 0^3+2\cdot 0 \;=\; 0+0 \;=\; 0\ ,$$

was durch 3 teilbar ist.
INDUKTIONSSCHLUSS: Unsere Induktionssannahme ist, dass $3|n^3+2n$. Wie gewohnt versuchen wir jetzt zu sehen, dass $3|(n+1)^3+2(n+1)$ gilt. Hier ist unsere Rechnung:

$$\begin{aligned}(n+1)^3+2(n+1) &= (n^3+3n^2+3n+1)+(2n+2)\\ &= n^3+(3n^2+3n+1)+2n+2\\ &= (n^3+2n)+3(n^2+n+1)\ .\end{aligned}$$

Der erste Summand ist nach Induktionsannahme durch 3 teilbar, der zweite offensichtlich, somit ist auch $3|(n+1)^3+2(n+1)$, und damit sind wir fertig. □

Hausaufgabe 7.81. *Beweisen Sie, dass $9|4^n+15n-1$.*

7.5. **Teilbarkeitsregel im Zehnersystem.** In diesem Abschnitt betrachten wir kurz, wie man verschiedene Teilbarkeitseigenschaften natürlicher Zahlen von ihrer Dezimaldarstellung ablesen kann. Im Zehnersystem schreibt man eine natürliche Zahl n als Ziffernfolge

$$n \;=\; (a_m, a_{m-1}, \ldots, a_1, a_0)_{10}\ ,$$

wobei die einzelnen Ziffer a_i aus der Menge $\{0,1,2,3,4,5,6,7,8,9\}$ kommen, mit der Einschränkung, dass $a_m \neq 0$ sein muss. Die Darstellung im Zehnersystem bedeutet dann

$$n \;=\; \sum_{i=0}^{m} a_i\cdot 10^i\ .$$

Bemerkung 7.82. Die Bedingung, dass $a_m\neq 0$ ist dient dazu, dass diese Darstellung eindeutig ist.

Beispiel 7.83. Als ganz konkretes Beispiel betracht wir

$$498 \;=\; 4\cdot 10^2+9\cdot 10^1+8\cdot 10^0 \;=\; (4,9,8)_{10}\ .$$

Ⓐ **7.84.** *Zerlegen Sie auf diese Weise die Zahlen* 5128 *und* 16902.

Proposition 7.85. *Es sei n eine natürliche Zahl. Dann ist n genau dann durch 2^k, 5^k oder 10^k teilbar, wenn die Zahl, die aus den letzten k Ziffern von n besteht, durch 2^k, 5^k oder 10^k teilbar ist.*

Beispiel 7.86. Der Beweis beruht auf der Idee, dass $10^m=2^m\cdot 5^m$ ist. Zum Beispiel wenn wir uns Fragen, ob $4|524$ gilt, können wir das wie folgt entscheiden:

$$524 \;=\; 500+24 \;=\; 5\cdot 10^2+24\ .$$

Es folgt, dass

$$524\equiv 24 (\mathrm{mod}\, 2^2)\ ,$$

damit haben die Zahlen 524 und 24 den gleichen Rest bei Division mit 4, insbesondere $4|524$ genau dann, wenn $4|24$, was stimmt.

Beweis: Es sein n eine positive ganze Zahl, $1 \leq k \leq m$. Dann gilt

$$\begin{aligned} n &= (a_m, a_{m-1}, \ldots, a_0)_{10} \\ &= (a_m, a_{m-1}, \ldots, a_k, 0 \ldots, 0)_{10} + (a_{k-1}, \ldots, a_0)_{10} \\ &= \sum_{i=k}^{m} a_i 10^i + (a_{k-1}, \ldots, a_0)_{10} \\ &= 10^k \cdot \sum_{i=0}^{m-k} a_{i-k} 10^i + +(a_{k-1}, \ldots, a_0)_{10} \\ &= 10^k \cdot (a_m, a_{m-1}, \ldots, a_k)_{10} + (a_{k-1}, \ldots, a_0)_{10} \\ &\equiv (a_{k-1}, \ldots, a_0)_{10} \pmod{10^k} . \end{aligned}$$

Das heißt, die Zahlen $n = (a_m, a_{m-1}, \ldots, a_0)_{10}$ und $(a_{k-1}, \ldots, a_0)_{10}$ haben den gleichen Rest bei Division mit 10^k. Insbesondere sind sie durch 10^k teilbar.

Wortwörtlich der gleiche Beweis zeigt die Teilbarkeitaussage durch 2^k und 5^k. □

(A) **7.87.** *Welche der folgenden Teilbarkeiten stimmen:* $4|618$, $125|453245243625$, $8|278$*?*

(A) **7.88.** *Schreiben Sie einen vollständigen Beweis der Teilbarkeitsbedingung durch* 2^k *auf.*

Beispiel 7.89. Um das bisher gelernte anzuwenden, möchten wir die kleinste natürliche Zahl n bestimmen, in der jede Ziffer genau einmal vorkommt und die durch 36 teilbar ist.

Wir zerlegen zunächst 36 in Primfaktoren und stellen fest, dass $36 = 4 \cdot 9 = 2^2 \cdot 3^2$. Nach der ersten Bedingung wissen wir, dass n folgende Form haben muss:

$$n = (a_9, \ldots, a_0)_{10} = \sum_{i=0}^{9} a_i 10^i,$$

wobei $a_9 \neq 0, a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ und $a_i \neq a_j$ für $i \neq j$ (das heißt die a_i sind paarweise verschieden und da es 10 verschiedene a_i gibt, muss jede Ziffer genau einmal vorkommen). Insbesondere wissen wir, dass $Q(n) = \sum_{i=0}^{9} i = 45$. Daraus schließen wir mit Proposition 7.95, dass n ohnehin durch $9 = 3^2$ teilbar ist, egal wie wir die Ziffern anordnen. Also müssen wir nur noch sicherstellen, dass $2^2 = 4 \mid n$ gewährleistet ist. Denn dann folgt, dass auch das Produkt $4 \cdot 9 = 36$ die Zahl n teilt. Nach Proposition 7.85 gilt $4 \mid n$ genau dann, wenn die Zahl $(a_1, a_0)_{10}$ durch 4 teilbar ist. Es bietet sich also an, die größte zweistellige Zahl zu suchen, die durch 4 teilbar ist. Das ist die Zahl 96. Nun müssen wir nur noch die letzten 8 Ziffern so anordnen, um die kleinstmögliche Zahl zu bekommen. Wir finden

$$n = 1023457896.$$

Hausaufgabe 7.90. *Welche Ziffer(n)* z *muss man in der Zahl* $4234z28$ *einfügen, damit diese durch* 8 *teilbar ist? Für welchen Wert von* z *ist die Zahl durch* 16 *teilbar?*

Definition 7.91 (Quersumme)**.** Es sei $n = (a_m, \ldots, a_0)_{10}$ eine positive ganze Zahl. Die *Quersumme* $Q(n)$ von n definieren wir als

$$Q(n) \stackrel{\text{def}}{=} \sum_{i=0}^{m} a_i \; = \; a_m + \ldots + a_0$$

Beispiel 7.92. Die Quersumme der Zahl 51782 ist

$$Q(51782) \;=\; 5+1+7+8+2 \;=\; 23\ .$$

(A) **7.93.** *Berechnen Sie die Quersummen der Zahlen* 7584375, 8940398509 *und* 87284300.

(A) **7.94.** *Beweisen Sie, dass* $Q(10^k \cdot n) = Q(n)$ *für alle positiven ganze Zahlen* n, k.

Zunächst betrachten wir die Teilbarkeit durch 3 und 9.

Proposition 7.95. *Es sein* n *eine positive ganze Zahl. Dann ist* n *genau dann durch* 3 *oder* 9 *teilbar, wenn* $Q(n)$ *durch* 3 *oder* 9 *teilbar ist.*

Die grundlegende Idee des Beweises ist, dass 10 und 1 den gleichen Rest modulo 3 und 9 haben. In der Notation von Bemerkung 7.51 heißt das

$$10 \equiv 1 \bmod 3 \quad \text{und} \quad 10 \equiv 1 \bmod 9\ .$$

Beweis: Wir zeigen den Beweis für Teilbarkeit durch 3, der Beweis für 9 ist wortwörtlich das Gleiche. Hier ist die Rechnung:

$$\begin{aligned} n &= (a_m, a_{m-1}, \ldots, a_0)_{10} \\ &= \sum_{i=0}^{m} a_i 10^i \\ &\equiv \sum_{i=0}^{m} a_i 1^i \mod 3 \\ &= \sum_{i=0}^{m} a_i \\ &= Q(n)\ . \end{aligned}$$

Das heißt, n und $Q(n)$ haben den gleichen Rest, wenn sie durch 3 geteilt werden. Insbesondere gilt $3|n$ genau dann, wenn $3|Q(n)$. □

(A) **7.96.** *Gehen Sie den Beweis für den Fall* $n = 1352$ *durch.*

(A) **7.97.** *Schreiben Sie einen vollständigen Beweis für Teilbarkeit durch* 9 *auf.*

Hausaufgabe 7.98. *Können wir eine Primzahl erhalten, indem wir die Ziffern* $1, 2, 3, 4, 5, 6, 7, 8$ *alle genau einmal benutzen?*

Hausaufgabe 7.99. *Betrachten wir die Zahl* $n = 12z34$*, wobei* z *eine Ziffer ist. Was kann* z *sein, wenn* n *durch* $3, 4, 6, 8, 9, 12$ *oder* 36 *teilbar ist?*

Hausaufgabe 7.100. *Bestimmen Sie alle mögliche Ziffern* z *und* y*, wenn* $36|3235z2y$.

Definition 7.101. Es sein $n = (a_m, \ldots, a_0)_{10}$ eine positive ganze Zahl. Die *alternierende Quersumme* $A(n)$ von n definieren wir als

$$A(n) \stackrel{\text{def}}{=} \sum_{i=0}^{m} (-1)^i a_i\ .$$

Beispiel 7.102. Betrachte die Zahl 64732. Ihre alternierende Quersumme ist

$$A(64732) \;=\; 2-3+7-4+6 \;=\; 8\ .$$

(A) **7.103.** *Berechnen Sie die alternierende Quersumme der Zahlen* 93853, 100001, 10001, 5438759834.

Alternierende Quersummen sind zur Charakterisierung der Teilbarkeit durch 11 nützlich.

Proposition 7.104. *Es sei n eine positive ganze Zahl. Dann gilt $11|n$ genau dann, wenn $11|A(n)$.*

Die Grundidee des Beweises ist die Beobachtung, dass $10 \equiv -1 \pmod{11}$, in anderen Worten, 10 geteilt durch 11 ergibt Rest 10.
Beweis: Die Aussage folgt aus der folgenden Rechnung:

$$\begin{aligned} n &= (a_m, \ldots, a_0)_{10} \\ &= \sum_{i=0}^{m} a_i 10^i \\ &\equiv \sum_{i=0}^{m} a_i (-1)^i \pmod{11} \\ &= A(n) \ . \end{aligned}$$

Das heißt, n und $A(n)$ liefern den gleichen Rest wenn geteilt durch 11. Insbesondere ist die eine durch 11 teilbar genau wenn die andere teilbar ist. □

(A) **7.105.** *Welche der folgenden Zahlen ist durch* 11 *teilbar:* 2837482, 1001, 10001, 100001, 234234, 283947*?*

Hausaufgabe 7.106. *Bestimmen Sie die kleinste sechsstellige Zahl, welche durch* 11 *teilbar ist und paarweise verschiedene Ziffern hat.*

7.6. **Übungsaufgaben.**

Hausaufgabe 7.107. *Teilen Sie die Menge* $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ *in zwei disjunkte Teilmengen auf, sodass die Summe der Zahlen in den Mengen gleich ist.*

Hausaufgabe 7.108. *Betrachten Sie die Mengen*

$$\begin{aligned} A &\stackrel{def}{=} \{m \in \mathbb{N} \mid 4|m\} \\ B &\stackrel{def}{=} \{m \in \mathbb{N} \mid 11|m\} \\ C &\stackrel{def}{=} \{m \in \mathbb{N} \mid 12|m\} \ . \end{aligned}$$

Finden Sie Elemente (wenn es welche gibt) in den folgenden Mengen: $A \cap B$, $(A \cap B) \setminus C$, $B \setminus C$, $A \cap B \cap C$.

Hausaufgabe 7.109. *Betrachten Sie die Mengen*

$$\begin{aligned} A &\stackrel{def}{=} \{m \in \mathbb{N} \mid m \leq 100\} \\ B &\stackrel{def}{=} \{m \in \mathbb{N} \mid 4|m\} \\ C &\stackrel{def}{=} \{m \in \mathbb{N} \mid 16|m\} \ . \end{aligned}$$

Welche der folgenden Mengen sind leer: $A \setminus B$,$A \setminus C$, $B \setminus C$,$C \setminus B$*?*

Hausaufgabe 7.110. *Es seien a und b ganze Zahlen. Zeigen Sie, dass*

$$7 \,|\, 10a + b \quad \Leftrightarrow \quad 7| \,|\, a - 2b \ .$$

Hausaufgabe 7.111. *Beweisen Sie: Zwei Primzahlen p und q mit $p \neq \pm q$ sind immer teilerfremd.*

Hausaufgabe 7.112. *Es sei m eine positive ganze Zahl. Berechnen Sie* $\mathrm{ggT}(3m+5, 7m+12)$.

Hausaufgabe 7.113. *Es sei $m \in \mathbb{Z}$. Beweisen Sie, dass $3|m^3 - m$. Stimmt es, dass sogar $6|m^3 - m$?*

Hausaufgabe 7.114. *Es sei $n \in \mathbb{Z}$. Beweisen Sie, dass*

(1) $n^6 = (n-1)(n^2+n+1)(n+1)(n^2-n+1)$ *und*
(2) $7|n^7 - n$.

Hausaufgabe 7.115. *Beweisen Sie die Aussage*

$$5040 \,|\, n^7 - 14n^5 + 49n^3 - 36n$$

in den folgenden Schritten.

(1) *Bestimmen Sie die Primfaktorzerlegung von* 5040 *(siehe 8.12).*
(2) *Beweisen Sie, dass*

$$n^7 - 14n^5 + 49n^3 - 36n \ = \ n(n^2-1)(n^2-4)(n^2-9) \ .$$

(3) *Zeigen Sie, dass* $5040 \,|\, n^7 - 14n^5 + 49n^3 - 36n$.

Hausaufgabe 7.116. *Benutzen Sie vollständige Induktion um zu zeigen, dass*

$$5 \,|\, 6^n - 1$$

für jede positive ganze Zahl n.

Hausaufgabe 7.117. *Sei n eine positive ganze Zahl. Welche der folgenden Brüchen lässt sich vereinfachen (das heißt, wann ist der ggT von Zähler und Nenner ungleich 1)?*

$$\frac{4n+2}{7n-1} \ , \ \frac{3n^2+1}{4n^2+3} \ , \ \frac{n^3-1}{n+1} \ .$$

Hausaufgabe 7.118. *Zeigen Sie, dass* $133|11^{n+1} + 12^{2n-1}$.

Hausaufgabe 7.119. *Für welche Werte der Ziffern x und y gilt* $99|x1995y$?

Hausaufgabe 7.120. *Es seien a, b, c Ziffern. Beweisen Sie, dass*

(1) $13|(a,b,c,a,b,c)_{10}$, *und*
(2) $37|(a,b,a,b,a,b)_{10}$.

7.7. **Weiterführende Literatur.**

(1) Fritsche: Mathematik für Einsteiger
(2) Stix: Elementare Zahlentheorie Skript

8. Teilbarkeit II. (Primfaktorenzerlegung und Irrationalität)

8.1. **Wiederholung.** Der Kapitel über Teilbarkeit, Quadratwurzel von reellen Zahlen, und was man in der Schule über rationale und reelle Zahlen gelernt hat.

Leitfrage. *Gibt es reelle Zahlen, die nicht rational sind? Falls ja, wie kann man zeigen, dass eine reelle Zahl, wie z.B.* $\sqrt{2}+\sqrt{3}$*,* keine *rationale Zahl ist?*

8.2. **Primfaktorzerlegung.** Wir fangen an mit der Wiederholung einer altbekannten Definition.

Definition 8.1 (Primzahl)**.** Eine ganze Zahl p heißt *prim*, falls sie genau zwei positive Teiler hat: 1 und $p \neq 1$.

Bemerkung 8.2. In anderen Worten ist $p \in \mathbb{Z}$ genau dann eine Primzahl, wenn die Zahlen ± 1 und $\pm p$ die einzigen Teiler von p sind. Es ist wichtig sich zu merken, dass ± 1 *keine* Primzahlen sind.

Bemerkung 8.3. Um zu zeigen, dass eine gewisse Zahl m *keine* Primzahl ist, brauchen wir nur einen Teiler $1 < d < m$ zu finden. Zum Beispiel ist 119 keine Primzahl, weil $7|119$. In der Tat, $119 = 7 \cdot 17$.

Die andere Richtung ist aufwändiger. Um zu zeigen, dass eine Zahl m prim ist, müssen wir nachweisen, dass keine der Zahlen $1 < d < m$ sie teilt.

A **8.4.** *Spielen Sie fünf Runden https://isthisprime.com/game/!*

A **8.5.** *Welche der folgenden Zahlen ist prim:* $139, 199, 217, 401$*? Finden Sie die kleinste Primzahl über* 500*.*

Lemma 8.6. *Sei $m \in \mathbb{Z}$. Wenn m nicht prim ist, dann gibt es einen Teiler $1 < d \leq \sqrt{m}$.*

Beweis: Wir führen einen Widerspruchsbeweis. Angenommen, alle Teiler $d > 1$ von m erfüllen $d > \sqrt{m}$. Da m keine Primzahl ist, existiert ein solcher Teiler $d < m$ und damit ist auch $1 < d/m < m$ ebenfalls ein Teiler von m. Es folgt aber

$$m \;=\; d \cdot \frac{m}{d} > \sqrt{m} \cdot \sqrt{m} \;=\; m \;,$$

ein Widerspruch. □

Bemerkung 8.7. Wenn wir untersuchen, ob konkrete Zahlen prim sind, reicht es also nach Lemma 8.6 die Zahlen bis $\sqrt{m}$ als mögliche Teiler zu überprüfen. Diese Beobachtung führt zur Methode bekannt als 'der Sieb des Eratosthenes' (s. [?StixEZ, Bemerkung 5.3]).

A **8.8.** *Finden Sie die kleinste Primzahl* > 1000*.*

Primzahlen haben besonders starke Teilbarkeitseigenschaften.

Lemma 8.9. *Es sei $m \in \mathbb{Z}$ und p eine Primzahl. Dann gilt*

$$\textit{entweder } p|m \textit{ oder } (p, m) = 1 \;.$$

Beweis: Wir werden $\mathrm{ggT}(p, m)$ analysieren. Zunächst ist $\mathrm{ggT}(p, m)$ ein positiver Teiler von p, daher muss er entweder p oder 1 sein. Falls $\mathrm{ggT}(p, m) = p$, dann gilt $p|m$. Ansonsten gilt $\mathrm{ggT}(p, m) = 1$. □

Die nächste Aussage beweist, was in der Algebra 'Primeigenschaft' genannt wird. Das ist im Grunde die Verallgemeinerung von Primzahlen für allgemeine Ringe (siehe Bemerkung 3.9). Was folgt, ist das zentrale technische Ergebnis dieses Kapitels.

Proposition 8.10 (Primeigenschaft)**.** *Es sei $p > 1$ eine ganze Zahl. Dann ist p genau dann prim, wenn für alle $a, b \in \mathbb{Z}$ aus $p|ab$ entweder $p|a$ oder $p|b$ folgt.*

Beweis:

($\Rightarrow$): Es sei also $p > 1$ eine Primzahl und a, b ganze Zahlen, sodass $p|ab$. Wenn $p|a$, dann sind wir fertig. Daher können wir annehmen, dass $p \not| a$. Aus Lemma 8.9 folgt, dass unter diesen Umständen $\mathrm{ggT}(p, a) = 1$ sein muss. Das wiederum impliziert $p|b$.

($\Leftarrow$): Es sei p mit den obigen Eigenschaften gegeben und wir nehmen an, dass $p = ab$ für gewisse ganze Zahlen a und b gegeben ist. Wir müssen nun zeigen, dass a und b (in irgendeiner Reihenfolge) ± 1 und $\pm p$ sind.

Nach Annahme gilt $p|ab$, daher muss entweder $p|a$ oder $p|b$ gelten. Wir nehmen ohne Einschränkung an, dass $p|a$ gilt, der Fall $p|b$ verläuft nämlich analog. Aus $p|a$ folgt $a = cp$ für ein geeignetes $c \in \mathbb{Z}$, insbesondere

$$p \;=\; ab \;=\; (cp)b \;=\; (cb)p \;.$$

Dementsprechend gilt $p(1 - bc) = 0$ und damit muss $bc = 1$ sein (da $p > 1$ ist muss der andere Faktor $1 - bc = 0$ sein), woraus $0 < |b|, |c| \leq 1$ folgt. Es muss also $b, c = \pm 1$ gelten und deswegen $a = \pm p$.

Wir haben bisher gezeigt, dass eine Zahl p mit den obigen Eigenschaften nur als Produkt $p \cdot 1$ oder $-p \cdot (-1)$ geschrieben werden kann. Sei nun d ein Teiler von p. Dann existiert ein $e \in \mathbb{Z}$ mit $de = p$. Also muss $d \in \{\pm 1, \pm p\}$ gelten. Somit ist die Zahl p nach Definition prim.

□

Hausaufgabe 8.11. *Beweisen Sie, dass zwei Primzahlen p und q entweder gleich oder teilerfremd sind.*

Satz 8.12 (Fundamentalsatz der Zahlentheorie)**.** *Es sei $0 \neq n \in \mathbb{Z}$ eine beliebige ganze Zahl. Dann existiert eine eindeutig bestimmte natürliche Zahl r, eindeutig bestimmte paarweise verschiedene Primzahlen $p_1, \ldots, p_r$, und eindeutig bestimmte positive ganze Zahlen $\alpha_1, \ldots, \alpha_r$, sodass*

$$n \;=\; \pm p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} \;.$$

Beweis: Diese Aussage werden wir nicht beweisen. □

Bemerkung 8.13. Eine Zerlegung von n als ein Produkt von Primzahlen nennt man eine *Primfaktorzerlegung* von n. Satz 8.12 sagt aus, dass jede ganze Zahl $n \neq 0$ eine (bis auf die Umsortierung der Faktoren) eindeutige Primfaktorzerlegung hat, d.h. $6 = 2 \cdot 3 = 3 \cdot 2$ ist die gleiche Zerlegung.

Ⓐ **8.14.** *Bestimmen Sie die Primfaktorzerlegung der folgenden Zahlen:*± 1, 17, 96, 256, 576, 1001.

Korollar 8.15. *Es sei $0 \neq n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ eine ganze Zahl. Dann hat n genau*

$$(\alpha_1 + 1) \cdot \ldots \cdot (\alpha_r + 1)$$

(positive) Teiler.

Beweis: Nach Satz 8.12 sind die Primzahlen p_i paarweise verschieden. Somit liefert jede Kombination der Primzahl(potenzen) einen Teiler von n. Da aber nicht jede Primzahl auch in jedem Teiler vorkommen muss, erlauben wir den Exponenten 0 und damit liefert jede einzelne Primzahl p_i genau $(\alpha_1 + 1)$ Teiler.
Etwas detaillierter: Das heißt für $m \in \mathbb{N}$ ist $m|n$ äquivalent dazu, dass m von der Form

$$m = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_r^{\beta_r}, \quad \text{mit } 0 \leq \beta_i \leq \alpha_i \text{ und } i = 1, 2, \ldots, r.$$

ist. Somit können wir jeden Teiler m mit den Exponenten $(\beta_1, \beta_2, \ldots, \beta_r)$ für $0 \leq \beta_i \leq \alpha_i$ und $i = 1, 2, \ldots, r$ identifizieren. Für jedes i gilt dabei $\beta_i \in \{0, 1, \ldots, \alpha_i\}$, also finden wir für jedes β_i genau $(\alpha_i + 1)$ Möglichkeiten. Multiplizieren wir diese alle, so erhalten wir das gewünschte Ergebnis. □

(A) **8.16.** *Bestimmen Sie die Anzahl der Teiler der folgenden Zahlen:*16*,* 72*,* 1024*,* 1001*,* 729*.*

Hausaufgabe 8.17. *Bestimmen Sie die kleinste positive ganze Zahl, die genau* 12 *bzw.* 13 *Teiler hat.*

Hausaufgabe 8.18. *Wie viele Rechtecke mit ganzzahligen Seitenlängen und Flächeninhalt* 2020 *gibt es?*

Bemerkung 8.19 (Erweiterte Primfaktorzerlegung)*.* Wir können die Primfaktorzerlegung der ganzen Zahlen umformulieren: Für eine natürliche Zahl n listen wir nicht die einzelnen Primfaktoren mit den entsprechenden Exponenten auf, sondern die Zahlen α_i für *alle Primzahlen.* Wenn eine Primzahl p unser n nicht teilt, dann ist der entsprechende Exponent 0.

Zum Beispiel für $n = 20$ schreiben wir dann

$$20 = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot \ldots \ ,$$

wobei für jede Prinzahl größer gleich 7 der Exponent immer 0 wird.

Wenn wir diesen Prozess auf alle ganze Zahlen anwenden, erhalten wir für jede Primzahl p eine Abbildung

$$\begin{array}{rccl} v_p \colon \mathbb{Z} \setminus \{0\} & \longrightarrow & \mathbb{N} & \\ n & \mapsto & \max\{\alpha \in \mathbb{N} \mid p^\alpha | n\} & \text{(die größte Potenz von } p\text{, die } n \text{ teilt).} \end{array}$$

Wenn wir zum Beispiel $p = 2$ betrachten, dann wird $v_2(20) = 2$, $v_2(-1) = 0$, $v_2(99) = 0$, und $v_2(32) = 5$. Die Tatsache, dass $v_p(m) = 0$ ist, bedeutet, dass die Primzahl p die Zahl m *nicht* teilt.

Beispiel 8.20. Die erweiterte Primfaktorzerlegung der Zahl 20 sieht so aus:

$$v_p(20) = \begin{cases} 2, & \text{falls } p = 2, \\ 1, & \text{falls } p = 5, \\ 0, & \text{für alle andere Primzahlen } p. \end{cases}$$

(A) **8.21.** *Berechnen Sie* $v_3(39)$*,* $v_7(91)$ *und* $v_3(-144)$*.*

(A) **8.22.** *Gegeben sei die Zahl* $m = 2^{20} \cdot 3^{17} \cdot 17^3 \cdot 39^1$*. Bestimmen Sie* $v_p(m)$ *für alle Primzahlen unter* 40*.*

A **8.23.** *Geben Sie die erweiterte Primfaktorzerlegung von* 144 *an.*

A **8.24.** *Bestimmen Sie die positive ganze Zahl m, für welche $v_3(m) = 2$, $v_5(m) = 1$ und $v_p(m) = 0$ für alle anderen p gilt.*

A **8.25.** *Es sei $m = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ die Primfaktorzerlegung der ganzen Zahl m im Sinne von Satz 8.12. Berechnen Sie $v_p(m)$ für alle Primzahlen!*

A **8.26.** *Bestimmen Sie $v_3(24)$, $v_3(18)$ und $v_3(432)$.*

Lemma 8.27. *Es sei p eine Primzahl, $a, b \in \mathbb{Z} \setminus \{0\}$. Dann gilt*

$$v_p(ab) \;=\; v_p(a) + v_p(b) \;.$$

Beweis: Nach Satz 8.12 haben sowohl a als auch b eine eindeutige Primfaktorzerlegung

$$a \;=\; p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} \text{ und } b \;=\; p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r},$$

wobei wir ohne Einschränkung davon ausgehen, dass $p_1, \ldots, p_r$ genau die Primzahlen sind, welche in der Zerlegung von a *oder* b vorkommen (das heißt einige der $alpha_i$ oder β_i können durchaus 0 sein). Aus den Potenzgesetzen folgt unmittelbar

$$ab \;=\; p_1^{\alpha_1+\beta_1} \cdot \ldots \cdot p_r^{\alpha_r+\beta_r}.$$

Anwenden von $v_p()$ auf a, b und ab liefert sofort die Behauptung. □

Korollar 8.28. *Es sei $a \neq 0$ eine ganze Zahl. Dann gilt*

$$a \;=\; \prod_{p\, prim} p^{v_p(a)} \;,$$

wobei $v_p(a) = 0$ für alle Primzahlen mit endlich vielen (möglicherweise keinen) Ausnahmen.

Beweis: Es folgt aus Satz 8.12, dass die Zahl a genau $v_p(a)$ Faktoren von p hat. □

A **8.29.** *Bestimmen Sie $v_p(24)$ und $v_p(144)$ für alle Primzahlen p.*

Lemma 8.30. *Es seien a und b von Null verschiedene ganze Zahlen. Dann gilt $a|b$ genau dann, wenn für jede Primzahl p die Ungleichung $v_p(a) \leq v_p(b)$ erfüllt ist.*

Beweis:

(⇒): Es gelte $a|b$. Aus der Definition von $v_p(a)$ folgt $p^{v_p(a)}|a$ und wegen der Transitivität der Teilbarkeit gilt $p^{v_p(a)}|b$. Aus Satz 8.12 und der Definition von v_p folgt, dass $v_p(b) \geq v_p(a)$ sein muss (da $v_p(b)$ dem größten Exponent von p entspricht).

(⇐): Jetzt nehmen wir an, dass $v_p(a) \leq v_p(b)$ gilt für alle Primzahlen p (wobei, nicht zu vergessen, $v_p(a)$ und $v_p(b)$ fast immer Null sind bis auf endlich viele Ausnahmen). Dann ist $v_p(b) - v_p(a) \geq 0$, und daher ist

$$m \stackrel{\text{def}}{=} \prod_{p\,\text{prim}} p^{v_p(b)-v_p(a)}$$

eine positive ganze Zahl. Wegen Korollar 8.28 gilt

$$\begin{aligned} b &= \prod_{p\,\text{prim}} p^{v_p(b)} \\ &= \prod_{p\,\text{prim}} p^{v_p(a)+(v_p(b)-v_p(a))} \\ &= \prod_{p\,\text{prim}} p^{v_p(a)} \cdot \prod_{p\,\text{prim}} p^{v_p(b)-v_p(a)} \\ &= a \cdot m \ , \end{aligned}$$

insbesondere folgt $a|b$, wie gewünscht.

□

A **8.31.** *Berechnen Sie* $v_3(42)$, $v_3(63)$, $v_3(\text{ggT}(42,63))$ *und* $v_3(\text{kgV}(42,63))$.

Korollar 8.32 (Primfaktorenzerlegung und ggT/kgV)**.** *Es seien* a *und* b *von Null verschiedenen ganze Zahlen. Dann sind die erweiterten Primfaktorzerlegungen von* $\text{ggT}(a,b)$ *und* $\text{kgV}(a,b)$ *gegeben durch*

$$\text{ggT}(a,b) = \prod_{p\,prim} p^{\min\{v_p(a),v_p(b)\}} \quad \textit{und} \quad \text{kgV}(a,b) = \prod_{p\,prim} p^{\max\{v_p(a),v_p(b)\}} \ .$$

Beweis: Wir müssen zeigen, dass für jede Primzahl p

$$v_p(\text{ggT}(a,b)) = \min\{v_p(a),v_p(b)\} \ \text{ und } \ v_p(\text{kgV}(a,b)) = \max\{v_p(a),v_p(b)\}$$

ist. Sei $d \in \mathbb{N}_+$ mit $v_p(d) = \min\{v_p(a),v_p(b)\}$ für alle Primzahlen p. Mit Lemma 8.30 folgt sofort $d|a$ und $d|b$, also auch $d|\,\text{ggT}(a,b)$ nach Proposition 7.59. Mit Lemma 8.30 wiederum folgt dann $\min\{v_p(a),v_p(b)\} = v_p(d) \le v_p(\text{ggT}(a,b))$. Eine erneute Anwendung von Lemma 8.30 liefert wegen $\text{ggT}(a,b)|a,b$ die Ungleichung $v_p(\text{ggT}(a,b)) \le \min\{v_p(a),v_p(b)\}$. Insgesamt haben wir (erneut wegen dem Lemma) sowohl $d|\,\text{ggT}(a,b)$ als auch $\text{ggT}(a,b)|d$, also $d = \text{ggT}$ und wir sind fertig. Der Beweis für $v_p(\text{kgV}(a,b)) = \max\{v_p(a),v_p(b)\}$ verläuft analog. □

A **8.33.** *Beweisen Sie mithilfe von Lemma 8.30 und Aussage 7.63 (analog zum Beweis für den ggT), dass*

$$v_p(\text{kgV}(a,b)) = \max\{v_p(a),v_p(b)\}.$$

Lemma 8.34. *Es seien* α *und* β *zwei beliebige reelle Zahlen. Dann gilt*

$$\max\{\alpha,\beta\} + \min\{\alpha,\beta\} = \alpha + \beta \ .$$

Beweis: Sei ohne Einschränkung $\alpha \ge \beta$. Dann ist $\max\{\alpha,\beta\} = \alpha$ und $\min\{\alpha,\beta\} = \beta$. Die Behauptung folgt sofort. □

Jetzt geben wir einen alternativen Beweis von Satz 7.71.

Satz 8.35 (Gleich wie Satz 7.71)**.** *Es seien* a *und* b *von Null verschiedene ganze Zahlen. Dann gilt*

$$\text{ggT}(a,b) \cdot \text{kgV}(a,b) = |ab| \ .$$

Beweis: Wir werden zeigen, dass die Aussage schnell aus Korollar 8.32 und Lemma 8.34 folgt. Ohne Einschränkung seien $a, b \geq 0$. Daher brauchen wir den Betrag auf der rechten Seite nicht mehr. Es gilt dann

$$\begin{aligned}
\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) &= \prod_{p \text{ prim}} p^{\min\{v_p(a),v_p(b)\}} \cdot \prod_{p \text{ prim}} p^{\max\{v_p(a),v_p(b)\}} \\
&= \prod_{p \text{ prim}} p^{\min\{v_p(a),v_p(b)\}} \cdot p^{\max\{v_p(a),v_p(b)\}} \\
&= \prod_{p \text{ prim}} p^{\min\{v_p(a),v_p(b)\}+\max\{v_p(a),v_p(b)\}} \\
&\overset{8.34}{=} \prod_{p \text{ prim}} p^{v_p(a)+v_p(b)} \\
&= \prod_{p \text{ prim}} p^{v_p(a)} \cdot \prod_{p \text{ prim}} p^{v_p(b)} \\
&= a \cdot b \ .
\end{aligned}$$

□

8.3. **Irrationale Zahlen.**

Definition 8.36. Eine reelle Zahl α heißt *irrational*, wenn sie nicht rational ist. Anstelle von „α ist irrational“ schreiben wir auch $\alpha \notin \mathbb{Q}$.

Bemerkung 8.37. Wir befinden uns jetzt in einer merkwürdigen Situation. Wir haben zwar den Begriff einer irrationalen Zahl definiert, wir haben sogar gehört, dass die Zahl $\pi = 3,1415926\ldots$ irrational ist, aber haben von keiner Zahl gesehen, dass sie tatsächlich irrational ist.

Das ist kein Zufall. Wir werden in einigen Fällen beweisen können, dass gewisse Zahlen irrational sind (wie $\sqrt{2}$ zum Beispiel), aber es ist oft sehr schwierig, solche Beweise durchzuführen. Der Beweis der Irrationalität von π zum Beispiel ist ziemlich kompliziert.

Bemerkung 8.38. Im Gegenteil zu rationalen Zahlen können Summen, Produkte usw. von irrationalen Zahlen sowohl rational als auch irrational sein. Es gibt keine allgemeine Regel.

Lemma 8.39. *Es sei α eine irrationale und $\beta \neq 0$ eine rationale Zahl. Dann sind sowohl $\alpha \pm \beta$, $\alpha\beta$ als auch α/β irrational.*

Beweis: Da aus β rational $-\beta$ und $1/\beta$ rational folgt, können wir β durch $-\beta$ oder $1/\beta$ ersetzen. Daher reicht es zu zeigen, dass $\alpha + \beta$ und $\alpha \cdot \beta$ irrational sind.

Wir führen einen Widerspruchsbeweis. Angenommen, es ist $\alpha+\beta \in \mathbb{Q}$. Da Summen/Differenzen von rationalen Zahlen ebenfalls rational sind, folgt daraus, dass

$$\alpha \ = \ (\alpha + \beta) - \beta \ \in \mathbb{Q}$$

sein muss, ein Widerspruch. Somit muss die Zahl α irrational sein.

Analog nehmen wir an, dass $\alpha\beta \in \mathbb{Q}$ ist. Da Produkte und Quotienten rationaler Zahlen wieder rational sind, folgt daraus, dass

$$\alpha \ = \ (\alpha \cdot \beta) \cdot \frac{1}{\beta} \ \in \mathbb{Q} \ ,$$

was unserer Bedingung $\alpha \notin \mathbb{Q}$ widerspricht. Deshalb ist $\alpha\beta$ irrational. □

A **8.40.** *Schreiben Sie einen vollständigen Beweis dafür, dass $\alpha - \beta$ eine irrationale Zahl ist, wenn $\alpha \notin \mathbb{Q}$ und $\beta \in \mathbb{Q}$.*

Das folgende Ergebnis ist grundlegend. Wir werden die eindeutige Primfaktorzerlegung verwenden, um die Irrationalität von $\sqrt{2}$ zu zeigen.

Satz 8.41. *Die Zahl $\sqrt{2}$ ist irrational.*

Beweis: Wir führen einen Widerspruchsbeweis. Nehmen wir an, dass $\sqrt{2} \in \mathbb{Q}$. Das bedeutet, dass es positive ganze Zahlen $p, q \in \mathbb{Z}$ mit $q \neq 0$ und $\mathrm{ggT}(p, q) = 1$ gibt, so dass

$$\sqrt{2} = \frac{p}{q} .$$

Nach quadrieren der beiden Seiten und Multiplikation mit q^2 folgt, dass

$$2q^2 = p^2 .$$

Da die Zahlen $2q^2$ und p^2 gleich sind, haben sie die gleiche Primfaktorzerlegung. Sei s die Potenz von 2 in der Primfaktorzerlegung von $2q^2 = p^2$.

Wir betrachten jetzt die Parität von s. Einerseits muss s gerade sein, weil p^2 eine Quadratzahl ist, und in einer Quadratzahl sind die Exponenten von Primzahlen alle gerade. Aus dem gleichen Grund ist aber s ungerade, weil der Exponent von 2 in q^2 gerade ist, somit in $2q^2$ um Eins größer, daher ungerade. Das ist der gewünschte Widerspruch. □

A **8.42.** *Finden Sie die Stelle im obigen Beweis, an der die Eindeutigkeit der Primfaktorzerlegung ausgenutzt wurde.*

Satz 8.43. *Es sei r eine Primzahl. Dann ist $\sqrt{r}$ eine irrationale Zahl.*

Beweis: Der Beweis ist wortwörtlich gleich dem von Satz 8.41, man muss lediglich 2 durch r ersetzen. □

A **8.44.** *Schreiben Sie einen vollständigen Beweis für die Irrationalität von $\sqrt{11}$.*

Beispiel 8.45. Wir werden zeigen, dass $18\sqrt{17} - 39$ eine irrationale Zahl ist. Wie bisher immer, werden wir per Widerspruch argumentieren. Angenommen, $\alpha \stackrel{\text{def}}{=} 18\sqrt{17} - 39$ ist eine rationale Zahl. Dann ist aber auch

$$\sqrt{17} = \frac{\alpha + 39}{18} \in \mathbb{Q} .$$

Das widerspricht Satz 8.43 und deshalb ist $18\sqrt{17} - 39 \notin \mathbb{Q}$.

A **8.46.** *Beweisen Sie mit einer ähnlichen Argumentation, dass $523\sqrt{31} + 1009$ eine irrationale Zahl ist.*

Lemma 8.47. *Es seien $a, b \in \mathbb{Q}$, und $\alpha \in \mathbb{R}$ eine irrationale Zahl. Dann ist auch $a\alpha + b$ irrational.*

Beweis: Angenommen, $a\alpha + b$ ist rational. Dann ist aber auch

$$\alpha = \frac{(a\alpha + b) - b}{a} \in \mathbb{Q} ,$$

ein Widerspruch. □

Satz 8.48. *Es seien $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen. Dann ist $\sqrt{p_1 \ldots p_r}$ eine irrationale Zahl.*

(A) **8.49.** *Welche der folgenden Zahlen sind irratonal: $\sqrt{6}, \sqrt{9}, \sqrt{12}, \sqrt{13}, \sqrt{91}, \sqrt{1001}$?*

Beispiel 8.50. Wie früher schon erwähnt, können wir im Allgemeinen nichts über die (Ir)Rationalität der Summe oder des Produkts zweier irrationaler Zahlen sagen. Es gilt zum Beispiel

$$\sqrt{2} - \sqrt{2} \;=\; 0 \in \mathbb{Q} \;,$$

oder eben

$$\sqrt{2} \cdot \sqrt{8} \;=\; 4 \in \mathbb{Q} \;.$$

Es gibt also Beispiele, bei denen die Summe oder das Produkt zweier irrationaler Zahlen rational ist.

Beispiel 8.51. Wir werden hier zeigen, dass $\sqrt{2} + \sqrt{5}$ eine irrationale Zahl ist. Angenommen, es ist nicht so und $\alpha \stackrel{\text{def}}{=} \sqrt{2} + \sqrt{5}$ ist rational. Dann ist

$$\alpha^2 \;=\; (\sqrt{2} + \sqrt{5})^2 \;=\; 2 + 2\sqrt{10} + 5 \;=\; 7 + 2\sqrt{10}$$

ebenfalls rational. Dann wäre aber auch $\sqrt{10}$ rational, was Satz 8.48 widerspricht. Es ist also $\sqrt{2} + \sqrt{5} \notin \mathbb{Q}$.

(A) **8.52.** *Beweise Sie, dass $\sqrt{7} + \sqrt{11} \notin \mathbb{Q}$.*

Hausaufgabe 8.53. *Zeigen Sie, dass $\sqrt{6} + \sqrt{10}$ irrational ist.*

Hausaufgabe 8.54. *Es seien $p_1, \ldots, p_m$ und $q_1, \ldots, q_n$ paarweise verschiedene Primzahlen. Verifizieren Sie, dass*

$$\sqrt{p_1 \cdots p_m} + \sqrt{q_1 \cdots q_n} \notin \mathbb{Q} \;.$$

Als letztes zeigen wir den folgenden interessanten Satz über Rationalität von Quadratwurzeln.

Satz 8.55. *Es sein n eine natürliche Zahl mit $\sqrt{n} \in \mathbb{Q}$. Dann ist $\sqrt{n}$ sogar eine natürliche Zahl.*

Beweis: Nehmen wir an, dass

$$\sqrt{n} \;=\; \frac{p}{q} \in \mathbb{Q} \;,$$

wobei ohne Einschränkung $\mathrm{ggT}(p, q) = 1$. Insbesondere sind die Primteiler von p und q paarweise verschieden. Es folgt, dass

$$q^2 n \;=\; p^2$$

und keiner der Primfaktoren von q taucht auf der rechten Seite auf. Wegen der eindeutigen Primfaktorzerlegung müssen die Primfaktoren auf beiden Seiten aber gleich sein. Also muss $q^2 = 1$ und somit auch $q = 1$ sein. □

8.4. **Übungsaufgaben.**

Hausaufgabe 8.56. *Welche dreistelligen Zahlen haben genau fünf Teiler?*

Hausaufgabe 8.57. *Es sei m eine Zahl, die genau 2019 Teiler hat. Beweisen Sie, dass m nicht durch 2020 teilbar sein kann.*

Hausaufgabe 8.58. *Zeigen Sie, dass $5\sqrt{7} - 3\sqrt{3} \notin \mathbb{Q}$.*

Hausaufgabe 8.59. *Dem Argument des Beweises von Satz 8.41 folgend, beweisen Sie, dass $\sqrt[3]{2}$ eine irrationale Zahl ist. Achten Sie darauf, ob der Exponent von 2 in den relevanten Primfaktorzerlegungen durch 3 teilbar ist oder nicht.*

8.5. **Weiterführende Literatur.**

(1) Fritsche: Mathematik für Einsteiger
(2) Stix: Elementare Zahlentheorie Skript, Kapitel 5

9.1. **Wiederholung.** Die beiden Kapitel über Teilbarkeit (besonders der Abschnitt 'Teilbarkeitsregel im Zehnersystem') und sammeln Sie Ihr Schulwissen über Zahlensysteme.

9.2. **Zahlensysteme im Allgemeinen.**

(A) **9.1.** *Wiederholen Sie das Römische Zahlensystem.*

(1) *Wie viel ist $MDCCXLIV$?*
(2) *Was sind wichtige Unterschiede zwischen dem Römischen und dem Zehnersystem?*
(3) *Was für Eigenschaften/Objekte/Möglichkeiten hat das Zehnersystem, die im Römischen System fehlen?*

Obwohl unser Leben zum Großteil im Rahmen des Zehnersystems verbracht wird, gibt es diverse andere Zahlensysteme, die in unserem Leben (bewusst oder nicht) wichtige Rollen spielen. Zum Beispiel Minuten und Sekunden messen wir im 60-er System und beim Aufbau und Programmieren von Rechnern haben die Zweier- und Sechzehnersysteme äußerst große Bedeutung.

Leitfrage. *Gibt es Teilbarkeitsregeln wie z.B. die Quersummenregel bei Teilbarkeit durch* 9 *oder die alternierende Quersummenregel bei Teilbarkeit durch* 11 *in anderen Zahlensystemen? Ist es richtig z.B. im Zwölfersystem die gleichen Regeln bei Teilbarkeit mit* 11 *und* 13 *zu erwarten?*

Im Laufe dieses Kapitels werden wir zeigen, dass wir zu jeder positiven ganzen Zahl b ein 'b-adisches' Zahlensystem definieren können. Insbesondere hat jede natürliche oder ganze Zahl eine eindeutige b-adische Entwicklung (gemeint ist eine Darstellung bezüglich der Basis b).

Beispiel 9.2. Ein b-adisches Zahlensystem wird normalerweise für $b \geq 2$ definiert. Für $b = 1$ können wir uns die 1-adische Entwicklung von $m \in \mathbb{N}$ als

$$m_1 \stackrel{\text{def}}{=} 1 \ldots 1$$

vorstellen, wobei die Entwicklung aus m 1-ern besteht. Für natürliche Zahlen m und n definiert man

$$(m+n)_1 \stackrel{\text{def}}{=} m_1\, n_1 \ ,$$

also einfach durch aneinanderreihen.

Für $b \geq 2$ versuchen wir haargenau das, was die Menschheit im Zehnersystem seit langer Zeit erfolgreich macht: jede ganze Zahl als eine Summe von Potenzen von b zu schreiben. Wir fangen mit der folgenden Hilfsaussage an, die uns sagt, wie lang so eine Entwicklung sein soll.

Lemma 9.3. *Es sei $b \geq 2$ eine ganze Zahl. Dann gibt es zu jeder positiven ganzen Zahl m eine eindeutig bestimmte natürliche Zahl n mit der Eigenschaft, dass*

$$b^n \ \leq \ m \ < \ b^{n+1} \ .$$

(A) **9.4.** *Bestimmen Sie dieses n für $b = 3$,$m = 242$ und $b = 2$, $m = 1024$. Was passiert, wenn $b = 19$ und $m = 4$ ist?*

(A) **9.5.** *Zeigen Sie mit vollständiger Induktion, dass für jede natürliche Zahl k die Ungleichung $b^k > k$ gilt, wenn $b \geq 2$ ist. Versuchen Sie anschließend die gleiche Behauptung mit Satz 6.41 zu verifizieren.*

Beweis: Sei $b \in \mathbb{Z}_{\geq 2}$ und $m \in \mathbb{N}_+$. Als erstes bemerken wir, dass nach obiger Aufgabe $b^k > k$ gilt für jedes $k \in \mathbb{N}$. Wir betrachten die Menge

$$A \stackrel{\text{def}}{=} \{s \in \mathbb{N} \mid b^s > m\} \ .$$

Wegen $b^m > m$ ist $A \neq \emptyset$. Somit ist A eine nicht-leere Teilmenge der natürlichen Zahlen und als solches besitzt A ein eindeutig bestimmtes kleinstes Element. Wir nehmen

$$n \stackrel{\text{def}}{=} \min(A) - 1 \ .$$

Da $n+1 \in A$ ist, gilt $b^{n+1} > m$, und weil $n+1$ das Minimum von A ist, gilt $m \geq b^n$. □

A **9.6.** *Warum kann im obigen Beweis n nicht negativ sein?*

Satz 9.7 (b-adische Entwicklung)**.** *Es sei $b \geq 2$ eine natürliche Zahl, $m \in \mathbb{Z}$. Dann gibt es ein eindeutig bestimmtes $n \in \mathbb{N}$ und eindeutig bestimmte ganze Zahlen $0 \leq a_0, \ldots, a_n < b$ mit $a_n \neq 0$, sodass*

$$m = a_0 \cdot b^0 + a_1 \cdot b^1 + \ldots + a_n \cdot b^n \ . \tag{9.1}$$

Definition 9.8. Gegeben seien b und m wie in Satz 9.7. Einfachheitshalber können wir ohne Einschränkung annehmen, dass $m \geq 0$ ist (anderseits schreiben wir $-(-m)$ und arbeiten mit $-m \geq 0$ weiter). Die Darstellung 9.1 nennt man die *b-adische Entwicklung von m*. Die Zahlen $a_0, \ldots, a_n$ sind die *b-adischen Ziffern* von m und man notiert

$$m = (a_n a_{n-1} \ldots a_0)_b \ .$$

Diese Ziffernfolge ist die Darstellung der Zahl m im b-adischen oder b-er Zahlensystem. Alternativ kann die Darstellung 9.1 von m auch als Darstellung bezüglich der (oder zur) *Basis* b bezeichnet werden.

A **9.9.** *Berechnen Sie die b-adische Entwicklung von 117 für $b = 2, 3, 5, 7$.*

A **9.10.** *Berechnen Sie die 5-adische Entwicklung von $(10110001)_2$ und $(1200220)_3$!*

Beweis von Satz 9.7: Seien b und m positive ganze Zahlen, wobei $b \geq 2$ ist. Dann existiert nach Lemma 9.3 eine wohlbestimmte natürliche Zahl n, für welche

$$b^n \leq m < b^{n+1}$$

gilt. Die Zahl n bestimmt die Länge der b-adischen Entwicklung von m. Die Existenz und Eindeutigkeit der b-adischen Entwicklung werden wir mit vollständiger Induktion beweisen. Der Beweis der Eindeutigkeit kann zunächst übersprungen werden.
INDUKTIONSANFANG: Wir betrachten den Fall $n = 0$. Dann gilt

$$b^0 = 1 \leq m < b^{0+1} = b$$

und dementsprechend ist $a_0 \stackrel{\text{def}}{=} m$ die eindeutig bestimmte Entwicklung von m.
INDUKTIONSSCHLUSS: Sei $n > 0$ und jede positive ganze Zahl $< b^n$ habe eine eindeutig bestimmte b-adische Entwicklung. Unser Ziel ist es, das Gleiche für alle Zahlen $< b^{n+1}$ zu zeigen.

Wir verwenden Division mit Rest bezüglich b^n und erhalten

$$m = c \cdot b^n + r \ ,$$

wobei $0 \leq r < b^n$ und $c \neq 0$ gelten. Insbesondere hat r nach Induktionsannahme eine eindeutige b-adische Entwicklung

$$r \;=\; \sum_{i=0}^{n-1} a_i b^i \;=\; (a_{n-1} \dots a_0)_b \;.$$

Anderseits gilt

$$c \cdot b^n \;=\; m - r < m < b^{n+1}$$

und daher $c < b$.

Mithilfe diese Beobachtungen konstruieren wir eine b-adische Entwicklung von m. Mit $a_n \stackrel{\text{def}}{=} c$ erhalten wir

$$m \;=\; c \cdot b^n + r \;=\; a_n \cdot b^n + \sum_{i=0}^{n-1} a_i b^i \;=\; \sum_{i=0}^{n} a_i b^i \;=\; (a_n \dots a_0)_b \;.$$

Es bleibt noch die Eindeutigkeit zu zeigen. Diese wird aus der Eindeutigkeit der Division mit Rest folgen. Es sei

$$m \;=\; (c_k \dots c_0) \;=\; \sum_{i=0}^{k} c_i \cdot b^i$$

eine weitere b-adische Entwicklung von m und wir nehmen an, dass $k \leq n$ gilt (andernfalls vertauschen wir die Rollen der beiden Entwicklungen). Gilt $k < n$, dann haben wir wegen

$$m \;=\; \sum_{i=0}^{n} a_i b^i \;\geq\; b^n \;\geq\; b^{k+1} > \sum_{i=0}^{k} c_i \cdot b^i \;=\; m$$

einen Widerspruch. Also muss $k = n$ gelten.

Nach Division mit Rest durch b^n erhalten wir

$$\begin{aligned} m \;&=\; c_n \cdot b^n + \sum_{i=0}^{n-1} c_i \cdot b^i \text{ und} \\ m \;&=\; a_n \cdot b^n + \sum_{i=0}^{n-1} a_i \cdot b^i \;. \end{aligned}$$

Aber der Quotient und der Rest sind eindeutig, daher

$$a_n \;=\; c_n \;\text{ und }\; \sum_{i=0}^{n-1} a_i \cdot b^i \;=\; \sum_{i=0}^{n-1} c_i \cdot b^i \;.$$

Nach der Induktionsannahme für die Reste gilt

$$(a_{n-1} \dots a_0)_b \;=\; (c_{n-1} \dots c_0)_b$$

und damit

$$(a_n \dots a_0)_b \;=\; (c_n \dots c_0)_b \;,$$

wie gewünscht. Somit stimmen die beiden Entwicklungen überein. □

Beispiel 9.11 (Binäres Zahlsystem). Das Zahlensystem zur Basis 2 kann man am einfachsten mit Strom implementieren, deswegen dient es als Basis für unsere Computertechnik. Die Ziffern sind dementsprechend 0 und 1. Es gelten zum Beispiel

$$19 \;=\; (10011)_2 \;\text{ und }\; (101010)_2 \;=\; 42 \;.$$

Ⓐ **9.12.** *Rechnen Sie die folgenden Zahlen ins Zehnersystem bzw. ins Binärsystem um:* 38*,* 91*,* 255*,* $(1100110)_2$*,* 1001 *und* $(10111)_2$*.*

Beispiel 9.13 (Hexadezimales Zahlensystem)*.* In der Informatik ist das Zahlensystem zur Basis 16, oft hexadezimales Zahlsystem genannt, von großer Relevanz. In diesem Fall gibt es die sechzehn Ziffern

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F \ .$$

Es gilt zum Beispiel

$$65 \ = \ (41)_{16} \ \text{ und } (FF)_{16} \ = \ 255 \ .$$

Ⓐ **9.14.** *Rechnen Sie die folgenden hexadezimalen Zahlen ins Zehnersystem um:* $(FE)_{16}$*,* $(ABC)_{16}$*,* $(9F)_{16}$ *und* $(11)_{16}$*.*

Bemerkung 9.15*.* Die Umrechnung zwischen dem binären und hexadezimalen Zahlensystemen ist besonders praktisch, da wir wegen $16 = 2^4$ Folgendes machen können: Es sei $(a_n \dots a_0)_{16}$ eine hexadezimale Zahl. Dann sind die Ziffern $a_n, \dots, a_0$ alle zwischen 0 und 16 (wobei 16 nicht erlaubt ist). Wir können daher jede Ziffer als eine vierstellige binäre Zahl darstellen, zum Beispiel

$$F \ = \ 1111 \ , \ 9 \ = \ 1001 \ , \ C \ = \ 1100 \ .$$

Um die binäre Darstellung der Zahl $(a_n \dots a_0)_{16}$ zu erhalten, müssen wir einfach die vierstelligen binären Darstellungen in der ursprünglichen Reihenfolge hinschreiben. Als konkretes Beispiel betrachten wir $(FA92)_{16}$. Die Binärdarstellung der einzelnen Ziffern ist

$$F \ = \ 1111 \ , \ A \ = \ 1010 \ , \ 9 \ = \ 1001 \ , \ 2 \ = \ 0010 \ ,$$

und somit

$$(FA92)_{16} \ = \ (1111101010010010)_2 \ .$$

Betrachten wir nun eine binäre Zahl $(c_n \dots c_0)_2$. Wir nehmen an, dass $n + 1$ (die Anzahl der Ziffern) durch 4 teilbar ist (andernfalls ergänzen wir 0-en, bis dem so ist). Dann teilen wir die Ziffern in Vierergruppen auf und rechnen diese Gruppen in Hexadezimalzahlen um. Die hexadezimale Entwicklung besteht dann aus den entsprechenden hexadezimalen Ziffern (in der ursprünglichen Reihenfolge).

Wir betrachten zum Beispiel $(1011010101011)_2$. Die Anzahl der Ziffern ist 13, die wir auf 16 ergänzen: 0001011010101011. Die Binärdarstellung der Blöcke ist dann

$$0001 \ = \ 1 \ , \ 0110 \ = \ 6 \ , \ 1010 \ = \ A \ , \ 1011 \ = \ B$$

und daher

$$(1011010101011)_2 \ = \ (16AB)_{16} \ .$$

Ⓐ **9.16.** *Geben Sie die Hexadezimal- bzw. Binärdarstellung der folgenden Zahlen an:* $(1010101010111110)_2$*,* $(31A4F)_{16}$*,*$(1001)_{16}$ *und* $(1111100010)_2$*.*

Die arithmetischen Operationen (Addition, Subtraktion, Multiplikation, Division) im b-adischen Zahlensystem verlaufen wie im Zehnersystem, mit dem einen großen Unterschied: Für zwei Zahlen $0 \leq a, c < b$ gilt

$$(a)_b + (c)_b = (1d)_b \ \text{ wenn } a + c \ \geq \ b \text{ und } a + c - b \ = \ d.$$

Beispiel 9.17. Addition im Zweiersystem ist besonders einfach. Die Addition von Ziffern sieht so aus:

$$0+0 = 0\ ,\ 0+1 = 1+0 = 1,\ 1+1 = 10\ .$$

Dementsprechend gilt

$$(1011)_2 + (10001)_2 = (11100)_2\ .$$

Wir können uns von der Richtigkeit des Ergebnisses leicht überzeugen: Es handelt sich um die Addition $(11)_{10} + (17)_{10} = (28)_{10}$.

(A) **9.18.** *Führen Sie die folgenden Additionen aus:*

(1) $(101001)_2 + (100110)_2 = ?$
(2) $(2102)_3 + (2021)_3 = ?$
(3) $(7541)_8 + (2005)_8 = ?$
(4) $(AB2E)_{16} + (1001)_{16} = ?$.

Beispiel 9.19. Wir führen die folgende Operation im 8-er System aus:

$$31721_8 - 15463_8$$

Um die Subtraktion zu berechnen, können wir einerseits die Zahlen ins Zehnersystem umrechnen, dann subtrahieren und das Ergebnis wieder ins 8-er System transferieren oder wir führen eine einfache schriftliche Subtraktion durch.

Möglichkeit 1: Es gilt nach 9.1

$$31721_8 = 3\cdot 8^4 + 1\cdot 8^3 + 7\cdot 8^2 + 2\cdot 8^1 + 1\cdot 8^0 = 13265$$
$$15463_8 = 1\cdot 8^4 + 5\cdot 8^3 + 4\cdot 8^2 + 6\cdot 8^1 + 3\cdot 8^0 = 6963.$$

Also gilt

$$31721_8 - 15463_8 = 13265 - 6963 = 6302 = 14236_8.$$

Dieses Verfahren hat offensichtliche Nachteile: Man muss unnötig viel rechnen. Für die letzte Gleichung muss man nämlich schauen wie oft 8^4 in 6302 passt, dann wie oft 8^3 in die Differenz usw. Daher:

Möglichkeit 2: Wir subtrahieren „schriftlich“

$$\begin{array}{rccccc} & 3 & 1 & 7 & 2 & 1 \\ - & 1 & 5 & 4 & 6 & 3 \\ & {\scriptstyle 1} & & {\scriptstyle 1} & {\scriptstyle 1} & \\ \hline & 1 & 4 & 2 & 3 & 6 \end{array}$$

Achten Sie beim Übertrag immer darauf die Zahlen korrekt ins jeweilige Zahlensystem zu übertragen!

Hausaufgabe 9.20. *Üben sie auch die anderen Operationen in den verschiedenen Zahlensystemen.*

9.3. **Teilbarkeitsregel im Zahlsystemen.** Die Teilbarkeitsregeln, die wir im Zehnersystem gesehen haben, sind für Teilbarkeit durch $2, 5, 3, 9$ und 11. Das ist kein Zufall. Die Zahlen 2 und 5 sind Teiler von 10, die Basis des Zahlsystem. Die Zahlen 3 und 9 sind Teiler von $9 = 10 - 1$ und 11 ist Teiler von $11 = 10 + 1$. Somit gibt es für jede Regel einen klaren Zusammenhang mit der Basis 10. Genau das erwarten wir auch bei einem allgemeinem Zahlensystem mit Basis b. In einem Zahlsystem mit Basis b suchen wir also Teilbarkeitsregeln für

- Teiler von b (wie viele 0-en gibt es am Ende?)
- Teiler von $b - 1$ (mittels der Quersumme der Ziffern)
- Teiler von $b + 1$ (mittels der alternierenden Quersumme der Ziffern)

Etwas später werden wir sehen, dass kompliziertere Summen von Ziffern zu weiteren Teilbarkeitsregel (zum Beispiel durch 13 oder 37) führen werden.

Die Aussagen und deren Beweise sind denen über das Zehnersystem äußerst ähnlich.

Proposition 9.21. *Es sei $b \geq 2$ eine ganze Zahl, s eine ganze Zahl, die b teilt und $n > 0$ eine natürliche Zahl. Dann ist n genau dann durch s^k teilbar, wenn die Zahl, die aus den letzten k Ziffern in der b-adischen Entwicklung von n besteht, durch s^k teilbar ist.*

(A) **9.22.** *Schreiben Sie die Aussage von Proposition 9.21 im Fall $b = 4$ auf. Sind die Zahlen $(1203)_4$,$(1023202)_4$, $(10300)_4$ durch 2 und 4 teilbar?*

Beweis: Es sein n eine positive ganze Zahl, $1 \leq k \leq m$. Dann gilt

$$\begin{aligned} n &= (a_m, a_{m-1}, \ldots, a_0)_b \\ &= (a_m, a_{m-1}, \ldots, a_k, 0 \ldots, 0)_b + (a_{k-1}, \ldots, a_0)_b \\ &= \sum_{i=k}^{m} a_i b^i + (a_{k-1}, \ldots, a_0)_b \\ &= b^k \cdot \sum_{i=0}^{m-k} a_{i-k} b^i + \ldots + (a_{k-1}, \ldots, a_0)_b \\ &= b^k \cdot (a_m, a_{m-1}, \ldots, a_k)_b + (a_{k-1}, \ldots, a_0)_b \\ &\equiv (a_{k-1}, \ldots, a_0)_b \pmod{s^k} , \end{aligned}$$

wobei im letzten Schritt $s|b$ und somit $s^k|b^k$ benutzt wurde. Das heißt die Zahlen $n = (a_m, a_{m-1}, \ldots, a_0)_b$ und $(a_{k-1}, \ldots, a_0)_b$ haben den gleichen Rest bei Division mit s^k. Insbesondere sind sie entweder beide durch s^k teilbar oder beide nicht. □

(A) **9.23.** *Finden sie die Unterschiede zwischen den Beweisen von Proposition7.85 und Proposition 9.21.*

Hausaufgabe 9.24. *Bestimmen Sie, ob die Zahlen $(127321)_8$, $(12320)_8$ und $(12804)_8$ durch 2, 4 oder 8 teilbar sind.*

Hausaufgabe 9.25. *Welche der Zahlen $(12393A)_{12}$, $(A2390)_{12}$ oder $(12932AB3)_{12}$ sind durch 3, 4, oder 6 teilbar?*

Bemerkung 9.26. Die Definition der Quersumme und der alternierenden Quersumme in Kapitel 7 ist unabhängig von der Basis des Zahlensystems, daher werden wir sie in jedem Zahlensystem genauso definieren. Wenn wir zeigen möchten, in welchem Zahlensystem wir arbeiten, schreiben wir $Q_b(m)$ für die Quersumme und $A_b(m)$ für die alternierende Quersumme.

A **9.27.** *Geben Sie die Definition der alternierenden Quersumme im Sechsersystem an.*

Proposition 9.28. *Es sei n eine positive ganze Zahl, $b \geq 2$ und s ein Teiler von $b-1$. Dann ist n genau dann durch s teilbar, wenn $Q_b(n)$ durch s teilbar ist.*

Der Grund für diese Eigenschaft ist, dass b und 1 den gleichen Rest modulo s haben. In der Notation von Bemerkung 7.51 schreiben wir

$$b \equiv 1 \bmod s \quad .$$

Beweis: Unser Argument beruht wieder auf der folgenden Rechnung:

$$\begin{aligned} n &= (a_m, a_{m-1}, \ldots, a_0)_b \\ &= \sum_{i=0}^{m} a_i b^i \\ &\equiv \sum_{i=0}^{m} a_i 1^i \mod s \\ &= \sum_{i=0}^{m} a_i \\ &= Q_b(n) \ . \end{aligned}$$

Das heißt n und $Q(n)$ haben den gleichen Rest, wenn sie durch s geteilt werden. Insbesondere gilt $s|n$ genau dann, wenn $s|Q_b(n)$. □

A **9.29.** *Gehen Sie den Beweis für den Fall $n = 567$, $b = 8$ und $s = 4$ durch.*

A **9.30.** *Bestimmen Sie alle Teilbarkeitsregeln im 12-ersystem. Welche der folgenden Zahlen sind durch 11 teilbar: $(123987AB)_{12}$, $(23432)_{12}$?*

A **9.31.** *Vergleichen Sie den Beweis mit dem von Proposition* **??**.

Hausaufgabe 9.32. *Welche Werte kann die Ziffer a haben, wenn $4|(1238a)_9$?*

Proposition 9.33. *Es sei n eine positive ganze Zahl, $b \geq 2$ die Basis unseres Zahlensystem und s ein Teiler von $b+1$. Dann gilt $s|n$ genau dann, wenn $s|A_b(n)$.*

A **9.34.** *Berechnen Sie die alternierenden Quersummen der folgenden Zahlen (immer im angegebenen Zahlensystem): $(3943ABE3)_{16}$, $(324324)_6$.*

Beweis: Die Aussage folgt aus der folgenden Rechnung:

$$\begin{aligned} n &= (a_m, \ldots, a_0)_b \\ &= \sum_{i=0}^{m} a_i b^i \\ &\equiv \sum_{i=0}^{m} a_i (-1)^i \ (\mathrm{mod}\ s) \\ &= A_b(n) \ . \end{aligned}$$

Das heißt n und $A_b(n)$ haben den gleichen Rest bei Division mit s, dementsprechend ist die eine Zahl genau dann durch s teilbar, wenn es die andere ist. □

(A) **9.35.** *Überprüfen Sie, welche der folgenden Teilbarkeiten stimmen:* $7|(320415)_6$, $12|(21932BA)_{11}$, $5|(32032011)_4$.

Hausaufgabe 9.36. *Angenommen, wir arbeiten im Zahlensystem zur Basis* 8 *und ein Kollege von uns behauptet, Teilbarkeit durch* 6 *könne man ebenfalls mit der alternierenden Quersumme verifizieren. Entscheiden Sie, ob der Kollege recht hat. Das heißt entweder geben Sie einen Beweis oder ein Gegenbeispiel an.*

Bemerkung 9.37 (Teilbarkeit durch 13 im Zehnersystem). Als Anwendung des Materials, das wir über Teilbarkeit in Zahlensystemen gelernt haben, zeigen wir eine weitere, nicht so allgemein bekannte Teilbarkeitsregel, nämlich die durch 13 im üblichen Zehnersystem. Diese beruht auf der Zerlegung

$$1001 \;=\; 7 \cdot 11 \cdot 13 \;,$$

Es sei jetzt n eine positive ganze Zahl. Zunächst schreiben wir n im Zahlensystem zur Basis 1000 auf. Das Verhältnis zwischen dem Zehnersystem und dem 1000-ersystem ist dem zwischen dem binären und hexadezimalen Systemen sehr ähnlich: Man nimmt die Entwicklung von n im Zehnersystem, unterteilt die Ziffern in Gruppen von drei (bei Bedarf ergänzt man die Zahl vorne mit 0-en) und betrachtet die Dreiergruppen als Ziffern im 1000-ersystem, zum Beispiel

$$n \;=\; (132598078910457914385)_{10} \;=\; (132\,598\,078\,910\,457\,914\,385)_{1000} \;.$$

Aus Proposition 9.33 mit Rollenverteilung $b = 1000$ und $s = 13$ erhalten wir, dass

$$13|n \;\text{ genau dann, wenn }\; 13|A_{1000}(n) \;.$$

Die alternierende Quersumme bezüglich des 1000-ersystem wird so berechnet: Wir nehmen die 'Ziffern' (die Blöcke der länge drei) und addieren Sie alternierend im Zehnersystem auf. Dabei fangen wir von rechts an.

In unserem Beispiel oben würde das so aussehen:

$$A_{1000}(n) \;=\; 385 - 914 + 457 - 910 + 78 - 598 + 132 \;=\; -1370 \;.$$

Jetzt können wir die Frage schon per Hand entscheiden, Division mit Rest durch 13 ergibt

$$1370 \;=\; 105 \cdot 13 + 5 \;,$$

das heißt, unsere Zahl n erfüllt

$$n \equiv 5 \pmod{13} \;,$$

und ist somit nicht durch 13 teilbar.

(A) **9.38.** *Nehmen Sie Ihr Geburtsdatum (ohne Punkte oder ähnliche Sonderzeichen) als sieben- oder achtstellige Zahl und finden Sie heraus, ob sie durch* 13 *teilbar ist.*

9.4. Übungsaufgaben.

Hausaufgabe 9.39. *Welche Ziffer(n) muss man für* x *in* $(1238x4)_8$ *einsetzen, damit die Zahl durch* 16 *teilbar ist?*

9.5. Weiterführende Literatur.

10. Polynome I. (Polynome und ihre Nullstellen)

10.1. **Wiederholung.** Vollständige Induktion und der Begriff einer Abbildung zwischen Mengen aus ELMA I., Rechnen mit Buchstaben aus der Schulmathematik. Außerdem Division mit Rest und, falls gegeben, Wiederholung von Polynomdivision.

Leitfrage. *Wie viele und welche reellen Nullstellen hat das Polynom* $f(X) = 2X^4 + 4X^3 - 24X^2 - 26X + 24$*?*

10.2. **Definition und erste Eigenschaften.**

(A) **10.1.** *Rechnen Sie die folgenden Ausdrücke aus:* $(x+1)^2$*,* $(a+b)^2$*,* $(x+y)^2$*,* $(p+q+r)^2$*. Für den letzten Ausdruck empfiehlt sich eine clevere Anwendung des Assoziativgesetzes.*

Polynome sind im Grunde genommen Summen von Termen. Man lernt sie in der Schule kennen, wenn man lernt mit Buchstaben zu rechnen. Insbesondere sind Geraden und Parabeln Spezialfälle von Polynomen. Ausdrucke wie $2X^5 - YZ^6$ oder $a^2b^3c \cdot 4$ können als Polynome in den Variablen X, Y, Z beziehungsweise a, b, c betrachtet werden. In diesem Abschnitt werden wir uns mit Polynomen in einer Variablen beschäftigen. Das heißt, wir studieren solche formale Ausdrücke, in welchen nur ein Buchstabe auftaucht. Wir werden sehen, dass $4X^4 - X^3 + 2$ oder $Y - 1$ Polynome in einer Variablen sind.

Definition 10.2 (Polynome I.)**.** Ein *Polynom mit Koeffizienten aus* $\mathbb{R}$ *in der Variablen* X ist ein formaler Ausdruck

$$f(X) \stackrel{\text{def}}{=} \sum_{i=0}^{d} a_i X^i \;=\; a_d X^d + \ldots a_1 X + a_0 \;,$$

wobei d eine natürliche Zahl ist, $a_0, \ldots, a_d \in \mathbb{R}$ sind und entweder gilt $a_d \neq 0$ oder $f(X) = 0$.

Wenn $f(X) \neq 0$ ist, dann nennen wir d den *Grad von* $f(X)$ und schreiben $\operatorname{grad}(f)$ dafür. Der Grad des Nullpolynoms ist definiert als $-\infty$. Die reellen Zahlen $a_0, \ldots, a_d$ heißen *Koeffizienten von* $f(X)$, die Zahl $a_d \neq 0$ heißt *Leitkoeffizient von* $f(X)$.

Bemerkung 10.3. Das Nullpolynom 0 hat nach dieser Definition keinen Leitkoeffizienten. Wir werden jedoch sagen, dass der Leitkoeffizient vom Polynom 0 die Zahl 0 ist. Dann ist das Nullpolynom das einzige Polynom mit Leitkoeffizient $0 \in \mathbb{R}$.

Die Polynome $f(X) = \alpha$ für ein $\alpha \in \mathbb{R}$, das heißt wenn $d = 0$ und $a_0 \neq 0$ ist, werden konstante Polynome genannt.

(A) **10.4.** *Bestimmen Sie die Grade der folgenden Polynome (bezüglich der gegebenen Variablen):* 3*,* $Y - 1$*,* $1000Z - 12$*,* $2X^2 - 3X + 1$*,* $17T^6 - 12000T^2$ *und* $12U^7 + 5U^2 - 1500U - 1$*.*

Definition 10.5 (Gleichheit von Polynomen)**.** Zwei Polynome $f(X) = a_d X^d + \ldots + a_0$ und $g(X) = b_e X^e + \ldots + b_0$ in der selben Variablen mit Koeffizienten aus $\mathbb{R}$ heißen *gleich*, wenn

$$d \stackrel{\text{def}}{=} \operatorname{grad} f(X) \;=\; \operatorname{grad} g(X) \stackrel{\text{def}}{=} e \text{ und}$$
$$a_i \;=\; b_i \text{ für alle } 0 \leq i \leq d.$$

Bemerkung 10.6. Nach Definition 10.5 betrachten wir Summen von Termen als gleich, wenn einer der Terme durch Anwenden des Kommutativ- oder Assoziativgesetzes (der Addition)

aus dem anderen hervorgeht. Insbesondere trifft das auf Polynome zu. Zum Beispiel gilt das für

$$2X^2 - 5X^7 \;=\; -5X^7 + 2X^2$$

und damit ist auch $2X^2 - 5X^7$ ein Polynom (hier ist lediglich die Reihenfolge anders als in Definition 10.2: Der Leitkoeffizient steht nicht vorne). Das ist wichtig dafür, dass später die gewohnten Eigenschaften der Addition und Multiplikation erhalten bleiben.

Bemerkung 10.7. Wenn wir von *Termen* sprechen, meinen wir meistens Ausdrücke der Form $a \cdot X^n$, wobei a eine reelle Zahl ist und n eine natürliche. Der üblichere Begriff dafür ist *Monom*.

Bemerkung 10.8. Analog lassen sich Polynome mit Koeffizienten aus $\mathbb{Z}$, $\mathbb{Q}$, und vielen anderen Zahlenbereichen definieren.

(A) **10.9.** *Definieren Sie den Begriffs eines Polynoms mit Koeffizienten aus* $\mathbb{Z}$.

Als Nächstes diskutieren wir die verschiedene algebraischen Operationen (Addition, Subtraktion und Multiplikation) zwischen Polynomen.

Definition 10.10 (Addition von Polynomen)**.** Es seien $f(X) = a_n X^n + \ldots + a_1 X + a_0$ und $g(X) = b_m X^m + \ldots + b_1 X + b_0$ Polynome mit Koeffizienten aus $\mathbb{R}$ (oder $\mathbb{Q}$ oder $\mathbb{Z}$). Ohne Beschränkung der Allgemeinheit werden nehmen wir $n \geq m$ an. Dann definieren wir

$$(f+g)(X) \stackrel{\text{def}}{=} \sum_{k=0}^{n} (a_k + b'_k) X^k \;,$$

wobei

$$b'_k \stackrel{\text{def}}{=} \begin{cases} b_k & \text{wenn } 0 \leq k \leq m, \\ 0 & \text{wenn } m < k \leq n. \end{cases}$$

(A) **10.11.** *Es seien* $f(X) = 3X^2 - 2X + 1$, $g(X) = X^5 - 34X^2$ *und* $h(X) = -14X^2 + X - \pi$. *Führen Sie die folgenden Additionen aus:* $f+g$, $g+f$, $f+h$, $h+f$, $g+h$, $f+(g+h)$ *und* $(f+g)+h$.

Lemma 10.12. *Die Addition von Polynomen mit Koeffizienten aus* $\mathbb{R}$ *(oder* $\mathbb{Q}$*) ist kommutativ und assoziativ. Das heißt, für beliebige Polynome* $f, g, h \in \mathbb{R}[X]$ *gelten*

(1) *(Kommutativität)* $f + g = g + f$,
(2) *(Assoziativität)* $(f+g)+h = f+(g+h)$.

Beweis. Der Beweis beruht auf den analogen Eigenschaften der reellen Zahlen und der Definition der Addition von Polynomen.

(1) Es seien $f(X) = a_n X^n + \ldots + a_1 X + a_0$ und $g(X) = b_m X^m + \ldots + b_1 X + b_0$. Wir nehmen an, dass $n \geq m$ ist. Dann gilt

$$(f+g)(X) \;=\; \sum_{k=0}^{n} (a_k + b'_k) X^k \;=\; \sum_{k=0}^{n} (b'_k + a_k) X^k \;=\; (g+f)(X) \;.$$

(2) (*) Wir überlassen den Beweis (der analog zum Teil (1) abläuft) dem Leser.

□

Korollar 10.13. *Für Polynome $f, g \in \mathbb{R}[X]$ gilt*

$$\operatorname{grad}(f+g) \leq \max\{\operatorname{grad}(f), \operatorname{grad}(g)\} \ .$$

Beweis. Sei $d \stackrel{\text{def}}{=} \max\{\operatorname{grad}(f), \operatorname{grad}(g)\}$. Dann hat keines der beiden Polynome Koeffizienten in Graden größer als d. Daher kann auch die Summe keine solchen Koeffizienten haben. □

Beispiel 10.14. Wenn zwei Polynome f und g den gleichen Grad d haben, dann kann der Grad der Summe alles $\leq d$ sein. Für ein konkretes Beispiel seien $f(X) = 2X^7 - X + 2$ und $g(X) = -2X^7 + X^6 + 3X$. Dann ist $\operatorname{grad} f = \operatorname{grad} g = 7$, aber

$$(f+g)(X) \ = \ X^6 + 2X + 2$$

und somit $\operatorname{grad}(f+g) = 6$.

Ⓐ **10.15.** *Finden Sie für Zahl $d = 0, 1, 2, 3$ jeweils Polynome f und g vom Grad drei, sodass $\operatorname{grad}(f+g) = d$ gilt.*

Hausaufgabe 10.16. *Es seien $f, g \in \mathbb{R}[X]$ mit $\operatorname{grad} f < \operatorname{grad} g$ gegeben. Dann gilt*

$$\operatorname{grad}(f+g) \leq \max\{\operatorname{grad}(f), \operatorname{grad}(g)\} \ = \ \operatorname{grad} g \ .$$

Eine einfache Operation mit Polynomen ist die Multiplikation mit einer (reellen oder rationalen) Zahl.

Definition 10.17 (Multiplikation mit Zahlen)**.** Es sei $f(X) = a_n X^n + \ldots + a_0 \in \mathbb{R}[X]$ und $\alpha \in \mathbb{R}$ beliebig. Dann definieren wir das Polynom $\alpha \cdot f$ oder $\alpha f \in \mathbb{R}[X]$ folgendermaßen:

$$(f \cdot \alpha) \ = \ (\alpha \cdot f)(X) \stackrel{\text{def}}{=} (\alpha a_n)X^n + \ldots + (\alpha a_0) \ .$$

Ⓐ **10.18.** *Berechnen Sie jede mögliche Kombination von αf für $f(X) = 5X^3 - 2X^2 + X - 17$ bzw. $f(X) = X^7 + (\pi/2)X$ und $\alpha = -3/4$ bzw. $\alpha = 4$.*

Lemma 10.19. *Es sei $f \in \mathbb{R}[X]$ und $\alpha \in \mathbb{R}$. Dann gilt $\alpha \cdot f \ = \ 0 \in \mathbb{R}[X]$ genau dann, wenn $\alpha = 0 \in \mathbb{R}$ oder $f = 0 \in \mathbb{R}[X]$.*

Beweis. Ein Polynom ist genau dann das Nullpolynom in $\mathbb{R}[X]$, wenn alle Koeffizienten gleich Null sind. Sei $f(X) = a_n X^n + \ldots a_0$. Dann gilt

$$\alpha \cdot f \ = \ 0 \in \mathbb{R}[X] \ \text{ genau dann wenn } \ \alpha \cdot a_i \ = \ 0 \ \text{ für alle } 0 \leq i \leq n.$$

(⇒): Angenommen, $\alpha \cdot f = 0 \in \mathbb{R}[X]$. Dann ist $\alpha \cdot a_i = 0$ für alle $0 \leq i \leq n$. Falls $\alpha = 0$, dann sind wir fertig. Sei also $\alpha \neq 0$. Existiert $0 \leq i \leq n$ mit $a_i \neq 0$, dann ist auch $\alpha \cdot a_i \neq 0$, ein Widerspruch. Es muss also $a_i = 0$ für alle $0 \leq i \leq n$ gelten und somit ist $f = 0 \in \mathbb{R}[X]$.
(⇐): Wenn $\alpha = 0$ ist, dann gilt automatisch $\alpha a_i = 0$ für alle $0 \leq i \leq n$ und daher $\alpha f = 0 \in \mathbb{R}[X]$. Ist andererseits $f = 0 \in \mathbb{R}[X]$, so folgt $a_i = 0$ für alle $0 \leq i \leq n$ und somit $\alpha a_i = 0$ für alle $0 \leq i \leq n$. Also ist $\alpha f = 0 \in \mathbb{R}[X]$. □

Lemma 10.20. *Für ein Polynom $f \in \mathbb{R}[X]$ und eine Zahl $\alpha \neq 0$ gilt*

$$\operatorname{grad}(\alpha f) \ = \ \operatorname{grad}(f) \ .$$

Beweis. Es gilt

$$\alpha \cdot \sum_{i=0}^{n} a_i X^i \ = \ \sum_{i=0}^{n} (\alpha a_i) X^i \ ,$$

und wegen $\alpha \neq 0$ ist $a_n \neq 0$ genau dann, wenn $\alpha \cdot a_n \neq 0$. □

Definition 10.21 (Subtraktion von Polynomen)**.** Es seien $f, g \in \mathbb{R}[X]$. Wir definieren

$$(f-g)(X) \stackrel{\text{def}}{=} f + (-1)\cdot g \ \in \mathbb{R}[X] \ .$$

A **10.22.** *Es seien* $f(X) = 4X^3 - 5X^2 - X$, $g(X) = 5X^2 - 2X + 7$ *und* $h(X) = X^2 - X - 2$. *Führen Sie alle mögliche Subtraktionen aus.*

Hausaufgabe 10.23. *Benutzen Sie die Definition der Subtraktion um zu beweisen, dass*

$$f - (g - h) \ = \ f - g + h$$

für beliebige Polynome $f, g, h \in \mathbb{R}[X]$ *gilt.*

Bemerkung 10.24 (Multiplikation mit X). Es ist natürlich zu erwarten, dass Multiplikation mit X die Koeffizienten unverändert lässt. Für ein Polynom $f = a_n X^+ \ldots + a_0 \in \mathbb{R}[X]$ definieren wir deshalb

$$(X \cdot f)(X) \stackrel{\text{def}}{=} a_n X^{n+1} + \ldots + a_0 X \in \mathbb{R}[X] \ .$$

A **10.25.** *Berechnen Sie* $X \cdot (5X^3 - 2X^2 + 9X - 1)$.

Als nächstes beschäftigen wir uns mit der Multiplikation von Polynomen. Wir haben schon zwei konkrete Beispiele gesehen: Multiplikation mit Konstanten und mit der Variablen X. Es stellt sich heraus, dass diese Spezialfälle gemeinsam mit dem (hoffentlich geltenden) Distributionsgesetz bezüglich Addition die allgemeine Definition der Multiplikation von Polynomen erzwingen.

Beispiel 10.26. Betrachten Sie die Polynome $g(X) = 3X^2 - 2X + 5$ und $f(X) = 3X - 7$. Wir möchten $f \cdot g \in \mathbb{R}[X]$ bestimmen (wenn es überhaupt Sinn macht) basierend auf:

(1) Multiplikation mit Konstanten
(2) Multiplitaion mit X
(3) **Wunsch:** für Polynome $f_1, f_2, h \in \mathbb{R}[X]$ soll $(f_1 + f_2)\cdot h \ = \ (f_1 \cdot h) + (f_2 \cdot h) \in \mathbb{R}[X]$ gelten (Distributivgesetz).

Hier ist die Rechnung:

$$\begin{aligned}
(3X-7)\cdot(3X^2-2X+5) &\stackrel{(3)}{=} (3X)\cdot(3X^2-2X+5) + (-7)\cdot(3X^2-2X+5) \\
&\stackrel{(2)}{=} 3\cdot(3X^3-2X^2+5X) + (-7)\cdot(3X^2-2X+5) \\
&\stackrel{(1)}{=} (9X^3-6X^2+15X) + (-21X^2+14X-35) \\
&= 9X^3 - 27X^2 + 29X - 35 \ .
\end{aligned}$$

Machen wir diese Rechnung ein Stück allgemeiner: Es seien

$$f(X) \ = \ a_1 X + a_0 \quad \text{und} \quad g(X) \ = \ b_2 X^2 + b_1 X + b_0 \ .$$

Dann gilt

$$\begin{aligned}
(a_1X+a_0)\cdot(b_2X^2+b_1X+b_0) &\stackrel{(3)}{=} (a_1X)\cdot(b_2X^2+b_1X+b_0) + a_0\cdot(b_2X^2+b_1X+b_0) \\
&\stackrel{(2)}{=} a_1(b_2X^3+b_1X^2+b_0X) + a_0\cdot(b_2X^2+b_1X+b_0) \\
&\stackrel{(1)}{=} ((a_1b_2)X^3 + (a_1b_1)X^2 + (a_1b_0)X) + \\
&\quad +((a_0b+2)X^2 + (a_0b_1)X + (a_0b_0)) \\
&= (a_1b_2)X^3 + (a_1b_1 + a_0b_2)X^2 + (a_1b_0 + a_0b_1)X + (a_0b_0) \ .
\end{aligned}$$

Wir können sehen, dass der Koeffizient von X^k aus Produkten von Koeffizienten besteht, bei denen die Summe der Indizes gleich k ist.

Definition 10.27 (Multiplikation von Polynomen)**.** Es seien $f(X) = a_n X^n + \ldots + a_0$ und $g(X) = b_m X^m + \ldots + b_0$ Polynome aus $\mathbb{R}[X]$. Wird defineren das Produkt $f \cdot g \in \mathbb{R}[X]$ von f und g als

$$(f \cdot g)(X) \stackrel{\text{def}}{=} \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a'_i b'_{k-i} \right) X^k \ ,$$

wo bei

$$a'_i \stackrel{\text{def}}{=} \begin{cases} a_i & \text{wenn } 0 \leq i \leq n, \\ 0 & \text{wenn } i > n, \end{cases}$$

und

$$b'_i \stackrel{\text{def}}{=} \begin{cases} b_i & \text{wenn } 0 \leq i \leq m, \\ 0 & \text{wenn } i > m. \end{cases}$$

(A) **10.28.** *Berechnen Sie* $(2X^2 - 3X + 1) \cdot (-X^2 + 5X - 14)$.

(A) **10.29.** *Gegeben* $f(X) = a_n X^n + \ldots + a_0$ *und* $g(X) = b_m X^m + \ldots + b_0 \in \mathbb{R}[X]$*, bestimmen Sie die Koeffizienten der Terme* $1, X$ *und* X^2 *von* $f \cdot g$.

Hausaufgabe 10.30. *Gegeben* $f(X) = a_n X^n + \ldots + a_0$ *und* $g(X) = b_m X^m + \ldots + b_0 \in \mathbb{R}[X]$*, bestimmen Sie die Koeffizienten der Terme* X^{n+m-2}*,* X^{n+m-1}*, und* X^{n+m} *von* $f \cdot g$.

(A) **10.31.** *Berechnen Sie das Produkt* $(X^5 + X - 1) \cdot (X^4 - X^3 + X^2 - 2)$.

Proposition 10.32. *Die Multiplikation von Polynomen ist kommutativ und assoziativ. Das heißt für gegebene Polynome* $f, g, h \in \mathbb{R}[X]$ *gilt*

(1) *(Kommutativität)* $fg = gf$,
(2) *(Assoziativität)* $(fg)h = f(gh)$.

Beweis. (1)

$$\begin{aligned} (f \cdot g)(X) &= \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a'_i b'_{k-i} \right) X^k \\ &= \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} b'_{k-i} a'_i \right) X^k \\ &\stackrel{j=k-i}{=} \sum_{k=0}^{m+n} \left(\sum_{j=0}^{k} b'_j a'_{k-j} \right) X^k \\ &= (g \cdot f)(X) \ . \end{aligned}$$

(2) (*) Wir überlassen den Beweis (der analog zum Teil (1) abläuft) dem Leser.

□

(A) **10.33.** *Berechnen Sie* $((X-1) \cdot (X-2)) \cdot (X-3)$ *und* $(X-1) \cdot ((X-2) \cdot (X-3))$.

Hausaufgabe 10.34. *Nehmen Sie die Polynome* $f(X) = X^2 - 3X + 2$*,* $g(X) = 7X - 1$*,* $h(X) = X^5 - 5$ *und gehen Sie mit diesen Beispielen den Beweis von Proposition 10.32 durch.*

Hausaufgabe 10.35. *Was ist jeweils der konstante Term von* $(X-1)(X-2)(X-3)(X-4)$ *und* $\prod_{i=1}^{n}(X+i)$ *(wobei* n *eine positive ganze Zahl ist)? Sobald Sie eine starke Vermutung für letzteres haben, können Sie diese mittels vollständiger Induktion beweisen.*

Hausaufgabe 10.36. *Was ist der konstante Term von* $\prod_{i=1}^{n}(X+i)$*? Geben Sie einen Beweis durch vollständige Induktion.*

Als Nächstes untersuchen wir die Verbindung zwischen Multiplikation und Addition von Polynomen. Wir hoffen, dass sich unser Wunsch aus Beispiel 5.25 (3) erfüllt.

(A) **10.37.** *Es seien* $f_1(X) = 3X^3 - X + 12$*,* $f_2(X) = 5X^2 - 7X + 3$ *und* $g(X) = 2X - 1$*. Berechnen Sie*

$$(f_1 + f_2) \cdot g \quad \textit{und} \quad (f_1 \cdot g) + (f_2 \cdot g) \ .$$

Proposition 10.38 (Distributivität)**.** *Es seien* $f_1, f_2, g \in \mathbb{R}[X]$ *Polynome mit reellen Koeffizienten. Dann gilt*

$$(f_1 + f_2) \cdot g \ = \ (f_1 \cdot g) + (f_2 \cdot g) \ .$$

Beweis. □

10.3. **Nullstellen von Polynomen.** Nullstellen von Polynomen sind aus der Schule wohlbekannt. So haben Sie zum Beispiel bei Geraden untersucht, an welcher Stelle diese die x-Achse schneiden und bei quadratischen Funktionen haben sie die Mitternachtsformel bzw. abc-Formel oder pq-Formel benutzt, um die Nullstellen zu ermitteln. Vor allem bei Kurvendiskussionen und bestimmten Integralen haben Sie ständig Nullstellen ausgerechnet. So sind zum Beispiel die Extremwerte die Nullstellen der Ableitung (die x-Koordinate), die Wendepunkte die Nullstellen der zweiten Ableitung und wenn Sie die Fläche (also das Integral) zwischen zwei Funktionen (meistens waren es Polynome) f und g berechnet haben, so haben Sie zunächst die Integralgrenzen bestimmt, welche durch die Nullstellen von $f - g$ gegeben waren.

Definition 10.39 (Polynomfunktion und Nullstelle)**.** Jedes Polynom $f(X) \in \mathbb{R}[X]$ definiert eine Abbildung $\tilde{f}\colon \mathbb{R} \to \mathbb{R}$ durch Einsetzen von reellen Zahlen für X. Für $f(X) = a_nX^n + \ldots + a_0 \in \mathbb{R}[X]$ und $\alpha \in \mathbb{R}$ ist

$$\begin{array}{rccl} \tilde{f}\colon \mathbb{R} & \longrightarrow & \mathbb{R} \\ \alpha & \mapsto & a_n\alpha^n + \ldots + a_1\alpha + a_0 \ . \end{array}$$

Eine Zahl $\alpha \in \mathbb{R}$ heißt *Nullstelle von (dem Polynom)* f, falls $\tilde{f}(\alpha) = 0$ ist. Gegeben ein Polynom $f \in \mathbb{R}[X]$ schreiben wir $\mathrm{NS}(f)$ für die Menge der Nullstellen von f.

(A) **10.40.** *Betrachten Sie das Polynom* $f(X) = -3X^3 + 2X - 1$ *und berechnen Sie* $\tilde{f}(\alpha)$ *für alle* $\alpha \in \{-2, -1, 0, 1, 2\}$*.*

Bemerkung 10.41. Es ist wahr, dass zwei Polynome $f, g \in \mathbb{R}[X]$ genau dann gleich sind (das heißt, die gleichen Koeffizienten haben), wenn $\tilde{f}$ und $\tilde{g}$ als Abbildungen $\mathbb{R} \to \mathbb{R}$ gleich sind. Das ist der Grund weshalb man keinen formalen Unterschied zwischen f und $\tilde{f}$ macht.

Bemerkung 10.42. Es seien $f, g \in \mathbb{R}[X]$ Polynome. Die Nullstellen von fg sind genau die Nullstellen von f und die Nullstellen von g, in anderen Worten

$$\mathrm{NS}(fg) \ = \ \mathrm{NS}(f) \cup \mathrm{NS}(g) \ .$$

Hausaufgabe 10.43. *Beweisen Sie, dass* $\mathrm{NS}(f+g) \subseteq \mathrm{NS}(f) \cap \mathrm{NS}(g)$ *für beliebige Polynome* $f, g \in \mathbb{R}[X]$.

Bemerkung 10.44. Nullstellen von Polynomen zu bestimmen ist eine schwierige Aufgabe. In der Schule lernt man, wie man lineare (Grad 1) und quadratische (Grad 2) polynomiale Gleichungen lösen kann (das heißt, deren Nullstellen zu bestimmen). Ab Grad 3 geht es aber bergab. Für Grad 3 und 4 gibt es noch Lösungsformeln (allerdings komplizierte). Ab Grad 5 kann man beweisen, dass es keine allgemeine Lösungsformel geben kann. Allerdings besteht die Möglichkeit, den Grad mittels Polynomdivision von bekannten Nullstellen oder durch Substitution zu verringern.

Ein möglicher Weg um Nullstellen von konkreten Polynomen zu finden ist kleine ganze Zahlen, zum Beispiel $0, \pm 1, \pm 2$ und so weiter einzusetzen und zu testen, ob man Null erhält oder nicht.

Im echten Leben benutzt man Algorithmen, die die gesuchten Nullstellen approximieren.

(A) **10.45.** *Finden Sie alle reellen Nullstellen der Polynome* X^2-3X+2, $X^3-6X^2+11X-6$, *entweder mit einer Lösungsformel oder durch probieren.*

Bemerkung 10.46. Es ist nicht kompliziert Polynome mit vorgeschriebenen Nullstellen zu konstruieren. Wenn wir zum Beispiel ein Polynom vierten Grades mit Nullstellen $1, 2, 4, 8$ haben möchten, dann wird

$$(X-1)(X-2)(X-4)(X-8)$$

passen.

(A) **10.47.** *Bestimmen Sie ein Polynom vom Grad* 5, *welches nur die Nullstellen* -1,1 *und* 12 *hat. Finden Sie ein weiteres?*

Hausaufgabe 10.48. *Seien reelle Zahlen* $\alpha_1, \ldots, \alpha_n$ *gegeben. Geben Sie ein Polynom mit Grad* n *und Nullstellen* $\alpha_1, \ldots, \alpha_n$ *an.*

(A) **10.49.** *Wie viele Nullstellen kann ein lineares Polynom haben? Wie viele ein quadratisches?*

Wie wir sehen werden, gibt es einen sehr engen Zusammenhang zwischen Nullstellen und Koeffizienten eines Polynoms.

Proposition 10.50 (Viéte-Formel)**.** *Es sei* $f(X) = X^2 + pX + q \in \mathbb{R}[X]$ *ein quadratisches Polynom mit zwei unterschiedlichen Nullstellen* α_1, α_2. *Dann gelten*

$$\alpha_1 + \alpha_2 \;=\; -p \quad \textit{und} \quad \alpha_1 \alpha_2 \;=\; q \;.$$

Beweis. Aus der Lösungsformel für quadratische Gleichungen erhalten wir

$$\alpha_{1,2} \;=\; \frac{-p \pm \sqrt{p^2 - 4q}}{2} \;,$$

dementsprechend ist

$$\alpha_1 + \alpha_2 \;=\; \frac{-p + \sqrt{p^2 - 4q}}{2} + \frac{-p - \sqrt{p^2 - 4q}}{2} \;=\; p$$

und

$$\begin{aligned}\alpha_1\alpha_2 &= \frac{-p \pm \sqrt{p^2-4q}}{2} \cdot \frac{-p \pm \sqrt{p^2-4q}}{2} \\ &= \frac{1}{4} \cdot \left(p^2 - (\sqrt{p^2-4q})^2\right) \\ &= \frac{1}{4} \cdot (p^2 - (p^2-4q)) \\ &= q\ ,\end{aligned}$$

wie behauptet. □

Bemerkung 10.51. Die Viéte-Formel ermöglicht es, diverse Kombinationen von Nullstellen auszurechnen ohne die Nullstellen bestimmen zu müssen. Hier ist ein Beispiel: Betrachte das Polynom $X^2 + 17X - 109$. Man kann leicht überprüfen, dass es zwei verschiedene Nullstellen $\alpha_1 \neq \alpha_2$ hat. Wir werden jetzt $(\alpha_1 - \alpha_2)^2$ bestimmen, ohne die Nullstellen zu kennen.

Man beachte

$$(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2\ .$$

Wegen der Viéte-Formel gilt dann

$$\alpha_1 + \alpha_2 = -17 \text{ und } \alpha_1\alpha_2 = -109\ ,$$

daher ist

$$(\alpha_1 - \alpha_2)^2 = (-17)^2 - 4 \cdot (-109) = 17^2 + 436 = 725\ .$$

(A) 10.52. *Es sei $f(X) = X^2 + 11X - 123$. Bestimmen Sie die dritte Potenz der Summe der Nullstellen von $f(X)$ mithilfe der Viéte-Formel.*

Hausaufgabe 10.53. *Betrachten Sie das Polynom $f(X) = X^2 - 2X + \beta$, wobei β eine unbekannte reelle Zahl ist.*

(1) *Für welche Werte von β hat f zwei verschiedene Nullstellen?*
(2) *Berechnen Sie $(\alpha_1 - \alpha_2)^4$ für solche Werte von β.*

Bemerkung 10.54. Richtig interpretiert gilt die Viéte-Formel auch dann, wenn das quadratische Polynom $f(X) = X^2 + pX + q$ nur eine Nullstelle hat. Das kommt genau dann vor, wenn $p - 4q = 0$ ist, zum Beispiel wenn

$$f(X) = X^2 - 2X + 1 = (X-1)^2\ .$$

In diesem Fall werden wir die Nullstelle 1 als 'doppelte Nullstelle' oder 'eine Nullstelle mit Multiplizität Zwei' betrachten (obwohl wir nie präzise definiert haben, was die Multiplizität sein soll) und $\alpha_1 = \alpha_2 = 1$ schreiben.

Es sei also $f(X) = X^2 + pX + q$ ein Polynom mit einer doppelten Nullstelle, das heißt $p^2 - 4q = 0$. Aus der Lösungsformel für quadratische Gleichungen erhalten wir

$$\alpha_1 = \alpha_2 = -\frac{p}{2}\ ,$$

und daher

$$\alpha_1 + \alpha_2 = -p \text{ und } \alpha_1\alpha_2 = \frac{(-p)^2}{4} = q\ .$$

Bemerkung 10.55. Eine Nullstelle ist doppelt, wenn sie auch eine Nullstelle der Ableitung ist (die Ableitung eines Polynoms ist ein Polynom).

Bemerkung 10.56. Die Viéte–Formel gibt es in leicht veränderter Form für das allgemeine quadratische Polynom $f(X) = aX^2 + bX + c$, wobei wir annehmen, dass $a \neq 0$. Man benutzt die Umrechnung

$$aX^2 + bX + c \;=\; a\left(X^2 + \frac{b}{a}X + \frac{c}{a}\right)$$

und die Beobachtung, dass die Nullstellen von $aX^2 + bX + c$ und $X^2 + (b/a)X + (c/a)$ genau die gleichen sind (nach Bemerkung 10.42). Somit erhalten wir

$$\alpha_1 + \alpha_2 \;=\; -\frac{b}{a} \quad \text{und} \quad \alpha_1\alpha_2 \;=\; \frac{c}{a}$$

Hausaufgabe 10.57. *Geben Sie einen detailierten Beweis für die allgemeine Viéte-Formel an. Hierzu dürfen Sie Proposition 10.50 verwenden.*

(A) **10.58.** *Es seien α_1, α_2 die Nullstellen des Polynoms $2X^2 + 6X + 4$. Bestimmen Sie $(\alpha_1 - \alpha_2)^2$.*

Genau wie für ganze Zahlen gibt es auch für Polynome Division mit Rest (Polynomdivision).

Satz 10.59 (Division mit Rest für Polynome)**.** *Es seien $f, d \in \mathbb{R}[X]$ Polynome. Dann existieren eindeutig definierte Polynome $q, r \in \mathbb{R}[X]$ so dass*

(1) $f \;=\; qd + r$, *wobei*
(2) *entweder* $r = 0 \in \mathbb{R}[X]$ *oder* $\operatorname{grad} r < \operatorname{grad} d$.

Beweis. Wir werden diese Aussage ohne Beweis als 'Black Box' annehmen. □

(A) **10.60.** *Führen Sie Division mit Rest durch für $f(X) = X^3 - 2X + 1$ und $d(X) = X - 1$.*

Division mit Rest liefert uns eine wichtige obere Schranke für die Anzahl der Nullstellen eines Polynoms.

Satz 10.61. *Ein Polynom $0 \neq f \in \mathbb{R}[X]$ vom Grad n kann höchstens n Nullstellen haben.*

Beweis. Wir beweisen den Satz mittels vollständiger Induktion über den Grad von f.
Induktionsanfang: Wenn $\operatorname{grad} f = 0$ ist, dann ist wegen $f \neq 0 \in \mathbb{R}[X]$ das Polynom f konstant. Da es aber nach Voraussetzung von $0 \in \mathbb{R}$ verschieden ist, hat es keine Nullstellen.
Induktionsschluss: Sei nun $n > 0$. Unsere Induktionsannahme ist, dass ein Polynom vom Grad $n - 1$ höchstens $n - 1$ Nullstellen haben kann. Sei jetzt f ein Polynom von Grad n. Wenn f keine Nullstellen hat, dann sind wir wegen $0 \leq n - 1 < n$ fertig.

Nehmen wir also an, dass f eine Nullstelle $\alpha \in \mathbb{R}$ hat. Wir teilen f durch $X - \alpha$ mit Rest:

$$f(X) \;=\; q(X) \cdot (X - \alpha) + r(X)\ , \tag{10.1}$$

wobei entweder $r(X)$ das Nullpolynom ist oder $\operatorname{grad} r \;<\; \operatorname{grad}(X - \alpha) \;=\; 1$. Das heißt, $r(X) \in \mathbb{R}[X]$ ist ein konstantes Polynom. Die Frage ist, was diese Konstante ist. Setzen wir α für X ein in der Gleichung (10.1):

$$0 \;=\; f(\alpha) \;=\; q(\alpha) \cdot (\alpha - \alpha) + r(\alpha)',$$

so folgt, dass $r = 0 \in \mathbb{R}[X]$. Dann gilt aber

$$f(X) \;=\; q(X) \cdot (X - \alpha)\ ,$$

und

$$n \;=\; \operatorname{grad} f \;=\; \operatorname{grad} q + \operatorname{grad}(X - \alpha) \;=\; \operatorname{grad}(q) + 1\ .$$

Dadurch erhalten wir $\operatorname{grad} q = n - 1$.

Nach der Induktionsannahme hat $q(X)$ höchstens $n - 1$ Nullstellen. Die Nullstellen von f sind die Nullstellen von q und α und somit ist deren Anzahl höchstens n. □

Korollar 10.62. *Es sei $f \in \mathbb{R}[X]$ ein Polynom vom Grad höchstens n. Falls f mehr als n Nullstellen hat, dann muss es das Nullpolynom sein.*

(A) **10.63.** *Es sei $f \in \mathbb{R}[X]$ ein Polynom vom Grad 7 mit der Eigenschaft, dass*

$$f(m) = 2 \quad \text{für jedes } 1 \leq m \leq 8.$$

Was können Sie über f sagen?

Bemerkung 10.64. Satz 10.61 ermöglicht die Bestimmung der Nullstellen von Polynomen höheren Grades ohne Lösungsformel in vielen Fällen. Es sei $f \in \mathbb{R}[X]$ ein Polynom und wir nehmen an, dass wir eine Nullstelle α irgendwie erraten können. Dann gilt $(X - \alpha) | f(X)$, und daher können wir

$$f(X) = f_1(X) \cdot (X - \alpha)$$

berechnen. Um die restlichen Nullstellen von f zu bestimmen, können wir mit f_1 weiterarbeiten, dessen Grad kleiner als $\operatorname{grad} f$ ist.

Beispiel 10.65. Betrachten wir das Polynom $f(X) = X^3 - 6X^2 + 11X - 6$. Durch Probieren erraten wir, dass f eine Nullstelle bei 1 hat. Teilen durch $X - 1$ ergibt

$$f(X) = (X^2 - 5X + 6)(X - 1) \ .$$

Uns bleibt jetzt übrig die Nullstellen von $X^2 - 5X + 6$ zum Beispiel durch die Lösungsformel zu bestimmen. Am Ende erhalten wir

$$\mathrm{NS}(X^3 - 6X^2 + 11X - 6) = \{1, 2, 3\} \ .$$

Wir sind nun in der Lage die Leitfrage ausführlich zu beantworten:

Beispiel 10.66. Gegeben sei das Polynom

$$f(X) = 2X^4 + 4X^3 - 24X^2 - 26X + 24.$$

Wir möchten alle Nullstellen von $f(X)$ bestimmen.

Zuallererst stellen wir fest, dass $2 | f(X)$. Wegen Bemerkung 10.42 können wir daher stattdessen die Nullstellen von

$$g(X) \stackrel{\text{def}}{=} X^4 + 2X^3 - 12X^2 - 13X + 12$$

bestimmen, da $\mathrm{NS}(f) = \mathrm{NS}(g) \cup \mathrm{NS}(2)$ und die Nullstellenmenge von konstanten Polynomen leer ist, also $\mathrm{NS}(f) = \mathrm{NS}(g)$. Es ist immer eine gute Idee den ggT der Koeffizienten herauszuteilen, da wir so tendenziell mit kleineren Zahlen rechnen müssen. Außerdem wissen wir wegen Satz 10.61, dass f bzw. g höchstens 4 reelle Nullstellen haben kann. Nun zur Berechnung. Da g leider Monome vom ungeraden Grad (z.B. $2X^3$), als auch Monome vom geraden Grad (z.B. X^4) hat, können wir nicht substituieren.

Bemerkung: Für Polynome der Form $aX^4 + bX^2 + c$ können wir $Y = X^2$ substituieren und zunächst die Nullstellen von $aY^2 + bY + c$ mit unserer Lieblingslösungsformel bestimmen. Ziehen wir dann jeweils die Wurzel (Resubstitution), so erhalten wir die gesuchten 4 Nullstellen (falls existent).

Es führt also kein Weg an der Polynomdivision, also Satz 10.59 vorbei (Ihr Taschenrechner aus der Schule sollte die Nullstellen von Polynomen bis Grad 3 berechnen können). Dafür müssen wir zunächst eine Nullstelle raten. Üblicherweise versucht man sein Glück mit kleinen Zahlen und geht (betragsmäßig) immer Eins hoch, wenn es nicht klappt:

$$\begin{aligned} f(0) &= 12 \\ f(1) &= -10 \\ f(-1) &= 12 \\ f(2) &= -30 \\ f(-2) &= -10 \\ f(3) &= 0. \end{aligned}$$

Also ist 3 eine Nullstelle, somit gilt $(X-3)|g(X)$ und wir können Division mit Rest machen:

$$\begin{array}{rl} \Big(& X^4+2X^3-12X^2-13X+12\Big) : \Big(X-3\Big) = X^3+5X^2+3X-4 \\ \underline{-X^4+3X^3} & \\ 5X^3-12X^2 & \\ \underline{-5X^3+15X^2} & \\ 3X^2-13X & \\ \underline{-3X^2+9X} & \\ -4X+12 & \\ \underline{4X-12} & \\ 0 & \end{array}$$

Somit müssen wir noch die Nullstellen von $h(X) = X^3+5X^2+3X-4$ bestimmen. Diese könnten Sie jetzt rein theoretisch mit dem Taschenrechner bestimmen. Machen wir aber nicht. Stattdessen suchen wir wie zuvor für $g(X)$ eine Nullstelle und teilen den davon erzeugten linearen Term raus. Nach ausreichend langem ausprobieren finden wir $h(-4) = 0$. Division mit Rest liefert dann:

$$\begin{array}{rl} \Big(& X^3+5X^2+3X-4\Big) : \Big(X+4\Big) = X^2+X-1 \\ \underline{-X^3-4X^2} & \\ X^2+3X & \\ \underline{-X^2-4X} & \\ -X-4 & \\ \underline{X+4} & \\ 0 & \end{array}$$

Es bleibt also $p(X) = X^2+X-1$ übrig. Da p Grad 2 hat, können wir mit der abc-Formel lösen und erhalten

$$X_{3,4} = \frac{1}{2}(-1 \pm \sqrt{5}).$$

Insgesamt ist also

$$\mathrm{NS}(f) = \{3, -4, \frac{1}{2}(-1+\sqrt{5}), \frac{1}{2}(-1-\sqrt{5})\}$$

(A) **10.67.** *Bestimmen Sie* alle *reellen Nullstellen des Polynoms* X^3-3X^2+X *und begründen Sie, wieso es keine weiteren geben kann!*

Hausaufgabe 10.68. *Bestimmen Sie alle Nullstellen der Polynome* $X^3 - 6X^2 + 3X + 10$, $X^4 - 4X^3 + 6X^2 - 4X + 1$ *und* $X^5 + 10X^4 + 40X^3 + 80X^2 + 80X + 32$.

Hausaufgabe 10.69. *Es seien* $f, g \in \mathbb{R}[X]$ *Polynome vom Grad höchstens* n *und* $\alpha_1, \ldots, \alpha_{n+1}$ *paarweise verschiedene reelle Zahlen. Wir nehmen an, dass*

$$f(\alpha_i) \;=\; g(\alpha_i) \quad \textit{für jedes } 1 \le i \le n+1.$$

Beweisen Sie, dass dann bereits $f = g$ *gelten muss.*

Zum Abschluss zeigen wir eine Methode, mit der man die rationalen Nullstellen eine Polynoms $f \in \mathbb{Q}[X]$ finden kann.

Beispiel 10.70. Es kommt oft vor, dass ein Polynom $f(X) \in \mathbb{Q}[X]$ (das heißt mit rationalen Koeffizienten) keine rationalen, sondern nur reelle Nullstellen hat. Ein bekanntes Beispiel dafür ist $X^2 - 2$ mit Nullstellen $\pm\sqrt{2} \notin \mathbb{Q}$, oder im Allgemeinen $X^2 - p$ für eine Primzahl $p \in \mathbb{Z}$.

Satz 10.71 (Rationale Nullstellen)**.** *Es sei* $f(X) = a_n X^n + \ldots + a_0 \in \mathbb{Q}[X]$ *ein Polynom mit ganzzahligen Koeffizienten und* $a_0 \neq 0$. *Falls* $p/q \in \mathbb{Q}$ *eine Nullstelle von* f *ist (wir nehmen an, dass* $\mathrm{ggT}(p, q) = 1$*), dann gilt*

$$q | a_n \quad \textit{und} \quad p | a_0.$$

Beweis. Wir setzen p/q für X ein:

$$f(p/q) \;=\; \sum_{k=0}^{n} a_k \left(\frac{p}{q}\right)^k \;=\; a_n \left(\frac{p}{q}\right)^n + \ldots + a_1 \left(\frac{p}{q}\right) + a_0 \;=\; 0\ ,$$

da p/q nach Voraussetzung eine Nullstelle von f ist. Wir multiplizieren beide Seiten mit q^n und erhalten

$$\sum_{k=0}^{n} a_k p^k q^{n-k} \;=\; a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_1 p q^{n-1} + a_0 q^n \;=\; 0\ . \tag{10.2}$$

Zunächst behandeln wir die Teilbarkeit $q | a_n$. Zu diesem Zweck formen wir die obige Gleichung um:

$$q(a_{n-1} p^{n-1} + \ldots + a_0 q^{n-1}) \;=\; -a_n p^n\ .$$

Da q und p teilerfremd sind, sind es auch q und p^n. Wir sehen, dass $q | a_n p^n$, woraus wegen der Teilerfremdheit von q und p^n die Teilbarkeit $q | a_n$ folgt.

Was die Aussage $p | a_0$ betrifft, so formen wir jetzt die Gleichung (10.2) auf eine andere Weise um:

$$p(a_n p^{n-1} + \ldots + a_1 q^{n-1}) \;=\; -a_0 q^n\ .$$

Wieder gilt, aus p und q teilerfremd folgt, dass p und q^n teilerfremd sind und deswegen können wir aus $p | a_0 q^n$ die Folgerung $p | a_0$ schließen. □

Beispiel 10.72. Betrachten wir das Polynom $f(X) = X^2 + 10X - 13$. Mit der Hilfe von Satz 10.71 werden wir zeigen, dass f *keine* rationalen Nullstellen hat. In der Tat, eine rationale Nullstelle p/q müsste $q | 1$ und $p | 13$ erfüllen, woraus $q = \pm 1$ und $p = \pm 1, \pm 13$ folgt. Insgesamt erhalten wir die Liste von Kandidaten $\pm 1, \pm 13$, wo wir einzeln prüfen können, das keine Kombination der Kandidaten eine Nullstelle von f ergibt.

A **10.73.** *Bestimmen Sie die rationalen Nullstellen des Polynoms* $X^{17} - X + 1$.

Korollar 10.74. *Es sei $f(X) \in \mathbb{Q}[X]$ ein Polynom mit ganzzahligen Koeffizienten und Leitkoeffizient 1. Dann sind alle rationalen Nullstellen von f ganze Zahlen.*

Beweis. Es sein $p/q \in \mathbb{Q}$ eine rationale Nullstelle von f. Laut Satz 10.71 muss $q|1$ gelten, da der Leitkoeffizient gleich 1 ist. Es folgt sofort, dass p/q eine ganze Zahl ist. □

10.4. **Polynome als Zahlenfolgen.** Mit der üblichen Definition von Polynomen aus dem vorherigen Abschnitt kann man gut arbeiten. Problem: Wir haben nicht definiert, was eine (formale) Variable ist. Da wir versuchen die ganze Mathematik auf Mengentheorie aufzubauen, ist diese Situation nicht befriedigend. Hier werden wir zeigen, wie man dieses Problem löst.

Definition 10.75 (Zahlenfolgen)**.** Eine *Folge in* $\mathbb{R}$ oder eine *reelle Zahlenfolge* ist eine Abbildung $f\colon \mathbb{N}_+ \to \mathbb{R}$. Es ist üblich eine Zahlenfolge nicht als Abbildung, sondern als Folge $f(1), f(2), \dots$ darzustellen.

Bemerkung 10.76. Die natürliche Definition einer Zahlenfolge wäre eine Abbildung $f\colon \mathbb{N} \to \mathbb{R}$. Das würde aber bedeuten, dass unsere Folgen offiziell mit $f(0)$ anfangen würden. Da die ganze Welt Folgen ab $f(1)$ hinschreibt, benutzen wir diese Variante. Es ist nicht schwierig zu sehen, dass die zwei Versionen äquivalent sind.

Beispiel 10.77. Betrachten wir die Abbildung $f\colon \mathbb{N} \to \mathbb{R}$, die durch $m \mapsto 2m-1$ definiert wird. Die entsprechende Zahlenfolge ist

$$-1, 1, 3, \dots, 2m-1, \dots \ .$$

Definition 10.78 (Polynome II.)**.** *Ein Polynom mit Koeffizienten aus* $\mathbb{R}$ ist eine Folge $f\colon \mathbb{N} \to \mathbb{R}$, so dass ein $m_0 \in \mathbb{N}$ existiert mit $f(m) = 0$ für alle $m \geq m_0$. Das größte $m \in \mathbb{N}$ für welches $f(m) \neq 0$ gilt nennen wir den *Grad des Polynoms* f.

Bemerkung 10.79. Wir zeigen in einem konkreten Beispiel, wie die beiden Definitionen zusammenpassen. Zunächst sei $f(X) = 5X^4 - 3X^3 + 7X^2 - X + 2 \in \mathbb{R}[X]$. Als Zahlenfolge entspricht f der Folge

$$2, -1, 7, -3, 5, 0, \dots \ .$$

Achtung, die Folge entspricht nicht der Folge $f(1), f(2), \dots$, bei der natürliche Zahlen in das Polynom eingesetzt werden, sondern es handelt sich um die Folge der Koeffizienten von $f(X)$, beginnend mit dem Koeffizienten von X^0.

Umgekehrt, aus der Folge $2, 7, -1, 0, 3, 0, \dots$ erhalten wir das Polynom $3X^4 - X^2 + 7X + 2$.

Im Allgemeinen gelten

$$\text{aus } \sum_{i=0}^{n} a_i X^i \text{ wird } \ a_0, a_1, \dots, a_n, 0, \dots \ ,$$

und

$$\text{aus der Folge } f(1), f(2), \dots, f(m), 0, \dots \text{ wird } f(m)X^{m-1} + \dots + f(2)X + f(1) = \sum_{i=0}^{m-1} f(i+1)X^i \ .$$

(A) 10.80. *Beschreiben Sie die folgenden Polynome als Zahlenfolgen: $X^7 - 3X^4 + 12\pi$, -1, X^{12}, $-X^4 - X^3 - X^2 - X - 1$ und überprüfen Sie anschließend, ob man aus diesen Folgen die ursprünglichen Polynome erhält.*

Als Nächstes betrachten wir algebraische Operationen auf Polynomen als Zahlenfolgen. Wir definieren die Addition und Multiplikation mit einer Zahl 'punktweise', wie es für Abbildungen üblicherweise gemacht wird (siehe auch Bemerkung 3.9).

Definition 10.81 (Addition, Multiplikation mit Zahlen)**.** Es seien $f, g \cdot \mathbb{N}_+ \to \mathbb{R}$ Polynome (als Zahlenfolgen) und $\alpha \in \mathbb{R}$. Dann definieren wir

$$\begin{array}{rccl} f+g\colon \mathbb{N}_+ & \to & \mathbb{R} \\ m & \mapsto & f(m)+g(m)\ , \end{array}$$

und

$$\begin{array}{rccl} \alpha \cdot f\colon \mathbb{N}_+ & \to & \mathbb{R} \\ m & \mapsto & \alpha \cdot f(m)\ . \end{array}$$

(A) **10.82.** *Berechnen Sie alle möglichen Summen der Polynome* $0,0,3,0,3,1,0,\ldots,1,2,3,4,5,0,\ldots$ *und* $-1/2, 3/4, 2, 1, 0, \ldots$ *(von jeweils zwei Polynomen).*

(A) **10.83.** *Sei* $f \stackrel{def}{=} 0,1,3,0,5,0,\ldots$, $g \stackrel{def}{=} 5,-4,3,-2,1,0,\ldots$ *und* $\alpha = 1/2$*. Berechnen Sie* αf *und* αg*.*

Proposition 10.84. *Die Addition von Polynomen als Zahlenfolgen ist kommutativ und assoziativ. Das heißt für* $f, g, h\colon \mathbb{N}_+ \to \mathbb{R}$ *gilt*

(1) $f+g = g+f$ *und*
(2) $(f+g)+h = f+(g+h)$*.*

Beweis. (1) Es sei $m \in \mathbb{N}_+$ beliebig, dann gilt

$$(f+g)(m) = f(m)+g(m) = g(m)+f(m) = (g+f)(m)$$

wegen der Kommutativität der Addition der reellen Zahlen und der Definition der Addition von Polynomen.

(2) Es sei $m \in \mathbb{N}_+$ beliebig, dann

$$\begin{array}{rcl} ((f+g)+h)(m) & = & (f+g)(m)+h(m) \\ & = & (f(m)+g(m))+h(m) \\ & = & f(m)+(g(m)+h(m)) \\ & = & f(m)+(g+h)(m) \\ & = & (f+(g+h))(m)\ , \end{array}$$

wobei wir die Definition der Addition von Polynomen und die Assoziativität der Addition von reellen Zahlen benutzt haben.

□

Hausaufgabe 10.85. *Überprüfen Sie, dass die Addition von Polynomen als Zahlenfolgen mit der vorherigen Definition kompatibel ist. Präziser gesagt, seien* $f, g \in \mathbb{R}[X]$ *Polynome und man schreibe* $\Phi(f), \Phi(g)\colon \mathbb{N}_+ \to \mathbb{R}$ *für die zugehörigen Zahlenfolgen. Beweisen Sie, dass*

$$\Phi(f+g) = \Phi(f)+\Phi(g)\ .$$

Diese Eigenschaft liefert einen alternativen Beweis für die Kommutativität und Assoziativität der Polynome als Zahlenfolgen.

Definition 10.86. Es seien $f, g\colon \mathbb{N}_+ \to \mathbb{R}$ Polynome. Das *Produkt* $f * g\colon \mathbb{N}_+ \to \mathbb{R}$ definieren wir wie folgt:

$$\begin{aligned} f * g\colon \mathbb{N}_+ &\to \mathbb{R} \\ m &\mapsto \sum_{k=1}^{m+1} f(k)g(m-k)\ . \end{aligned}$$

(A) **10.87.** *Berechnen Sie $f * g$ für $f = 1, 2, 3, 4, 5, 0, \ldots$ und $g = 1, 1, 1, 1, 1, 1, 0, \ldots$.*

Bemerkung 10.88. Wir schreiben vorübergehend $f * g$ statt $f \cdot g$ oder fg, weil letzteres im Kontext von Folgen die *punktweise* Multiplikation

$$\begin{aligned} fg\colon \mathbb{N}_+ &\to \mathbb{R} \\ m &\mapsto f(m)g(m) \end{aligned}$$

meint, welche *nicht* die gewünschten Eigenschaften liefert.

(A) **10.89.** *Es seien $f = 0, 2, 5, 4, 0, \ldots$ und $g = 2, 0, 0, 0, 2, 0, \ldots$. Vergewissern Sie sich, dass $f * g$ und die punktweise Multiplikation fg nicht gleich sind.*

Bemerkung 10.90. Die Operation $*$ ist für beliebige Zahlenfolgen unverändert sinnvoll. In diesem Kontext nennt man $f * g$ die *Konvolution der Folgen f und g*. Als illustratives Beispiel betrachten wir $f, g\colon \mathbb{N}_+ \to \mathbb{R}$ mit Abbildungsvorschriften

$$f(m) = m \text{ bzw. } g(m) = 1 \quad \text{für alle } m \in \mathbb{N}_+.$$

Dann gilt für $m \in \mathbb{N}_+$ mit dem kleinen Gauß

$$(f * g)(m) = \sum_{k=1}^{m+1} f(k)g(m-k) = \sum_{k=1}^{m+1} k \cdot 1 = \frac{(m+1)(m+2)}{2}\ .$$

(A) **10.91.** *Bestimmen Sie $f * f\colon \mathbb{N}_+ \to \mathbb{R}$ mit der Notation aus Bemerkung 10.90.*

Hausaufgabe 10.92. *Bestimmen Sie $f * f * f\colon \mathbb{N}_+ \to \mathbb{R}$ mit der Notation von Bemerkung 10.90.*

Proposition 10.93. *Die Multiplikation von Polynomen (definiert als Konvolution von Zahlenfolgen) ist kommutativ und assoziativ. Das heißt es es gilt*

(1) $f * g = g * f$ *und*
(2) $(f * g) * h = f * (g * h)$

für beliebige Polynome als Zahlenfolgen $f, g, h\colon \mathbb{N}_+ \to \mathbb{R}$.

Beweis. Der Beweis ist notationstechnisch kompliziert und nicht sehr erhellend, daher werden wir uns damit nicht beschäftigen. □

Bemerkung 10.94. **Vorsicht:** Für ein Polynom $f \in \mathbb{R}[X]$ sind die Polynomfunktion $\tilde{f}\colon \mathbb{R} \to \mathbb{R}$ und das Polynom $f\colon \mathbb{N}_+ \to \mathbb{R}$ als Zahlenfolge zwei *wesentlich verschiedene Objekte*. Es ist zum Beispiel grob falsch, dass $\tilde{f}$ eingeschränkt auf $\mathbb{N}_+$ die Zahlenfolge f wäre.

Proposition 10.95. *Die Multiplikation von Polynomen als Zahlenfolgen zusammen mit der Addition (von Polynomen als Zahlenfolgen) erfüllt das Distributivgesetz. Das hießt für beliebige Polynome $f, g, h\colon \mathbb{N}_+ \to \mathbb{R}$ gilt*

$$f * (g + h) = (f * g) + (f * h)\ .$$

Beweis. Für $m \in \mathbb{N}_+$ gilt

$$\begin{aligned}
(f * (g+h))(m) &= \sum_{k=1}^{m+1} f(k)((g+h)(m-k)) \\
&= \sum_{k=1}^{m+1} f(k)(g(m-k)+h(m-k)) \\
&= \sum_{k=1}^{m+1} f(k)g(m-k) + f(k)h(m-k) \\
&= \sum_{k=1}^{m+1} f(k)g(m-k) + \sum_{k=1}^{m+1} f(k)h(m-k) \\
&= (f*g)(m) + (f*h)(m) \ .
\end{aligned}$$

□

10.5. **Übungsaufgaben.**

10.6. **Weiterführende Literatur.**

11. Polynome II. (Irreduzibilität und rationale Funktionen)

Leitfrage. *Wie kann man beweisen, dass das Polynom $f(X) = X^7 + 14X^5 + 20 \in \mathbb{Q}[X]$ nicht als Produkt von nicht-konstanten Polynomen kleineren Grades mit Koeffizienten aus $\mathbb{Q}$ geschrieben werden kann?*

11.1. **Irreduzible Polynome.** Irreduzible Polynome in $\mathbb{R}[X]$ oder $\mathbb{Q}[X]$ spielen die Rolle von Primzahlen in $\mathbb{Z}$. Im Gegensatz zu Operationen für Polynome, wo der Zahlenbereich nicht so wichtig war, wird hier eine entscheidende Rolle spielen, ob wir Polynome über $\mathbb{Q}$ oder über $\mathbb{R}$ betrachten.

Definition 11.1 (Irreduzibilität)**.** Ein Polynom $f \in \mathbb{Q}[X]$ heißt *reduzibel*, falls es nicht-konstante Polynome $g, h \in \mathbb{Q}[X]$ mit $1 \leq \operatorname{grad} g, \operatorname{grad} h < \operatorname{grad} f$ gibt, sodass $f = gh$ gilt. Polynome, die nicht reduzibel sind, heißen *irreduzibel*.

Bemerkung 11.2 (Irreduzibilität über $\mathbb{R}$). Wir definieren reduzible und irreduzible Polynome mit Koeffizienten aus $\mathbb{R}$ analog. Man muss aber aufpassen, da es Polynome $f \in \mathbb{Q}[X]$ gibt, die als Element von $\mathbb{Q}$ irreduzibel sind, als Element von $\mathbb{R}[X]$ aber nicht.

Beispiel 11.3. Wegen $X^2 + 3X + 2 = (X + 1)(X + 2)$ ist das Polynom $X^2 + 3X + 2 \in \mathbb{R}[X]$ reduzibel.

Beispiel 11.4 (Lineare Polynome sind irreduzibel). Jedes lineare Polynom in $\mathbb{R}[X]$ ist irreduzibel. Das können wir wie folgt sehen: Es sei $f = aX + b \in \mathbb{R}[X]$ ein lineares Polynom. Angenommen, es ist doch reduzibel, also $f = gh$ für zwei nicht-konstante Polynome $g, h \in \mathbb{R}[X]$. Wegen der Eigenschaften des Grades gilt dann

$$1 \;=\; \operatorname{grad} f \;=\; \operatorname{grad}(gh) \;=\; \operatorname{grad} g + \operatorname{grad} h \leq 1 + 1 \;=\; 2\ ,$$

ein Widerspruch. Also muss f irreduzibel sein.

(A) **11.5.** *Zeigen Sie die Aussage von Beispiel 11.4 für Polynome mit Koeffizienten aus $\mathbb{Q}$. Ist es wichtig ob wir die Koeffizienten aus $\mathbb{R}$, $\mathbb{Q}$ oder gar $\mathbb{Z}$ nehmen?*

(A) **11.6.** *Welche der folgenden quadratischen Polynome aus $\mathbb{R}[X]$ sind reduzibel, welche irreduzibel: $X^2 - 1$, $X^2 - 3X + 2$, $X^2 + 1$ und $X^2 - 2$?*

Aussage 11.7. *Es sei $f(X) = aX^2 + bX + c \in \mathbb{R}[X]$ ein quadratisches Polynom (insbesondere gilt $a \neq 0$). Dann ist f genau dann reduzibel, wenn die Gleichung*

$$f(X) \;=\; 0$$

(mindestens) eine Nullstelle in $\mathbb{R}$ hat.

(A) **11.8.** *Für welche Werte von $\alpha \in \mathbb{R}$ ist das Polynom $f(X) = 2X^2 - 5X + \alpha \in \mathbb{R}[X]$ irreduzibel?*

Beweis von Aussage 11.7. ($\Rightarrow$): Sei f reduzibel. Dann gibt es nicht-konstante Polynome $g, h \in \mathbb{R}[X]$ mit $f = gh$. Da g, h nicht-konstant sind, folgt $\operatorname{grad} g, \operatorname{grad} h \geq 1$. Zusammen mit der Gradgleichung

$$2 \;=\; \operatorname{grad} f \;=\; \operatorname{grad}(gh) \;=\; \operatorname{grad} g + \operatorname{grad} h \;\geq\; 1 + 1 \;=\; 2$$

folgt, dass $\operatorname{grad} g$ und $\operatorname{grad} h$ beide gleich 1 sein müssen. Sei also $g(X) = \alpha X + \beta$ für $\alpha, \beta \in \mathbb{R}$ und $\alpha \neq 0$ (ansonsten wäre g konstant). Dann gilt

$$g(-\beta/\alpha) \;=\; \alpha \cdot (-\beta/\alpha) + \beta \;=\; 0\ ,$$

woraus

$$f(-\beta/\alpha) \;=\; (gh)(-\beta/\alpha) \;=\; g(-\beta/\alpha) \cdot h(-\beta/\alpha) \;=\; 0 \cdot h(-\beta/\alpha) \;=\; 0$$

folgt. Also ist die Zahl $-\beta/\alpha$ eine Nullstelle von f.

(⇐): Da $f(X)$ eine Nullstelle hat, folgt aus der quadratischen Lösungsformel (oder quadratischer Ergänzung), dass entweder

$$f(X) \;=\; \alpha(X-\gamma)^2 \quad \text{oder} \quad f(X) \;=\; \alpha(X-\gamma_1)(X-\gamma_2)$$

mit $\alpha, \gamma, \gamma_1, \gamma_2 \in \mathbb{R}$ gilt, aber in beiden Fällen zerfällt f in Linearfaktoren (soll heißen: f ist Produkt von linearen Polynomen). Es folgt, dass f reduzibel ist. □

Hausaufgabe 11.9. *Formulieren und beweisen Sie Aussage 11.7 für $\mathbb{Q}$ statt $\mathbb{R}$. Was ist anders als im reellen Fall?*

Beispiel 11.10. Wir werden jetzt illustrieren, dass die Irreduzibilität eines Polynoms davon abhängen kann, in welchem Zahlenbereich wir es betrachten. Als Beispiel nehmen wir

(1) $f(X) = X^2 - 2 \in \mathbb{R}[X]$, und
(2) $g(X) = X^2 - 2 \in \mathbb{Q}[X]$.

Das Polynom $f(X) \in \mathbb{R}[X]$ ist laut Aussage 11.7 *reduzibel* und in der Tat lässt es sich als

$$f(X) \;=\; (X + \sqrt{2})(X - \sqrt{2})$$

zerlegen.

Andererseits hat das Polynom $g(X)$ keine Nullstellen in $\mathbb{Q}$, da alle rationalen Nullstellen zugleich reelle Nullstellen sind, aber davon gibt es nur $\pm\sqrt{2} \notin \mathbb{Q}$. Insbesondere ist $g(X)$ irreduzibel.

(A) **11.11.** *Geben Sie einen direkten Beweis dafür, dass $X^2 - 2 \in \mathbb{Q}[X]$ irreduzibel ist, indem Sie annehmen, dass es lineare Polynome $X + \alpha, X + \beta \in \mathbb{Q}[X]$ gibt, für welche*

$$(X + \alpha)(X + \beta) \;=\; X^2 - 2$$

gilt, und einen Widerspruch anstreben.

Aussage 11.12. *Es sei $f \in \mathbb{Q}[X] \subseteq \mathbb{R}[X]$ ein Polynom mit rationalen Koeffizienten.*

(1) *Falls $f \in \mathbb{Q}[X]$ reduzibel ist, dann ist auch $f \in \mathbb{R}[X]$ reduzibel;*
(2) *falls $f \in \mathbb{R}[X]$ irreduzibel ist, dann ist auf $f \in \mathbb{Q}[X]$ irreduzibel.*

Beweis. Die Idee des Beweises ist, dass jede rationale Zahl reell ist. Es sei also $f \in \mathbb{Q}[X]$. Wenn f als Polynom aus $\mathbb{Q}[X]$ betrachtet reduzibel ist, bedeutet das, dass Polynome $g, h \in \mathbb{Q}[X]$ mit $f = gh$ existieren. Da aber $g, h \in \mathbb{Q}[X] \subseteq \mathbb{R}[X]$ sind, gilt die Gleichheit $f = gh$ auch in $\mathbb{R}[X]$, insbesondere ist $f \in \mathbb{R}[X]$ reduzibel. Die zweite Aussage ist die Kontraposition der Ersten. □

Bemerkung 11.13. Polynome mit reellen Koeffizienten vom Grad mindestens 4 können auch reduzibel sein ohne Nullstellen zu haben. Ein Beispiel ist

$$f(X) \;=\; (X^2 + 1)^m \;\in\; \mathbb{R}[X]\ ,$$

welches Grad $2m$ hat und offensichtlich reduzibel ist, aber wegen $\alpha^2+1>0$ für $\alpha\in\mathbb{R}$ beliebig keine Nullstellen hat.

Bemerkung 11.14. (*) Es ist eine interessante Eigenschaft der reellen Zahlen $\mathbb{R}$, dass jedes Polynom vom Grad mindestens 3 reduzibel ist. Das heißt, die irreduziblen Elemente von $\mathbb{R}[X]$ kann man konkret beschreiben: Es sind (nicht-konstante) lineare Polynome, und quadratische Polynome ohne Nullstellen. Diese Aussage werden wir nicht beweisen.

Wir werden sofort sehen, dass die Situation bei Polynomen mit rationalen Koeffizienten ganz anders ist, hier gibt es irreduzible Polynome von jedem Grad. Dazu werden wir Irreduzibilität über $\mathbb{Q}$ mit Irreduzibilität über $\mathbb{Z}$ vergleichen.

(A) **11.15.** *Definieren Sie, was es bedeutet für ein Polynom $f\in\mathbb{Z}[X]$ irreduzibel zu sein.*

(A) **11.16.** *Es sei $f\in\mathbb{Z}[X]\subseteq\mathbb{Q}[X]$. Zeigen Sie, dass aus $f\in\mathbb{Z}[X]$ reduzibel folgt, dass $f\in\mathbb{Q}[X]$ ebenfalls reduzibel sein muss.*

Definition 11.17 (Primitivität für Polynome)**.** Ein Polynom $f(X)=a_nX^n+\ldots+a_0\in\mathbb{Z}[X]$ heißt *primitiv*, falls

$$\mathrm{ggT}(a_0,\ldots,a_n)\;=\;1$$

ist.

(A) **11.18.** *Welche der folgenden Polynomen aus $\mathbb{Z}[X]$ sind primitiv: $2X^2-4X+12$, X^2-6X+6, $X^5-5X+10$, $6X^5-10X^3+15$?*

Proposition 11.19 (Gauß Lemma)**.** *Es seien $f,g\in\mathbb{Z}[X]$ primitive Polynome. Dann ist auch $fg\in\mathbb{Z}[X]$ primitiv.*

(A) **11.20.** *Betrachten Sie die Polynome $2X^2-X+3$ und X^2+X+3. Zeigen Sie, dass beide Polynome primitiv sind, berechnen Sie deren Produkt und überprüfen Sie, ob das Produkt ebenfalls primitiv ist.*

Beweis von Proposition 11.19. Es seien $f(X)=a_nX^n+\ldots a_0$ und $g(X)=b_mX^m+\ldots b_0\in\mathbb{Z}[X]$. Wir schreiben

$$fg(X)\;=\;\sum_{k=0}^{n+m}c_kX^k\;=\;\sum_{k=0}^{n+m}\left(\sum_{j=0}^{k}a_jb_{k-j}\right)X^k$$

für das Produkt. Es gilt also

$$c_k\;=\;a_0b_k+\ldots+a_kb_0$$

für alle $0\le k\le m+n$.

Wir führen einen Widerspruchsbeweis und nehmen daher an, dass fg kein primitives Polynom ist. Dementsprechend gilt

$$\mathrm{ggT}(c_0,\ldots,c_{m+n})>1$$

und es muss insbesondere eine Primzahl p geben, sodass $p|c_k$ für alle $0\le c_k\le m+n$.

Anderseits, da f primitiv ist, teilt p nicht alle Koeffizienten a_i von f, somit gibt es einen kleinsten Index $0\le i\le n$ mit $p\not|a_i$. Ebenfalls ist g kein primitives Polynom, und deswegen

gibt es einen kleinsten Index $0 \leq j \leq m$ für welchen $p \not| b_j$ gilt. Wir sehen uns jetzt c_{i+j} genauer an und untersuchen Teilbarkeit durch p. Es gilt

$$c_{i+j} = \sum_{s=0}^{i+j} a_s b_{i+j-s} \ .$$

Für einen Index $0 \leq s \leq i+j$ (falls nicht $s = i$ und $i+j-s = j$ ist) muss entweder $s < i$ oder $i+j-s < j$ gelten. Wenn $s < i$ gilt, dann ist a_s durch p teilbar, wenn $i+j-s < j$ ist, dann ist b_{i+j-s} durch p teilbar. Wir erhalten, dass

$$c_{i+j} = \sum_{s=0}^{i+j} a_s b_{i+j-s} \equiv a_i b_j \bmod p \ .$$

Da p eine Primzahl ist und weder a_i noch b_j durch p teilbar sind, kann $a_i b_j$ nicht durch p teilbar sein. Anderseits gilt $p | c_{i+j}$ per Annahme. Damit haben wir den gewünschten Widerspruch erhalten. □

Satz 11.21 (Gauß Lemma über Irreduzibilität)**.** *Es sei $f \in \mathbb{Z}[X]$ ein nicht-konstantes Polynom. Dann ist f genau dann irreduzibel, wenn $f \in \mathbb{Q}[X]$ irreduzibel ist und $f \in \mathbb{Z}[X]$ primitiv ist.*

Beweis. Die Aussage werden wir hier nicht beweisen. □

Satz 11.22 (Eisensteins Kriterium für Irreduzibilität)**.** *Es sei $f(X) = a_n X^n + \ldots + a_0$ ein Polynom mit Koeffizienten aus $\mathbb{Z}$. Falls es eine Primzahl p gibt, so dass*

(1) *$p | a_i$ für alle $0 \leq i < n$,*
(2) *$p \not| a_n$, und*
(3) *$p^2 \not| a_0$,*

dann ist $f(X) \in \mathbb{Q}[X]$ irreduzibel.

Beweis. Die Aussage werden wir hier nicht beweisen. □

Beispiel 11.23. Wir betrachten das Polynom $f(X) = 2X^5 - 25X^4 + 15X^2 - 10$. Um Eisensteins Kriterium anwenden zu können, brauchen wir eine Primzahl p, so dass

(1) $p | -25, 15, -10$,
(2) $p \not| 2$, und
(3) $p^2 \not| -10$.

Da die Zahl 5 die einzige Primzahl ist, die die erste Bedingung erfüllt, ist es vernünftig es mit $p = 5$ zu versuchen. In der Tat erfüllt 5 auch die andere zwei Bedingungen, und damit ist f laut Satz 11.22 irreduzibel.

(A) **11.24.** *Zeigen Sie die Irreduzibilität der folgenden Polynome mit der Hilfe von Eisensteins Kriterium:*

$$X^{11} + 7X + 14 \ , X^5 + 2X^2 + 6 \ , \ 6X^4 - 14X^3 + 49X - 21 \ .$$

Bemerkung 11.25. Wenn Eisensteins Kriterium nicht erfüllt ist, bedeutet dies nicht, dass das betroffene Polynom reduzibel sein muss. Betrachten wir zum Beispiel das Polynom $f(X) = X^2 + 5X + 100$. Wie Sie schnell nachrechnen können, gibt es keine Primzahl, die die Bedingungen in Satz 11.22 erfüllt. Anderseits hat f keine reelle Nullstellen und kann daher weder über $\mathbb{Q}$ noch $\mathbb{R}$ reduzibel sein.

(A) **11.26.** *Beantworten Sie die Leitfrage dieses Abschnittes.*

Hausaufgabe 11.27. *Erfinden Sie Beispiele, bei denen Eisensteins Kriterium anwendbar ist.*

Beispiel 11.28. Satz 11.22 kann auch in Situationen verwendet werden, in denen zunächst der Eindruck erweckt wird, dass eine Anwendung nicht möglich ist. Eine solche Situation entsteht aus der Beobachtung, dass ein Polynom $f \in \mathbb{Q}[X]$ genau dann irreduzibel ist, wenn eine Zahl $\alpha \in \mathbb{Q}$ existiert sodass $f(X+\alpha)$ irreduzibel ist.

Als konkretes Beispiel betrachten wir $f(X) = X^4 + 1$. Direkt kann Satz 11.22 nicht angewendet werden. Daher schauen wir uns die Substitution $X \mapsto X+1$ an:

$$(X+1)^4 + 1 \;=\; X^4 + 4X^3 + 6X^2 + 4X + 2 \;.$$

Jetzt ist Eisensteins Kriterium mit $p = 2$ anwendbar und somit ist $(X+1)^4 + 1$ irreduzibel. Dann aber auch $X^4 + 1$.

(A) **11.29.** *Beweisen Sie mit Eisensteins Kriteriums, dass $X^7 + 6 \in \mathbb{Q}[X]$ irreduzibel ist.*

11.2. **Rationale Funktionen.** Rationale Funktionen sind Brüche von Polynomen wie zum Beispiel $\frac{1}{X-1}$ oder $\frac{2X-3}{X^5-2X+9}$. Bevor wir die formale Definition angeben, machen wir ein kleines Detour zu rationalen Zahlen.

Bemerkung 11.30. [Rationale Zahlen als Äquivalenzklassen] (*)
Die Tatsache, dass $1/2 = 2/4$ gilt, obwohl die Paare $(1,2)$ und $(2,4)$ offensichtlich verschieden sind, lässt sich wie folgt mathematisch sauber formulieren. Es sei

$$S \stackrel{\text{def}}{=} \{(a,b) \mid a \in \mathbb{Z}\ ,\ b \in \mathbb{Z} \setminus \{0\}\}\ .$$

Wir definieren jetzt eine Äquivalenzrelation $\sim \subseteq S \times S$ auf S (für die Definition siehe Bemerkung 2.41). Für Paare $(a,b), (c,d) \in S$ sagen wir

$$(a,b) \sim (c,d) \quad \text{falls} \quad ad \;=\; bc\ .$$

Für ein Paar $(a,b) \in S$ schreiben wir

$$\frac{a}{b} \stackrel{\text{def}}{=} \text{ die Äquivalenzklasse von } (a,b) \text{ in } S \text{ unter } \sim\ .$$

Wir können nun die rationalen Zahlen formal definieren als

$$\mathbb{Q} \stackrel{\text{def}}{=} S/\sim\ ,$$

also als die Menge der Äquivalenzklassen von $\sim$ (eine Äquivalenzklasse besteht aus allen Paaren, die zueinander äquivalent sind). Die ganzen Zahlen $m \in \mathbb{Z}$ werden wir als $m/1 \in \mathbb{Q}$ auffassen. Es gilt auch die Gleichheit

$$\frac{a}{b} \;=\; \frac{c}{d} \;\Leftrightarrow\; (a,b) \sim (c,d) \;\Leftrightarrow ad \;=\; bc\ ,$$

welche die eingangs erwähnte Tatsache erklärt. Jetzt, wo wir die formale Definition von $\mathbb{Q}$ zur Hand haben, können wir darauf die üblichen Operationen definieren.

Hausaufgabe 11.31. (*) *Überprüfen Sie, dass die Relation $\sim$ auf S tatsächlich eine Äquivalenzrelation ist.*

Definition 11.32 (Rationale Funktion)**.** Eine *rationale Funktion ϕ mit Koeffizienten aus $\mathbb{R}$* ist der Quotient $\phi = f/g$ von zwei Polynomen, wobei $g \neq 0 \in \mathbb{R}[X]$. Zwei rationale Funktionen f_1/g_1 und f_2/g_2 sind gleich, falls

$$f_1 g_2 \;=\; f_2 g_1\ .$$

Wir schreiben $\mathbb{R}(X)$ für die Menge aller rationalen Funktionen mit reellen Koeffizienten.

Beispiel 11.33. Die folgenden Ausdrücke sind rationale Funktionen:

$$\frac{1}{X}\ ,\ \frac{2X}{X^2-1}\ ,\ \frac{3X^5-2}{X^3+12X-1}\ ,\ \frac{X}{X^2}\ .$$

(A) **11.34.** *Wie viele verschiedene rationale Funktionen gibt es in der folgenden Liste:*

$$\frac{X-1}{X}\ ,\ \frac{X}{X-1}\ ,\ \frac{X^2}{X}\ ,\ \frac{1}{X}\ ,\ \frac{X^{12}}{X^{11}}\ ,\ \frac{X^2-X}{X^2}\ ?$$

Definition 11.35 (Grad einer rationalen Funktion)**.** Es sei $\phi = f/g \in \mathbb{R}(X)$ eine rationale Funktion. Wir definieren den *Grad von* ϕ durch

$$\operatorname{grad}\phi \stackrel{\text{def}}{=} \operatorname{grad} f - \operatorname{grad} g\ .$$

Bemerkung 11.36. Es folgt aus der Definition, dass der Grad einer rationalen Funktion auch negativ sein kann. Es gilt zum Beispiel

$$\operatorname{grad}\frac{1}{X^n} \ =\ \operatorname{grad} 1 - \operatorname{grad} X^n \ =\ 0 - n \ =\ -n\ .$$

(A) **11.37.** *Bestimmen sie den Grad jeder rationalen Funktion aus Beispiel 11.33.*

Bemerkung 11.38. Aus der Definition ist es noch nicht klar, ob der Grad einer rationalen Funktion wirklich sinnvoll ist. Es könnte nämlich vorkommen, dass $\phi = f_1/g_1 = f_2/g_2$ gilt, aber $\operatorname{grad} f_1 - \operatorname{grad} g_1 \neq \operatorname{grad} f_2 - \operatorname{grad} g_2$. Wir werden jetzt zeigen, dass dieses Problem in Wirklichkeit nicht vorkommt.

Es seien wie oben $f_1/g_1 = f_2/g_2$. Dann gilt $f_1 g_2 = f_2 g_1$, woraus

$$\operatorname{grad} f_1 + \operatorname{grad} g_2 \ =\ \operatorname{grad}(f_1 g_2) \ =\ \operatorname{grad}(f_2 g_1) \ =\ \operatorname{grad} f_2 + \operatorname{grad} g_1$$

folgt und somit

$$\operatorname{grad} f_1 - \operatorname{grad} g_1 \ =\ \operatorname{grad} f_2 - \operatorname{grad} g_2\ .$$

Der Grad einer rationalen Funktion ist also wohldefiniert.

Bemerkung 11.39 (Rationale Funktionen als Äquivalenzklassen). (*)
Dem Beispiel von rationalen Zahlen folgend, werden wir hier die präzise Definition von rationalen Funktionen diskutieren. Wir schreiben zunächst

$$S \stackrel{\text{def}}{=} \{(f,g) \mid f,g \in \mathbb{R}[X]\ ,\ g \neq 0\} \subseteq \mathbb{R}[X] \times \mathbb{R}[X]\ .$$

Auf der Mengen S führen wir die folgende Äquivalenzrelation ein:

$$(f_1,g_1) \sim (f_2,g_2) \quad :\Leftrightarrow \quad f_1 g_2 = f_2 g_1.$$

Rationale Funktionen sind dann als Äquivalenzklassen definiert:

$$\mathbb{R}(X) \stackrel{\text{def}}{=} S/\sim\ ,$$

mit der Notation

$$\frac{f}{g} \stackrel{\text{def}}{=} \text{die Äquivalenzklasse von } (f,g) \text{ bezüglich } \sim\ .$$

Man betrachtet Polynome als rationale Funktionen mittels der Abbildung

$$\begin{array}{rcl} \mathbb{R}[X] & \to & \mathbb{R}(X) \\ f & \mapsto & \dfrac{f}{1}\,. \end{array}$$

Hausaufgabe 11.40. *Zeigen Sie, dass die erwartete Gleichheit*

$$\frac{f_1}{g_1} = \frac{f_2}{g_2} \quad \textit{genau dann gilt, wenn} \quad f_1 g_2 = f_2 g_1$$

ist.

Definition 11.41 (Operationen mit rationalen Funktionen)**.** Es seien $f_1/g_1, f_2/g_2 \in \mathbb{R}(X)$ rationale Funktionen. Dann definieren wir

$$\begin{array}{rcl} \dfrac{f_1}{g_1} \pm \dfrac{f_2}{g_2} & \stackrel{\text{def}}{=} & \dfrac{f_1 g_2 \pm f_2 g_1}{g_1 g_2}\,, \\ \dfrac{f_1}{g_1} \cdot \dfrac{f_2}{g_2} & \stackrel{\text{def}}{=} & \dfrac{f_1 f_2}{g_1 g_2}\,, \text{und} \\ \dfrac{f_1}{g_1} : \dfrac{f_2}{g_2} & \stackrel{\text{def}}{=} & \dfrac{f_1 g_2}{f_2 g_1} \end{array}$$

.

(A) **11.42.** *Es seien* $\phi_1 = \frac{2X-1}{3X^2+2}, \phi_2 = \frac{X^4+X-1}{X+5}$*. Berechnen Sie die rationalen Funktionen* $\phi_1 \pm \phi_2, \phi_1 \cdot \phi_2$*, und* ϕ_1/ϕ_2*.*

(A) **11.43.** *Berechnen Sie* $\left(X + \frac{1}{X}\right)^m$ *für* $m = 2, 3, 4$*.*

(A) **11.44.** *Benutzen Sie die Definition der Addition von rationalen Funktionen um zu zeigen, dass*

$$\frac{f_1}{g} + \frac{f_2}{g} = \frac{f_1 + f_2}{g}$$

für alle Polynome $f_1, f_2, g \in \mathbb{R}(X)$*.*

(A) **11.45.** *Berechnen Sie*

$$\frac{\frac{1}{X} + \frac{2}{X+1}}{\frac{3}{X+2} + \frac{4}{X+3}}\,.$$

Lemma 11.46. *Die Multiplikation von rationalen Funktionen ist kommutativ und assoziativ.*

Beweis. Die Aussage folgt sofort aus der Definition der Multiplikation von rationalen Funktionen und den entsprechenden Eigenschaften von Polynomen. □

(A) **11.47.** *Geben sie einen Beweis für Lemma 11.46.*

Lemma 11.48. *Die Addition von rationalen Funktionen ist kommutativ und assoziativ. Konkreter, für rationale Funktionen* $f_1/g_1, f_2/g_2, f_3/g_3 \in \mathbb{R}(X)$ *gelten*

(1) $\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_2}{g_2} + \frac{f_1}{g_1}$,
(2) $\left(\frac{f_1}{g_1} + \frac{f_2}{g_2}\right) + \frac{f_3}{g_3} = \frac{f_1}{g_1} + \left(\frac{f_2}{g_2} + \frac{f_3}{g_3}\right)$.

Beweis. (1) Es folgt aus der Definition der Addition von rationalen Funktionen und der Kommutativität der Addition von Polynomen.

(2) Die gewünschte Eigenschaft erfolgt aus einer direkten Rechung:

$$\begin{aligned}
\left(\frac{f_1}{g_1}+\frac{f_2}{g_2}\right)+\frac{f_3}{g_3} &= \frac{f_1g_2+f_2g_1}{g_1g_2}+\frac{f_3}{g_3}\\
&= \frac{(f_1g_2+f_2g_1)g_3+f_3(g_1g_2)}{(g_1g_2)g_3}\\
&= \frac{f_1g_2g_3+f_2g_1g_3+f_3g_1g_2}{g_1g_2g_3}\\
&= \frac{f_1(g_2g_3)+(f_2g_3+f_3g_2)g_1}{g_1(g_2g_3)}\\
&= \frac{f_1}{g_1}+\frac{f_2g_3+f_3g_2}{g_2g_3}\\
&= \frac{f_1}{g_1}+\left(\frac{f_2}{g_2}+\frac{f_3}{g_3}\right) .
\end{aligned}$$

Bei der ersten, zweiten, fünften, und sechsten Gleichungen haben wir die Definition der Division von rationalen Funktionen benutzt, bei der dritten und vierten die Kommutativität und Assoziativität der Addition und Multiplikation von Polynomen. □

Ⓐ **11.49.** *Überprüfen Sie die Rechnung des Beweises im Fall* $\phi_1=\frac{X-2}{X+3}, \phi_2=\frac{X^2}{2X-1}, \phi_3=\frac{X+1}{X^2-2}$.

Lemma 11.50. *Die Multiplikation rationaler Funktionen ist distributiv bezüglich der Addition rationaler Funktionen. Genauer gilt für alle rationalen Funktionen* $f_1/g_1, f_2/g_2, f_3/g_3 \in \mathbb{R}(X)$

$$\frac{f_1}{g_1}\cdot\left(\frac{f_2}{g_2}+\frac{f_3}{g_3}\right) = \left(\frac{f_1}{g_1}\cdot\frac{f_2}{g_2}\right)+\left(\frac{f_1}{g_1}\cdot\frac{f_3}{g_3}\right) .$$

Beweis. Wir rechnen beide Seiten aus, und stellen fest, dass sie gleich sind:

$$\begin{aligned}
\frac{f_1}{g_1}\cdot\left(\frac{f_2}{g_2}+\frac{f_3}{g_3}\right) &= \frac{f_1}{g_1}\cdot\frac{f_2g_3+f_3g_2}{g_2g_3}\\
&= \frac{f_1(f_2g_3+f_3g_2)}{g_1(g_2g_3)}\\
&= \frac{f_1f_2g_3+f_1f_3g_2}{g_1g_2g_3}\\
&= \frac{f_1f_2g_3}{g_1g_2g_3}+\frac{f_1f_3g_2}{g_1g_2g_3}\\
&= \frac{f_1f_2}{g_1g_2}\cdot\frac{g_3}{g_3}+\frac{f_1f_3}{g_1g_3}\cdot\frac{g_2}{g_2}\\
&= \frac{f_1f_2}{g_1g_2}+\frac{f_1f_3}{g_1g_3}\\
&= \left(\frac{f_1}{g_1}\cdot\frac{f_2}{g_2}\right)+\left(\frac{f_2}{g_2}\cdot\frac{f_3}{g_3}\right) .
\end{aligned}$$

□

A **11.51.** *Erklären Sie für jeden Schritt in der Rechnung im Beweis von Lemma 11.50, welche Eigenschaft von Polynomen oder rationalen Funktionen benutzt wird.*

Hausaufgabe 11.52. *Es seien ϕ_1, und $\phi_2 \in \mathbb{R}(X)$ von Null verschiedene rationale Funktionen. Dann gilt*

$$\operatorname{grad}(\phi_1 \cdot \phi_2) \;=\; \operatorname{grad}\phi_1 + \operatorname{grad}\phi_2 \;.$$

Bemerkung 11.53. (Partialbruchzerlegung)
Nun, da wir rationale Funktionen definiert haben und deren Rechenoperationen studiert haben, können wir uns als Anwendung dessen mit der Partialbruchzerlegung beschäftigen. Wir möchten die rationale Funktion $\frac{X^5-1}{(X-2)^2(X+1)}$ als Summe von Brüchen zerlegen, sodass die Nenner jeweils den Nullstellen (mit Multiplizität) von $(X-2)^2(X+1)$ entsprechen. Das heißt, wir suchen reelle Zahlen A, B, C und ein Polynom $f \in \mathbb{R}[X]$, sodass gilt

$$\frac{X^5-1}{(X-2)^2(X+1)} = \frac{A}{X-2} + \frac{B}{(X-2)^2} + \frac{C}{X+1} + f(X).$$

Sei $P(X) = X^5 - 1$, $Q(X) = (X-2)^2(X+1)$ und $R = \frac{P}{Q}$. Wir stellen fest, dass Q bereits in Linearfaktoren zerlegt ist und die die doppelte Nullstelle 2 und die einfache Nullstelle -1 hat. Da der Grund von P größer ist als der von Q, müssen wir eine Polynomdivision durchführen, da wir sonst keine Partialbruchzerlegung bestimmen können

$$\begin{array}{rrrrl}
(\; X^5 & & & & -1) : (X^3 - 3X^2 + 4) = X^2 + 3X + 9 + \frac{23X^2 - 12X - 37}{X^3 - 3X^2 + 4} \\
\underline{-X^5 + 3X^4} & & & -4X^2 & \\
3X^4 & & & -4X^2 & \\
\underline{-3X^4 + 9X^3} & & -12X & & \\
9X^3 & -4X^2 & -12X & -1 & \\
\underline{-9X^3 + 27X^2} & & & -36 & \\
 & 23X^2 & -12X & -37 &
\end{array}$$

und arbeiten nun weiter mit $R^*(X) = \frac{23X^2-12X-37}{X^3-3X^2+4}$. Da jetzt der Zählergrad kleiner als der Nennergrad ist, können wir eine Partialbruchzerlegung bestimmen. Es folgt direkt $f(X) = X^2 + 3X + 9$. Wir bezeichnen ferner den Zähler mit $Z(X)$ und den Nenner mit $N(X)$ (wobei natürlich $N(X) = Q(X)$ gilt! Einfach Q ausmultiplizieren). Zu jeder Nullstelle bekommen wir einen Bruch in der Partialbruchzerlegung, das heißt wir suchen A, B, C mit

$$\frac{23X^2 - 12X - 37}{X^3 - 3X^2 + 4} = \frac{A}{X-2} + \frac{B}{(X-2)^2} + \frac{C}{X+1}.$$

Bringen wir die rechte Seite auf den Nenner der Linken, so können wir den rechten Zähler mit Koeffizientenvergleich bestimmen. Es gilt also folgende Gleichung zu lösen:

$$\begin{aligned}
23X^2 - 12X - 37 &= A(X-2)(X+1) + B(X+1) + C(X-2)^2 \\
&= AX^2 + AX - 2AX + 2A + BX + B + CX^2 - 4CX + 4C \\
&= (A+C)X^2 + (-A+B-4C)X + (-2A+B+4C).
\end{aligned}$$

Dies führt zu einem LGS (lineares Gleichungssystem) mit 3 Gleichungen und 3 Unbekannten:

$$\begin{aligned} 23 &= A + C \\ -12 &= -A + B - 4C \\ -37 &= -2A + B + 4C \;\Leftrightarrow\; B = 2A - 4C - 37. \end{aligned}$$

Wir setzen die 3. in die 2. Gleichung ein und erhalten

$$-12 = -A + 2A - 4C - 37 - 4C = A - 8C - 37 \;\Rightarrow\; A = 8C + 25.$$

Mithilfe der ersten Gleichung folgt dann

$$23 = 8C + 25 + C \;\Rightarrow\; C = -\frac{2}{9}$$

Damit ist $A = -\frac{16}{9} + 25 = \frac{209}{9}$ und schließlich $B = 2A - 4C - 37 = \frac{31}{3}$. Also ist

$$\frac{X^5 - 1}{(X-2)^2(X+1)} = \frac{209/9}{X-2} + \frac{31/3}{(X-2)^2} + \frac{-2/9}{X+1} + f(X).$$

Definition 11.54 (Nullstellen und Polstellen von rationalen Funktionen)**.**

11.3. **Übungsaufgaben.**

Hausaufgabe 11.55. *Beweisen Sie, dass das Polynom $X^4 + 4X^3 + 26 \in \mathbb{Q}[X]$ irreduzibel ist.*

Hausaufgabe 11.56. *Es sei p eine Primzahl.*

(1) *Zeigen Sie, dass $p | \binom{p}{i}$ für alle $1 \leq p \leq p-1$.*
(2) *Beweisen Sie, dass das Polynom $X^p + (p-1) \in \mathbb{Q}[X]$ irreduzibel ist.*

Hausaufgabe 11.57. *Das Polynom $X^4 + 4 \in \mathbb{Q}[X]$ ist reduzibel. Finden Sie die Zerlegung von f in irreduzible Polynome.*

Hausaufgabe 11.58. *Zeigen Sie, dass ein Polynom $f \in \mathbb{Q}[X]$ dritten Grades genau dann irreduzibel ist, wenn es keine Nullstelle hat.*

Hausaufgabe 11.59. *Es seien $\phi_1, \phi_2 \in \mathbb{R}(X)$ rationale Funktionen mit $\phi_1, \phi_2, \phi_1 + \phi_2$ ungleich 0. Was können wir über das Verhältnis zwischen $\operatorname{grad}(\phi_1 + \phi_2)$ und $\operatorname{grad}\phi_1$,$\operatorname{grad}\phi_2$ sagen?*

Hausaufgabe 11.60. *Finden Sie reelle Zahlen A, B und ein Polynom $f \in \mathbb{R}[X]$, sodass gilt*

$$\frac{X^3 + 3X + 2}{(X+3)^2} = \frac{A}{X+3} + \frac{B}{(X+3)^2} + f(X).$$

11.4. **Wiederholungsaufgaben.**

Hausaufgabe 11.61. *Beweisen Sie, dass das Polynom $X^4 + 4X^3 + 26 \in \mathbb{Q}[X]$ irreduzibel ist.*

Hausaufgabe 11.62. *Es sei $n \geq 2$ eine natürliche Zahl, p eine Primzahl. Beweisen Sie, dass das Polynom $X^n - p \in \mathbb{Q}[X]$ irreduzibel ist.*

Hausaufgabe 11.63. *Es sei p eine Primzahl.*

(1) *Zeigen Sie, dass $p | \binom{p}{i}$ für alle $1 \leq p \leq p-1$.*
(2) *Beweisen Sie, dass das Polynom $X^p + (p-1) \in \mathbb{Q}[X]$ irreduzibel ist.*

11.5. **Weiterführende Literatur.**

12. Ungleichungen

12.1. **Wiederholung.** Alles was Sie in der Schule über Ungleichungen gelernt haben, die Analyse quadratischer Funktionen aus ELMA I. und Eigenschaften des Absolutbetrags aus Abschnitt 3.

Leitfrage. *Für welche reelle Zahlen x gilt die Ungleichung*

$$\frac{x-1}{x-2} < \frac{2x-3}{x-4} \ ?$$

12.2. **Positivität und Ungleichungen.** Als Erstes beschreiben wir unsere Strategie für die Arbeit mit Ungleichungen zwischen reellen Zahlen. Wir möchten sagen, dass $a < b$ gilt, wenn $0 < b - a$ ist, oder in anderen Worten, wenn die Differenz $b - a$ positiv ist.

Das führt zur Idee, uns zunächst mit dem Begriff der Positivität zu beschäftigen.

Definition 12.1 (Positivität von Zahlen)**.**

(1) Eine ganze Zahl m heißt *positiv*, wenn m eine natürliche Zahl ungleich Null ist (Notation: $m \in \mathbb{N}_+$).
(2) Eine rationale Zahl $\alpha \in \mathbb{Q}$ heißt *positiv*, wenn es positive Zahlen $p, q \in \mathbb{Z}$ gibt, so dass $\alpha = p/q$.
(3) Eine reelle Zahl $t \in \mathbb{R}$ heißt *positiv*, wenn sie auf der Zahlengeraden rechts von der 0 liegt.

Wir schreiben $\mathscr{P}$ für die Menge positiver reellen Zahlen, statt $t \in \mathbb{R}$ schreiben wir oft $t > 0$. Eine ganze/rationale/reelle Zahl heißt *nichtnegativ*, wenn sie positiv oder gleich 0 ist. Eine Zahl heißt *negativ*, wenn sie nicht nichtnegativ ist. Die Menge der negativen Zahlen ist logischerweise $-\mathscr{P}$. Für t nichtnegativ schreiben wir $t \geq 0$.

Bemerkung 12.2. Man sieht schnell, dass positive ganze Zahlen genau die Elemente von $\mathbb{Z} \cap \mathscr{P}$ sind und positive rationale Zahlen die Elemente von $\mathbb{Q} \cap \mathscr{P}$.

Von den Eigenschaften der positiven Zahlen werden wir die Folgenden brauchen.

Proposition 12.3. *Es seien a, b reelle Zahlen. Dann gelten*

(1) *aus $a, b \in \mathscr{P}$ folgt $a + b \in \mathscr{P}$.*
(2) *aus $a, b \in \mathscr{P}$ folgt $ab \in \mathscr{P}$.*
(3) *jede reelle Zahl $a \in \mathbb{R}$ ist in genau einer der Mengen $\mathscr{P}, \{0\}, -\mathscr{P}$ enthalten.*

Beweis. Da wir keine axiomatische Einführung der reellen Zahlen gegeben haben, werden wir diese Aussage nicht beweisen (können). Für ganze oder rationale Zahlen folgen die Eigenschaften aus den jeweiligen Definitionen. □

Bemerkung 12.4. Aus Teil (3) von Proposition 12.3 folgt, dass 0 weder positiv noch negativ ist, das heißt, $0 \notin \mathscr{P}, -\mathscr{P}$.

Lemma 12.5. *Es sei $a \in \mathbb{R}$ eine beliebige reelle Zahl. Dann ist $a \in \mathscr{P}$ genau dann wenn $-a \in -\mathscr{P}$.*

Beweis. Aus $a \in \mathscr{P}$ folgt $a \neq 0$ wegen Proposition 12.3 (3). Dann gilt $-a \neq 0$, und daher gilt entweder $-a \in -\mathscr{P}$ oder $a \in -\mathscr{P}$. Die erste Möglichkeit kann aber nicht gelten, weil dann

$$0 = a + (-a) \in \mathscr{P}$$

nach Proposition 12.3 (1), was Proposition 12.3 (3) widerspricht. Es bleibt also $-a \in -\mathscr{P}$ übrig.

Die andere Richtung des Beweises folgt aus gleichen Argument, indem wir a durch $-a$ ersetzen. □

In diesem Abschnitt werden wir eine axiomatische Behandlung von Ungleichungen geben, wobei wir nicht auf unsere Erfahrung mit positiven Zahlen und Ungleichungen bauen, sondern ausschließlich auf die Eigenschaften in Proposition 12.3.

Bemerkung 12.6. Mit der Notation $a > 0$ lassen sich die Eigenschaften aus Proposition 12.3 wie folgt formulieren:

(1) Aus $a > 0$ und $b > 0$ folgt $a + b > 0$.
(2) Aus $a > 0$ und $b > 0$ folgt $ab > 0$.
(3) Für jede reelle Zahl a gilt genau eine der Folgenden Eigenschaften:

$$a > 0 \quad , \quad a = 0 \quad , \quad -a > 0 \; .$$

Bemerkung 12.7. Bei rationalen Zahlen muss man etwas vorsichtiger sein: Die Zahl $\frac{-5}{-9}$ ist nämlich positiv, da

$$\frac{-5}{-9} = \frac{5}{9} \; .$$

Hausaufgabe 12.8. *Beweisen Sie die folgenden Eigenschaften der Nichtnegativität:*

(1) *Aus* $a \geq 0$ *und* $b \geq 0$ *folgt* $a + b \geq 0$.
(2) *Aus* $a \geq 0$ *und* $b \geq 0$ *folgt* $ab \geq 0$.
(3) *Aus* $a \geq 0$ *und* $-a \geq 0$ *folgt* $a = 0$.

Bemerkung 12.9. Vorsicht: An dieser Stelle macht der Ausdruck $a < 0$ offiziell noch keinen Sinn.

A **12.10.** *Beweisen Sie: Aus* $a > 0$ *und* $b \geq 0$ *folgt* $a + b > 0$.

Jetzt können wir definieren, was Ungleichungen zwischen Zahlen bedeuten.

Definition 12.11 (Ungleichungen)**.** Es seien $a, b \in \mathbb{R}$. Wir definieren

$$a > b \quad \text{falls} \quad a - b > 0 \; (\Leftrightarrow \; a - b \in \mathscr{P})$$
$$a \geq b \quad \text{falls} \quad a - b \geq 0 \; (\Leftrightarrow \; a - b \in \mathscr{P} \text{ oder } a - b = 0)$$

Bemerkung 12.12. Bevor wir irgendwas tun, müssen wir nachweisen, dass $a > 0$ im Sinne von Proposition 12.3 und Definition 12.11 äquivalent sind. Das stimmt aber, weil $a \in \mathscr{P}$ ist äquivalent zu $a - 0 \in \mathscr{P}$ für jede reelle Zahl a.

Lemma 12.13. *Es sei* $a \in \mathbb{R}$. *Dann ist* $0 > a$ *äquivalent zu* $a \in -\mathscr{P}$.

Beweis. Nach Definition 12.11 und Lemma 12.5 gilt

$$0 > a \quad \Leftrightarrow \quad 0 - a > 0 \quad \Leftrightarrow \quad -a > 0 \quad \Leftrightarrow \quad -a \in \mathscr{P} \quad . \Leftrightarrow \quad a \in -\mathscr{P}$$

□

Lemma 12.14. *Es seien* a *reelle Zahlen. Dann gelten die folgenden Eigenschaften:*

(1) $a > 0$ *gilt genau dann, wenn* $-a < 0$.
(2) $a > 0$ *und* $a < 0$ *können nicht zugleich richtig sein.*
(3) *Aus* $a \geq 0$ *und* $a \leq 0$ *folgt* $a = 0$.

Beweis. (1) Folgt sofort aus Lemma 12.5 durch

$$a > 0 \quad \Leftrightarrow \quad a \in \mathscr{P} \quad \Leftrightarrow \quad -a \in -\mathscr{P} \quad \Leftrightarrow -a < 0 \ .$$

(2) Aus $a < 0$ folgt wegen Teil (1) $-a > 0$. Daher würden $a < 0$ und $a > 0$ implizieren, dass $a, -a \in \mathscr{P}$ und damit $0 = a + (-a) \in \mathscr{P}$. Dies widerspricht Proposition 12.3.

(3) Folgt sofort aus Teil (2).

□

Folgende Regeln sind die Grundregeln für die Arbeit mit Ungleichungen.

Lemma 12.15. *Es seien $a, b, c \in \mathbb{R}$.*

(1) *Aus $a < b$ und $b < c$ folgt $a < c$. (Transitivität)*
(2) *Aus $a < b$ folgt $a + c < b + c$.*
(3) *Für $a < b$ gilt die Implikation*

$$a < b \Longrightarrow \begin{cases} ac < bc & \text{falls } c > 0, \\ ac > bc & \text{falls } c < 0. \end{cases}$$

Beweis. (1) Nach Definition 12.11 bedeutet $a < b$ genau $b - a \in \mathscr{P}$ und $b < c$ analog $c - b \in \mathscr{P}$. Dann folgt aus (1) von Proposition 12.3

$$c - a \ = \ (c - b) + (b - a) \in \mathscr{P} \ ,$$

das heißt $a < c$, wie behauptet.

(2) $a < b$ bedeutet nach Definition $b - a \in \mathscr{P}$. Dann gilt aber

$$(b + c) - (a + c) \ = \ b - a \in \mathscr{P} \ ,$$

anders ausgedrückt $a + c < b + c$.

(3) Wie früher bedeutet $a < b$ genau $b - a \in \mathscr{P}$ und aus Proposition 12.3 (2) folgt, dass dann für $c \in \mathscr{P}$ auch

$$bc - ac \ = \ (b - a)c \in \mathscr{P}$$

gilt. Es folgt $ac < bc$ für $c > 0$.

Wenn $c < 0$, dann gilt $-c \in \mathscr{P}$ und daher

$$ac - bc \ = \ (b - a)(-c) \in \mathscr{P} \ ,$$

also $bc < ac$.

□

A **12.16.** *Es seien $a, b \in \mathbb{R}$. Zeigen Sie, dass aus $a < b$ folgt $-b < -a$.*

Korollar 12.17. *Es seien $a, b, c \in \mathbb{R}$.*

(1) *Aus $a \leq b$ und $b \leq c$ folgt $a \leq c$. (Transitivität)*
(2) *Aus $a \leq b$ folgt $a + c \leq b + c$.*
(3) *Aus $a \leq b$ folgt*

$$a \leq b \Longrightarrow \begin{cases} ac \leq bc & \text{falls } c > 0, \\ ac \geq bc & \text{falls } c < 0. \end{cases}$$

Hausaufgabe 12.18. *Beweisen Sie Korollar 12.17.*

Bemerkung 12.19. Die Eigenschaft (3) aus Lemma 12.15 bzw. Korollar 12.17 ist genau die Regel, dass bei Multiplikation von Ungleichungen mit negativen Zahlen die Ungleichung umgedreht wird. Dies müsste Ihnen aus der Schule bekannt sein.

(A) **12.20.** *Beweisen Sie, dass aus $a < b$ und $b \leq c$ die Relation $a < c$ folgt.*

Lemma 12.21. *Es gelten die folgenden Eigenschaften der Positivität von reellen Zahlen.*

(1) *Aus $a > 0$ und $b < 0$ folgt, dass $ab < 0$ ist.*
(2) *Aus $a, b < 0$ folgt, dass $ab > 0$ ist.*

Hausaufgabe 12.22. *Beweisen Sie Lemma 12.21.*

Bemerkung 12.23. Die Aussage von Lemma 12.21 entspricht genau der aus der Schule bekannten Faustregel, dass das Vorzeichen eines Produktes negativ ist, wenn die Anzahl der Minus-Symbole ungerade ist und positiv ist, wenn diese Anzahl gerade ist.

Die folgende einfache Eigenschaft der reellen Zahlen hat viele und wichtige Konsequenzen.

Proposition 12.24 (Positivität von Quadraten)**.** *Es sei $a \in \mathbb{R}$ eine beliebige reelle Zahl. Dann gilt $a^2 \geq 0$ und $a^2 = 0$ genau dann, wenn $a = 0$.*

Beweis. Wir machen eine Fallunterscheidung, je nachdem, ob $a = 0$, $a > 0$, oder $a < 0$. Falls $a = 0$, dann gilt

$$a^2 = a \cdot a = 0 \cdot 0 = 0 ,$$

daher $a^2 \geq 0$.

Falls $a > 0$ (in anderen Worten $a \in \mathscr{P}$), dann folgt aus Proposition 12.3 (2), dass

$$a^2 = a \cdot a \in \mathscr{P} ,$$

in anderen Worten $a^2 > 0$.

Falls $a < 0$, dann gilt $-a > 0$ und damit ist $(-a)^2 > 0$. Dann gilt aber auch

$$a^2 = (-a) \cdot (-a) > 0 .$$

Wir müssen noch die Rückrichtung der letzten Aussage beweisen. Sei dafür $a^2 = 0$. Gilt $a > 0$, dann ist auch $a^2 > 0$ nach Proposition 12.3 (2), ein Widerspruch. Das gleiche Argument zeigt, dass $a < 0$ ebenfalls nicht möglich ist. Die Behauptung folgt jetzt sofort mit Proposition 12.3 (3). □

Korollar 12.25. *Es seien $0 < a, b$ reelle Zahlen. Dann gilt $a < b$ genau dann, wenn $a^2 < b^2$.*

Beispiel 12.26. Wir werden ohne Taschenrechner entscheiden können, welche der irrationalen Zahlen $2+\sqrt{5}$ und $3\sqrt{2}$ größer ist. Laut Korollar 12.25 reicht es die Anordnung der Quadraten zu überprüfen, diese sind $9 + 4\sqrt{5}$ und 18. Wir subtrahieren 9 von beiden Zahlen. Dann kommen wir auf $4\sqrt{5}$ und 9. Jetzt betrachten wir wieder die Quadrate und erhalten somit $80 < 81$. Es stellt sich heraus, dass $2 + \sqrt{5} < 3\sqrt{2}$.

Bemerkung 12.27. Für diese Bemerkung vergessen wir Definition 12.1 komplett und betrachten nur Proposition 12.3 was die Eigenschaften von Positivität betrifft. Wir können sehen, dass

$$1 = 1 \cdot 1 > 0$$

und durch vollständige Induktion lässt sich beweisen, dass alle Zahlen $1 + \ldots + 1$ (die wir nicht ganz zufällig 'positive ganze Zahlen' nennen) positiv sein müssen.

Lemma 12.28. *Es seien $0 < a < b$ reelle Zahlen. Dann gilt*

$$0 < \frac{1}{b} < \frac{1}{a} .$$

Beweis. Zunächst beweisen wir, dass aus $a > 0$ sofort $1/a > 0$ folgt. Wir wissen, dass $1/a \neq 0$, daher gibt es die zwei Möglichkeiten $1/a > 0$ und $1/a < 0$. Angenommen, $1/a < 0$. Dann gilt aus Lemma 12.21, dass $1 = a \cdot (1/a) < 0$, was Proposition 12.24 widerspricht, kann also nicht wahr sein. Es folgt daher $1/a > 0$ und analog $1/b > 0$, insbesondere gilt $1/ab > 0$ ebenfalls.

Die Relation $a < b$ bedeutet $0 < b - a$, wegen $1/ab > 0$ folgt aus Proposition 12.3 (2)

$$0 < (b-a) \cdot \frac{1}{ab} = \frac{b-a}{ab} = \frac{b}{ab} - \frac{a}{ab} = \frac{1}{a} - \frac{1}{b} ,$$

in anderen Worten

$$\frac{1}{b} < \frac{1}{a} ,$$

wie versprochen. □

Bemerkung 12.29. Aus Lemma 12.28 folgt, dass 'positive rationale Zahlen' aus Definition 12.1 schon wegen Proposition 12.3 alle > 0 sein müssen.

Beispiel 12.30. Wir lösen die Ungleichung

$$2(x-7) < -1 .$$

Bei unseren ersten Beispielen zeigen wir jeden Schritt, später werden wir die Einfachen weglassen.

$$\begin{aligned} 2(x-7) &< -1 \quad \text{wir teilen durch } 2 > 0 \\ x - 7 &< -\frac{1}{2} \quad \text{wir addieren } 7 \\ x &< 7 - \frac{1}{2} = \frac{13}{2} . \end{aligned}$$

Beispiel 12.31. Wir lösen die Ungleichung

$$\left|\frac{1}{n}\right| < \frac{1}{100} ,$$

für eine positive ganze Zahl n.

Als Erinnerung, für eine reelle Zahl a ist

$$|a| \stackrel{\text{def}}{=} \begin{cases} a & \text{falls } a \geq 0 \\ -a & \text{falls } a < 0. \end{cases}$$

Eine Konsequenz der Definition ist, dass für reelle Zahlen $a, b \in \mathbb{R}$ gilt

$$|a| \leq b \quad \Leftrightarrow \quad -b \leq a \leq b .$$

Es folgt dass

$$\left|\frac{1}{n}\right| < \frac{1}{100} \quad \Leftrightarrow \quad -\frac{1}{100} \leq \frac{1}{n} \leq \frac{1}{100} .$$

Wir multiplizieren die Ungleichung mit der positiven Zahl $\frac{100}{n}$ und erhalten dadurch

$$-n \leq 100 \leq n.$$

Da $n > 0$, wird die Ungleichung zu

$$100 \leq n ,$$

das ist unsere Lösung.

Hausaufgabe 12.32. *Es seien $a, b \in \mathbb{R}$. Dann gelten*

(1) $|a| \leq b$ *genau dann, wenn* $-b \leq a$ *und* $a \leq b$*;*
(2) $|a| \geq b$ *genau dann, wenn* $a \geq b$ *oder* $-a \leq b$*.*

Was passiert bei den Ungleichungen, wenn $b < 0$ *ist?*

Beispiel 12.33. Wir lösen die Ungleichung

$$(*) \qquad |3x-1| - |2x+3| > 2$$

innerhalb der reellen Zahlen. Um Beträge auflösen zu können, führt kein Weg an Fallunterscheidungen vorbei. Wir müssen also untersuchen, wann der Ausdruck im jeweiligen Betrag positiv oder negativ ist. Für den ersten Betrag sehen wir, dass $3x-1 \geq 0$ genau dann, wenn $x \geq \frac{1}{3}$ und für den zweiten Betrag gilt $2x+3 \geq 0$ genau dann, wenn $x \geq -\frac{3}{2}$. Es ergeben sich offensichtlich 3 verschiedene Fälle:

Fall 1: Sei $x < -\frac{3}{2}$. Dann sind beide Ausdrücke in den Beträgen negativ. Wir müssen beim auflösen des Betrags also jeweils mit -1 multiplizieren, damit es positiv wird. Die Gleichung * ist damit äquivalent zu

$$\begin{aligned} -(3x-1) - (-1)(2x+3) &> 2 \\ \Leftrightarrow \quad -3x+1+2x+3 &> 2 \\ \Leftrightarrow \quad -x+4 &> 2 \\ \Leftrightarrow \quad -x &> -2 \\ \Leftrightarrow \quad x &< 2. \end{aligned}$$

Es folgt, dass die Ungleichung stimmt für

$$x \in (-\infty, -\frac{3}{2}) \cap (-\infty, 2) = (-\infty, -\frac{3}{2}) =: \mathbb{L}_1.$$

Fall 2: Sei $-\frac{3}{2} \leq x < \frac{1}{3}$. Dann ist der erste Ausdruck im Betrag negativ und der zweite positiv. Die Gleichung * ist jetzt äquivalent zu

$$\begin{aligned} -(3x-1) - (2x+3) &> 2 \\ \Leftrightarrow \quad -3x+1-2x-3 &> 2 \\ \Leftrightarrow \quad -5x-2 &> 2 \\ \Leftrightarrow \quad -5x &> 4 \\ \Leftrightarrow \quad x &< -\frac{4}{5}. \end{aligned}$$

Es folgt, dass die Ungleichung stimmt für

$$x \in (-\infty, -\frac{4}{5}) \cap [-\frac{3}{2}, \frac{1}{3}) = [-\frac{3}{2}, -\frac{4}{5}) =: \mathbb{L}_2.$$

Fall 3: Sei $x \geq \frac{1}{3}$. In diesem Fall sind alle Ausdrücke in den Beträgen positiv, wir können diese also einfach weglassen. Damit wird * zu

$$\begin{aligned} (3x-1) - (2x+3) &> 2 \\ \Leftrightarrow \quad 3x-1-2x-3 &> 2 \\ \Leftrightarrow \quad x-4 &> 2 \\ \Leftrightarrow \quad x &> 6. \end{aligned}$$

Es folgt, dass die Ungleichung stimmt für

$$x \in [\frac{1}{3}, \infty) \cap (6, \infty) = (6, \infty) =: \mathbb{L}_3.$$

Insgesamt ist die Ungleichung also genau dann lösbar, wenn

$$x \in \mathbb{L}_1 \cup \mathbb{L}_2 \cup \mathbb{L}_3 = (-\infty, -\frac{4}{5}) \cup (6, \infty) =: \mathbb{L}.$$

In Worten: x ist größer als 6 und kleiner als $-0,8$.

Hausaufgabe 12.34. *Lösen Sie die Ungleichung*

$$|2x + 3| \leq 12$$

innerhalb der reellen Zahlen. Zeigen Sie in ihrer Lösung bei jedem Schritt welche Eigenschaft aus Proposition 12.3 Sie benutzen.

Hausaufgabe 12.35. *Lösen Sie die Ungleichung*

$$|7x - 3| \geq 2$$

in den reellen Zahlen. In ihrer Lösung zeigen Sie bei jedem Schritt welche Eigenschaft aus Proposition 12.3 Sie benutzen.

Proposition 12.36 (Bernoulli'sche Ungleichung)**.** *Es sei n eine natürliche Zahl, $t > -1$ reell. Dann gilt*

$$1 + nt \leq (1 + t)^n .$$

Beweis. Wir benutzen vollständige Induktion.
Induktionsanfang: Für $n = 0$ gilt

$$1 + 0 \cdot t = 1 \leq 1 = (1 + t)^0 ,$$

was klar richtig ist. Wenn $n = 1$ ist, dann haben wir

$$1 + 1 \cdot t = 1 + t \leq 1 + t = (1 + t)^1 ,$$

was ebenso stimmt. Induktionsschluss: Als Induktionsannahme betrachten wir

$$1 + nt \leq (1 + t)^n , \tag{12.1}$$

wobei $t > -1$ eine ansonsten beliebige reelle Zahl ist. Da $1 + t > 0$, bleibt die Ungleichung nach Multiplikation mit $1 + t$ erhalten:

$$(1 + nt)(1 + t) \leq (1 + t)^{n+1} .$$

Wir können die linke Seite ausmultiplizieren

$$(1 + nt)(1 + t) = 1 + (n + 1)t + nt^2 \geq 1 + (n + 1)t$$

und damit sind wir fertig. □

Hausaufgabe 12.37. *Beweisen Sie die Bernoulli'sche Ungleichung für $t > 0$ mittels des Newton'schen binomischen Satzes (Satz 6.41).*

12.3. **Quadratische Ungleichungen.** Wegen ihrer Wichtigkeit schreiben wir die Aussage von Proposition 12.24 noch einmal hin.

Proposition 12.38 (= Proposition 12.24)**.** *Es sei $a \in \mathbb{R}$ eine beliebige reelle Zahl. Dann gilt $a^2 \geq 0$ und $a^2 = 0$ genau dann, wenn $a = 0$.*

Hausaufgabe 12.39. *Für beliebige reelle Zahlen a, b gilt*

$$a^2 + b^2 \;=\; 0 \quad \Leftrightarrow \quad a \;=\; 0 \quad \textit{und} \quad b \;=\; 0 \;.$$

Korollar 12.40. *Es seien a und b beliebige reelle Zahlen, dann gilt $(a-b)^2 \geq 0$ und $(a-b)^2 = 0$ genau dann, wenn $a = b$.*

Beweis. Wir wenden Proposition 12.24 mit der Wahl $\alpha \stackrel{\text{def}}{=} a - b$ an. Dann ist

$$0 \leq \alpha^2 \;=\; (a-b)^2$$

mit Gleichheit genau dann, wenn $\alpha = 0$. Das heißt, falls $a = b$. □

Diese Beobachtung ist die Quelle von sehr vielen Ungleichungen zwischen Kombinationen reeller Zahlen. Es gilt zum Beispiel die folgende Kette von Ungleichungen.

Definition 12.41 (Mittel reeller Zahlen)**.** Es seien a und b positive reelle Zahlen. Wir definieren die folgenden Mittel von a und b.

$$\begin{aligned}
\text{Arithmetisches Mittel:} \quad & A(a,b) \stackrel{\text{def}}{=} \frac{a+b}{2} \;, \\
\text{Geometrisches Mittel:} \quad & G(a,b) \stackrel{\text{def}}{=} \sqrt{ab} \;, \\
\text{Harmonisches Mittel:} \quad & H(a,b) \stackrel{\text{def}}{=} \frac{2}{\frac{1}{a} + \frac{1}{b}} \;, \\
\text{Quadratisches Mittel:} \quad & Q(a,b) \stackrel{\text{def}}{=} \sqrt{\frac{a^2+b^2}{2}} \;.
\end{aligned}$$

Bemerkung 12.42. Der Ausdruck für das harmonische Mittel lässt sich vereinfachen:

$$H(a,b) \;=\; \frac{1}{\frac{1}{a} + \frac{1}{b}} \;=\; \frac{2}{\frac{a+b}{ab}} \;=\; \frac{2ab}{a+b} \;.$$

(A) **12.43.** *Berechnen Sie alle vier Mittel für die Zahlen $a = 2$ und $b = 1/2$ und überprüfen Sie, ob die gewünschten Ungleichungen tatsächlich stimmen.*

Hausaufgabe 12.44. *Finden Sie positive Zahlen a und b mit $G(a,b) = 10$ und $A(a,b) = 25/2$.*

Satz 12.45 (Ungleichungen zwischen den Mitteln)**.**
Es seien a, b positive reelle Zahlen. Dann gelten die Ungleichungen

$$H(a,b) \;\leq\; G(a,b) \;\leq\; A(a,b) \;\leq\; Q(a,b) \;. \tag{12.2}$$

Bei jedem einzelnen Schritt gilt Gleichheit genau dann, wenn $a = b$ ist.

Bemerkung 12.46. Es lohnt sich, diese Ungleichungen mit Formeln hinzuschreiben:

$$\frac{2ab}{a+b} \;\leq\; \sqrt{ab} \;\leq\; \frac{a+b}{2} \;\leq\; \sqrt{\frac{a^2+b^2}{2}} \;.$$

Beispiel 12.47. In der Küche steht ein Tisch mit genau 10000 Quadratzentimetern Oberfläche. Wie klein kann dessen Umfang sein? Solche Aufgaben lassen sich mit Hilfe der Ungleichung zwischen Arithmetischem und Geometrischem Mittel lösen.

Bemerkung 12.48. Alle drei Ungleichungen beruhen auf der folgenden Beobachtung: Für positive Zahlen a, b gilt

$$4ab \leq (a+b)^2 .$$

Das folgt aus

$$0 \leq (a-b)^2 = a^2 - 2ab + b^2,$$

nachdem wir auf beiden Seiten $4ab$ addieren.

Beweis. Wir werden die drei Ungleichungen

$$H(a,b) \leq G(a,b) \ , \ G(a,b) \leq A(a,b) \ , \ A(a,b) \leq Q(a,b)$$

einzeln beweisen (zusammen mit der Bedingungen für Gleichheit). Aus diesen Aussagen folgt dann der Satz.
$H(a,b) \leq G(a,b)$: In konkreten Formeln sollen wir die Ungleichung

$$\frac{2ab}{a+b} \leq \sqrt{ab}$$

beweisen. Da beide Seiten positiv sind, ist Quadrieren eine äquivalente Umformung. Daher reicht es zu zeigen, dass

$$\frac{4a^2b^2}{(a+b)^2} \leq ab$$

ist. Der Nenner der linken Seite ist immer positiv, somit ist Multiplikation mit $(a+b)^2$ wieder eine äquivalente Umformung. Wir erhalten dann

$$4a^2b^2 \leq ab(a+b)^2 = ab(a^2+2ab+b^2) .$$

Nach Subtraktion von $4a^2b^2$ bekommen wir

$$0 \leq ab(a^2+2ab+b^2) - 4a^2b^2 = ab(a^2-2ab+b^2) = ab(a-b)^2 .$$

Da $a, b, (a-b)^2 \geq 0$, gilt die letzte Ungleichung und damit $H(a,b) \leq G(a,b)$. Ebenfalls: wegen $a, b > 0$ gilt

$$a = b \Leftrightarrow (a-b)^2 = 0 \Leftrightarrow H(a,b) = G(a,b) .$$

$G(a,b) \leq A(a,b)$: Wir müssen die Ungleichung

$$\sqrt{ab} \leq \frac{a+b}{2}$$

zeigen. Da $a, b > 0$, sind beide Seiten positiv und daher ist Quadrieren eine äquivalente Umformung. Wir erhalten

$$ab \leq \left(\frac{a+b}{2}\right)^2 ,$$

oder, nach Multiplikation mit 4,

$$4ab \leq (a+b)^2 = a^2 + 2ab + b^2 .$$

Das ist zu

$$0 \leq a^2 - 2ab + b^2 = (a-b)^2$$

äquivalent, also stimmt die Ungleichung. Außerdem gilt Gleichheit überall genau dann, wenn $(a-b)^2 = (a+b)^2$ gilt, das heißt, wenn $a = b$ ist.
$A(a,b) \leq Q(a,b)$: In konkreten Formeln müssen wir

$$\frac{a+b}{2} \leq \sqrt{\frac{a^2+b^2}{2}}$$

beweisen. Nach Quadrieren und Multiplikation mit 4 (beides äquivalente Umformungen) erhalten wir

$$(a+b)^2 \leq 2(a^2+b^2)$$

und wenn man $a^2 + 2ab + b^2$ auf beiden Seiten subtrahiert, bekommen wir

$$0 \leq a^2 - 2ab + b^2 = (a-b)^2 .$$

Die Ungleichung haben wir damit bewiesen und in der Tat herrscht Gleichheit genau dann, wenn $a = b$ ist, wie gewünscht. □

Beispiel 12.49. Es seien $a, b, c > 0$ reelle Zahlen. Dann gilt

$$\frac{(a+b)(b+c)(c+a)}{8} \geq abc .$$

Der Beweis geht unerwartet schnell. Man sieht direkt:

$$A(a,b) \cdot A(b,c) \cdot A(c,a) = \frac{(a+b)(b+c)(c+a)}{8}$$
$$G(a,b) \cdot G(b,c) \cdot G(c,a) = abc.$$

Mit Satz 12.45, also $A(a,b) \geq G(a,b)$ folgt die Behauptung.

Hausaufgabe 12.50. *Es sei $a > 0$ eine reelle Zahl. Beweisen Sie, dass*

$$a + \frac{1}{a} \geq 2 .$$

Hausaufgabe 12.51. *Die Dörfer X und Y haben beide Sportfelder. Beide Felder haben einen Umfang von* 320 *Meter. Das Feld von Dorf X ist quadratisch, das Feld von Dorf Y hat die Gestalt eines Rechtecks, welches* kein *Quadrat ist. Wer hat das größere Sportfeld?*

Bemerkung 12.52. Alle Mittel, die wir definiert haben, sind auch sinnvoll für mehr als zwei Zahlen. Es seien jetzt $a_1, \ldots, a_n > 0$, wobei $n \geq 2$ eine ganze Zahl ist.

$$\text{Arithmetisches Mittel:} \quad A(a_1,\ldots,a_n) \stackrel{\text{def}}{=} \frac{a_1+\ldots+a_n}{n} = \frac{1}{n}\sum_{i=1}^{n} a_i ,$$

$$\text{Geometrisches Mittel:} \quad G(a_1,\ldots,a_n) \stackrel{\text{def}}{=} \sqrt[n]{a_1 \cdot \ldots \cdot a_n} = \left(\prod_{i=1}^{n} a_i\right)^{\frac{1}{n}} ,$$

$$\text{Harmonisches Mittel:} \quad H(a_1,\ldots,a_n) \stackrel{\text{def}}{=} \frac{n}{\frac{1}{a_1}+\ldots+\frac{1}{a_n}} ,$$

$$\text{Quadratisches Mittel:} \quad Q(a_1,\ldots,a_n) \stackrel{\text{def}}{=} \sqrt{\frac{a_1^2+\ldots+a_n^2}{2}} .$$

Satz 12.53 (Ungleichung zwischen den Mitteln)**.** *Für beliebige positive ganze Zahl $n \geq 2$ und positive reelle Zahlen $a_1, \ldots, a_n$ gelten die Ungleichungen*

$$H(a_1,\ldots,a_n) \leq G(a_1,\ldots,a_n) \leq A(a_1,\ldots,a_n) \leq Q(a_1,\ldots,a_n) .$$

Beweis. Die Ungleichungen können zum Beispiel durch vollständige Induktion bewiesen werden, wir werden es hier aber nicht tun. □

(A) **12.54.** *Schreiben Sie die vier Mittel im Fall $n = 3$ auf.*

Hausaufgabe 12.55. *Es seien $0 < a, b, c$ reelle Zahlen. Zeigen Sie, dass*

$$a^3 + b^3 + c^3 \;=\; 3abc + (a+b+c)(a^2+b^2+c^2-ab-ac-bc) \;.$$

Hausaufgabe 12.56. *Beweisen Sie, dass für beliebige positive Zahlen a, b, c*

$$(a+b+c)\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right) \;\geq\; 9$$

gilt.

Hausaufgabe 12.57. *Zeigen Sie, dass für beliebige $a, b, c > 0$ gilt*

$$\frac{a}{b}+\frac{b}{c}+\frac{c}{a} \;\geq\; 3 \;.$$

Die nächste Gruppe von Ungleichungen, die wir betrachten, spielt eine große Rolle in der Geometrie.

Proposition 12.58 (Cauchy–Schwarz-Ungleichung, $n = 2$)**.** *Es seien a_1, a_2, b_1, b_2 reelle Zahlen. Dann gilt*

$$(a_1b_1 + a_2b_2)^2 \;\leq\; (a_1^2+a_2^2)(b_1^2+b_2^2) \;. \tag{12.3}$$

Beweis. Zunächst rechnen wir die beiden Seiten aus:

$$\begin{aligned} \text{Linke Seite:} \quad & (a_1b_1+a_2b_2)^2 \;=\; a_1^2b_1^2 + 2a_1b_1a_2b_2 + a_2^2b_2^2 \;, \\ \text{Rechte Seite:} \quad & (a_1^2+a_2^2)(b_1^2+b_2^2) \;=\; a_1^2b_1^2 + a_1^2b_2^2 + a_2^2b_1^2 + a_2^2b_2^2 \;. \end{aligned}$$

Nach dem Vergleich der beiden Seiten ist (12.3) äquivalent zu

$$2a_1b_1a_2b_2 \;\leq\; a_1^2b_2^2 + a_2^2b_1^2 \;.$$

Wir subtrahieren $2a_1a_2b_1b_2$ von beiden Seiten und erhalten

$$0 \;\leq\; a_1^2b_2^2 + a_2^2b_1^2 - 2a_1a_2b_1b_2 \;=\; (a_1b_2 - a_2b_1)^2 \;.$$

Damit sind wir fertig. □

Korollar 12.59. *Es seien a, b reelle Zahlen. Dann gilt*

$$(a+b)(\frac{1}{a}+\frac{1}{b}) \;\geq\; 4 \;.$$

Beweis. Wir wenden die Proposition 12.58 an mit der Rollenverteilung

$$a_1 \;=\; \sqrt{a} \;,\; a_2 \;=\; \sqrt{b} \;,\; b_1 \;=\; \frac{1}{\sqrt{a}} \;,\; b_2 \;=\; \frac{1}{\sqrt{b}} \;.$$

Dann erhalten wir nämlich

$$(a_1b_1+a_2b_2)^2 \;=\; \left(\sqrt{a}\cdot\frac{1}{\sqrt{a}} + \sqrt{b}\cdot\frac{1}{\sqrt{b}}\right)^2 \;=\; (1+1)^2 \;=\; 4 \;,$$

und

$$\begin{aligned}(a_1^2+a_2^2)(b_1^2+b_2^2) &= \left((\sqrt{a})^2+(\sqrt{b})^2\right)\cdot\left(\left(\frac{1}{\sqrt{a}}\right)^2+\left(\frac{1}{\sqrt{b}}\right)^2\right)\\ &= (a+b)\cdot\left(\frac{1}{a}+\frac{1}{b}\right)\ ,\end{aligned}$$

und wir sind wegen der Cauchy–Schwarz-Ungleichung fertig. □

Satz 12.60 (Cauchy–Schwarz-Ungleichung)**.** *Es seien $a_1,\dots,a_n$ und $b_1,\dots,b_n$ reelle Zahlen. Dann gilt*

$$\left(\sum_{i=1}^n a_ib_i\right)^2 \le \left(\sum_{i=1}^n a_i^2\right)\cdot\left(\sum_{i=1}^n b_i^2\right)\ .$$

(A) **12.61.** *Schreiben Sie den Fall $n=3$ konkret hin.*

Korollar 12.62. *Es seien $a,b,c>0$. Dann gilt*

$$(a+b+c)^2 \le 3(a^2+b^2+c^2)\ .$$

Beweis. Wir wenden die Cauchy-Schwarz-Ungleichung (im Fall $n=3$) für die Tripel

$$a,b,c \quad\text{und}\quad 1,1,1$$

an. Daraus ergibt sich

$$(a\cdot 1+b\cdot 1+c\cdot 1)^2 \overset{\text{C-S}}{\le} (a^2+b^2+c^2)(1^2+1^2+1^2)\ ,$$

was genau die gewünsche Ungleichung ist. □

Bemerkung 12.63 (Dreiecks-Ungleichung im $\mathbb{R}^3$). (*) Hier erklären wir die fundamentale geometrische Signifikanz der Cauchy-Schwarz-Ungleichung. Für diese Bemerkung betrachten wir 'Vektoren' aus $\mathbb{R}^3$, das heißt, Elemente $v=(v_1,v_2,v_3)\in\mathbb{R}^3$. Man definiert das Skalarprodukt von zwei Vektoren $v=(v_1,v_2,v_3), w=(w_1,w_2,w_3)\in\mathbb{R}^3$ als

$$v\cdot w \overset{\text{def}}{=} v_1w_1+v_2w_2+v_3w_3\in\mathbb{R}\ .$$

Das Skalarprodukt besitzt die folgenden Eigenschaften:

(1) $v\cdot v\ge 0$ für jeden Vektor $v\in\mathbb{R}^3$ und $v\cdot v=0$ genau dann, wenn $v=0$;
(2) $v\cdot w = w\cdot v$ für alle Vektoren $v,w\in\mathbb{R}^3$;
(3) $v\cdot(w_1+w_2)=v\cdot w_1+v\cdot w_2$ für alle $v,w_1,w_2\in\mathbb{R}^3$.

Desweiteren hat die Cauchy-Schwarz-Ungleichung eine sehr wichtige Konsequenz (auch Cauchy-Schwarz-Ungleichung genannt): für beliebige Vektoren v,w gilt

$$(v,w)^2 \le (v,v)\cdot(w,w)\ .$$

Aufbauend auf diesem Begriff können wir viele geometrische Begriffe, zum Beispiel Länge, Distanz, und Winkel von Vektoren definieren. Die *Länge von v* wird als

$$\|v\| \overset{\text{def}}{=} \sqrt{v\cdot v}\ .$$

definiert. Aus den obigen Eigenschaften des Skalarprodukt erfolgen wichtige Beobachtungen für die Länge eines Vektors.

(1) $\|v\|\ge 0$ und $\|v\|=0$ genau dann, wenn $v=0\in\mathbb{R}^3$ ist.
(2) $\|\lambda v\| = |\lambda|\cdot\|v\|$ für alle $\lambda\in\mathbb{R}$ und $v\in\mathbb{R}^3$.

(3) ('Vorfahre' der Dreiecks-Ungleichung) für beliebige Vektoren $v, w \in \mathbb{R}^3$ gilt

$$\|v + w\| \leq \|v\| + \|w\| \ . \tag{12.4}$$

Wir werden jetzt zeigen, wie die Ungleichung $\|v+w\| \leq \|v\| + \|w\|$ aus Cauchy–Schwarz folgt. Da beide Seiten von (12.4) nicht-negativ sind, ist Quadrieren eine äquivalente Umformung. Dadurch erhalten wir

$$\|v + w\|^2 \overset{\text{C-S}}{\leq} (\|v\| + \|w\|)^2$$

Die linke Seite ist

$$\|v + w\|^2 = (v + w, v + w) = (v, v) + 2(v, w) + (w, w) \ ,$$

die rechte Seite

$$(\|v\| + \|w\|)^2 = \|v\|^2 + 2\|v\| \cdot \|w\| + \|w\|^2 = (v, v) + 2\|v\| \cdot \|w\| + (w, w) \ .$$

Es folgt

$$(v, v) + 2(v, w) + (w, w) \leq (v, v) + 2\|v\| \cdot \|w\| + (w, w) \ ,$$

oder äquivalent

$$(v, w) \leq \|v\| \cdot \|w\| = \sqrt{(v, v)} \cdot \sqrt{(w, w)} \ .$$

Falls die linke Seite negativ ist, dann sind wir fertig. Falls nicht-negativ, dann ist Quadrieren wieder eine äquivalente Umformung:

$$(v, w)^2 \leq (v, v) \cdot (w, w) \ .$$

Jetzt, nachdem wir die Begriffe von Skalarprodukt und Länge hinter uns haben, können wir den Abstand von zwei Vektoren definieren: Für $v, w \in \mathbb{R}^3$ definieren wir

$$d(v, w) \overset{\text{def}}{=} \|v - w\| \ .$$

Man kann schnell nachrechnen, dass unser Abstandbegriff $d\colon \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}_{\geq 0}$ erfüllt und die folgenden erwarteten Eigenschaften hat: Für Vektoren $x, y, z \in \mathbb{R}^3$ gilt

(1) $d(x, y) \geq 0$ mit $d(x, y) = 0$ genau dann, wenn $x = y$,
(2) $d(x, y) = d(y, x)$ und
(3) (Dreiecks-Ungleichung) $d(x, y) \leq d(x, z) + d(z, y)$.

Die Dreiecks-Ungleichung folgt sofort aus (12.4) mit $v \overset{\text{def}}{=} x - z$ und $w \overset{\text{def}}{=} z - y$.

12.4. **Wiederholungsaufgaben.**

Hausaufgabe 12.64. *Bestimmen Sie per Hand welche Zahl größer ist: 2^{500} oder 3^{300}.*

Hausaufgabe 12.65. *Es seien $0 < a, b, c, d$ reelle Zahlen. Beweisen Sie die folgenden Ungleichungen:*

(1) *$\frac{a}{b} < \frac{c}{d}$ genau dann, wenn $ad < bd$;*
(2) *Falls $\frac{a}{b} < \frac{c}{d}$, dann $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$.*

Hausaufgabe 12.66. *Lösen Sie die Ungleichung*

$$|3x - 1| - |2x + 4| \leq 2$$

innerhalb der reellen Zahlen.

Hausaufgabe 12.67. *Wie groß kann die Fläche eines rechteckigen Grundstücks sein, falls der Umfang 240 Meter ist?*

Hausaufgabe 12.68. *Alice und Bob arbeiten im Supermarkt neben dem Studium. Im Jahr 2018 haben beide monatlich nach Steuer 500 Euro bekommen, im Jahr 2020 schon 720 Euro. Der monatliche Nettolohn von Alice in 2019 und 2020 ist um die gleiche Summe gestiegen. Für Bob war es aber anders: Er hat in 2019 soviel Mal mehr bekommen (im Verhältnis zu 2018), wie im Verhältnis von 2020 zu 2019. Wie viel haben Alice und Bob im Jahr 2019 monatlich verdient?*

Hausaufgabe 12.69. *Es sei ABC ein Dreieck mit einem Rechteck bei dem Eckpunkt B. Angenommen $|AB| + |BC| = 20$, wie groß kann die Fläche des Dreiecks sein?*

Hausaufgabe 12.70. *Beweisen Sie die Ungleichung*

$$2 \leq \frac{a^2 + b^2 + 1}{\sqrt{a^2 + b^2}}$$

für beliebige reelle Zahlen $a, b > 0$.

Hausaufgabe 12.71. *Im Dorf gibt es ein rechteckiges Feld mit einer Oberfläche von* 10000 *Quadratmetern. Wie lang kann die Diagonale sein? Wie groß kann der Umfang sein?*

Hausaufgabe 12.72. *Es seien a, b, c reelle Zahlen. Dann gilt*

$$a^2 + b^2 + c^2 \geq ab + bc + ca \ .$$

12.5. **Weiterführende Literatur.**

(1) Fritsche: Mathematik für Einsteiger

13. Konvergenz von Folgen

13.1. **Wiederholung.** Das Material über Abbildungen aus ELMA I., vollständige Induktion, rationale Funktionen.

Leitfrage. *Konvergiert die Zahlenfolge*

$$\frac{2n^2+3n+5}{3n^2+n+\pi n}?$$

Falls ja, wie kann man ihren Grenzwert bestimmen?

13.2. **Folgen.** Grob gesagt beschreiben Zahlenfolgen Folgen von Beobachtungen, zum Beispiel wie viel Kleingeld an einem gegebenen Tag in meiner Tasche ist. Hierbei arbeiten wir mit der Abstraktion / Annahme, dass wir für jede natürliche Zahl einen Wert haben werden und somit ersetzen wir 'sehr groß' durch 'beliebig groß' und sogar 'unendlich'.

Eine 'Folge' kann a priori eine Folge von beliebigen Objekten sein, hier werden wir uns nur mit Folgen von Zahlen beschäftigen und daher meinen wir mit 'Folge' immer eine Folge von Zahlen.

Beispiel 13.1. Man schreibe a_n für die Anzahl der Corona-infizierten Menschen in Deutschland am Tag n, wenn Tag 1 der 1.1.2020 ist.

Definition 13.2 (Zahlenfolgen)**.** Eine *Folge von reellen Zahlen* ist eine Abbildung $a\colon \mathbb{N}_+ \to \mathbb{R}$. In diesem Zusammenhang schreiben wir oft a_n für $a(n)$. Manchmal schreibt man (a_n) oder $(a_n)_{n\in\mathbb{N}_+}$ für eine Zahlenfolge.

Beispiel 13.3. Im folgenden geben wir viele Beispiele von Zahlenfolgen an.

(1) $a_n = 0$ für alle $n \in \mathbb{N}_+$.
(2) $a_n = 1$ für alle $n \in \mathbb{N}_+$.
(3) $a_n = n$ für alle $n \in \mathbb{N}_+$.
(4) $a_n = (-1)^n$ für alle $n \in \mathbb{N}_+$.
(5) $a_n = 2^n$ für alle $n \in \mathbb{N}$.
(6) $a_n = 2n^2 + 3n - 1$ für alle $n \in \mathbb{N}_+$.

Bemerkung 13.4. Folgen, die nur einen Wert annehmen, nennen wir konstante Folgen.

(A) **13.5.** *Berechnen Sie die ersten fünf Elementen (in anderen Worten $a(1), \dots, a(5)$) aller Folgen in Beispiel 13.3.*

Beispiel 13.6. Jedes Polynom oder allgemeiner, jede rationale Funktion ohne Polstellen in den positiven ganzen Zahlen, bestimmt eine Folge. Für $f \in \mathbb{R}(X)$ ist diese Folge

$$a_f(n) \stackrel{\text{def}}{=} f(n)\ .$$

Zum Beispiel für $f(X) = \frac{3X-1}{X^2+2}$ ist die Folge

$$a_f(n) = \frac{3n-1}{n^2+2}\ .$$

Ⓐ **13.7.** *Bestimmen Sie die ersten fünf Elemente der den folgenden rationalen Funktionen entsprechenden Folgen*

$$X^2 - 3X,\ \frac{1}{X+1},\ \frac{3X^2 - X + 1}{X - 3}\ .$$

Beispiel 13.8 (Arithmetische Folge). Es seien $a, d \in \mathbb{R}$. Die Folge

$$a_n \stackrel{\text{def}}{=} a + nd$$

heißt *arithmetische Folge*.

Beispiel 13.9 (Geometrische Folge). Es seien $c, q \in \mathbb{R}$, dann nennen wir die Folge

$$a_n \stackrel{\text{def}}{=} cq^n$$

eine *geometrische Folge*. Das Verhalten der Folge hängt stark davon ab, ob $q = 0$, $|q| > 1$, $|q| = 1$, oder $|q| < 1$ ist. Falls $q = 0, 1$, dann ist a_n eine konstante Folge. Im Fall $|q| < 1$ werden die Elementen im Betrag beliebig klein (wir werden im folgenden Abschnitt sehen, was das ganz präzise bedeutet). Im Fall $a > 0$ und $q > 1$ werden die a_n's beliebig groß.

Ⓐ **13.10.** *Schreiben Sie die geometrische Folge hin für $c = 1$, $q = -1$.*

Beispiel 13.11 (Harmonische Folge). Diese Folge definieren wir durch

$$a_n \stackrel{\text{def}}{=} \sum_{i=1}^{n} \frac{1}{i}\ ,$$

somit sind die ersten Elemente

$$a_1 = 1\ ,\ a_2 = 1 + \frac{1}{2} = \frac{3}{2},\ a_3 = 1 + \frac{1}{2} + \frac{1}{3} = \frac{11}{6}\ .$$

Es ist eine interessante Frage, ob die harmonische Folge eine obere Schranke hat, oder die Folgenglieder beliebig groß werden können.

Definition 13.12 (Operationen mit Zahlenfolgen)**.** Es seien $a, b\colon \mathbb{N}_+ \to \mathbb{R}$ Zahlenfolgen. Dann definieren wir die Addition, Subtraktion, Multiplikation, und Division von Folgen durch die entsprechende Operationen auf Abbildungen. Konkreter

(1) $a + b\colon \mathbb{N}_+ \to \mathbb{R}$ ist durch $(a + b)(n) \stackrel{\text{def}}{=} a(n) + b(n)$ gegeben,
(2) $a - b\colon \mathbb{N}_+ \to \mathbb{R}$ ist durch $(a - b)(n) \stackrel{\text{def}}{=} a(n) - b(n)$ gegeben,
(3) $a \cdot b\colon \mathbb{N}_+ \to \mathbb{R}$ ist durch $(a \cdot b)(n) \stackrel{\text{def}}{=} a(n) \cdot b(n)$ gegeben, und
(4) falls $b(n) \neq 0$ für alle $n \in \mathbb{N}_+$, dann ist $(a/b)(n) \stackrel{\text{def}}{=} a(n)/b(n)$.

Ⓐ **13.13.** *Betrachten Sie die Folgen*

$$a_n = \frac{1}{n}\ ,\ b_n = n^2 - 2n\ ,\ c_n = 3 + n\ .$$

Berechnen Sie $a_n \pm b_n$, $a_n \cdot b_n$ und b_n/c_n.

Lemma 13.14. *Es gelten die üblichen Gesetze für die arithmetischen Operationen von Folgen.*

Beweis. Alles folgt aus der Tatsache, dass die gewünschten Eigenschaften punktweise richtig sind. □

Bemerkung 13.15. Wir können die Elemente einer Zahlenfolge beliebig vermischen. Das heißt, für jede bijektive Abbildung $\phi\colon \mathbb{N}_+ \to \mathbb{N}_+$ und jede Folge reeller Zahlen $a\colon \mathbb{N}_+ \to \mathbb{R}$ ist

$$a \circ \phi\colon \mathbb{N}_+ \to \mathbb{R}$$

ebenfalls eine Zahlenfolge.

Definition 13.16 (Beschränkte Folgen)**.** Eine Folge $a\colon \mathbb{N}_+ \to \mathbb{R}$ heißt *von oben beschränkt*, falls eine Zahl M existiert, für welche gilt

$$a_n \leq M \quad \text{für jedes } n \in \mathbb{N}_+.$$

Die Folge a_n heißt *von unten beschränkt*, falls eine Zahl M' existiert, für welche gilt

$$a_n \geq M' \quad \text{für jedes } n \in \mathbb{N}_+.$$

Wir nennen eine Folge *beschränkt*, falls sie von oben und von unten beschränkt ist.

Bemerkung 13.17. Eine Folge $a \cdot \mathbb{N}_+ \to \mathbb{R}$ is genau dann beschränkt, wenn es eine Zahl M'' gibt, für welche gilt

$$|a_n| \leq M'' \quad \text{für jedes } n \in \mathbb{N}_+.$$

(A) **13.18.** *Betrachten Sie alle Beispiele von Folgen in diesem Abschnitt und entscheiden Sie in jedem Fall, ob diese von oben beschränkt/von unten beschränkt/beschränkt sind.*

Hausaufgabe 13.19. *Es sein $a\colon \mathbb{N}_+ \to \mathbb{R}$ eine beschränkte Folge, $\phi\colon \mathbb{N}_+ \to \mathbb{N}_+$ eine bijektive Abbildung. Dann ist auch die Folge $a \circ \phi$ beschränkt.*

Definition 13.20 (Monotone Folgen)**.** Eine Zahlenfolge a_n heißt *monoton wachsend/streng monoton wachsend*, falls für jedes $n \in \mathbb{N}_+$ die Ungleichung $a_n \leq a_{n+1}$ bzw. $a_n < a_{n+1}$ gilt. Eine Zahlenfolge a_n heißt *monoton fallend/streng monoton fallend*, falls für jedes $n \in \mathbb{N}_+$ die Ungleichung $a_n \geq a_{n+1}$ bzw. $a_n > a_{n+1}$ gilt.

Beispiel 13.21. Die konstante Folge $a_n = 1$ ist (wie jede andere konstante Folge) monoton wachsend und monoton fallend zugleich. Umgekehrt ist eine Folge, die monton wachsend und monoton fallend ist, eine konstante Folge.

Die Folge $a_n = n$ ist streng monoton wachsend, $a_n = -n$ ist streng monoton fallend.

(A) **13.22.** *Zeigen Sie, dass eine Folge a_n genau dann monoton wachsend ist, wenn die Folge $-a_n$ monoton fällt.*

(A) **13.23.** *Für welche Werte von a und d ist die arithmetische Folge $a_n = a + dn$ monoton wachsend/streng monoton wachsend/monoton fallend/streng monoton fallend? Fangen Sie mit konkreten Beispielen an!*

Hausaufgabe 13.24. *Für welche Werte von c und q ist die geometrische Folge $a_n = cq^n$ monoton wachsend/streng monoton wachsend/monoton fallend/streng monoton fallend?*

Hausaufgabe 13.25. *Es sei a_n eine monoton wachsende/fallende Folge und $k \in \mathbb{N}_+$ beliebig. Dann gilt $a_n \leq a_{n+k}$ / $a_n \geq a_{n+k}$ für jede $n \in \mathbb{N}_+$.*

(A) **13.26.** *Finden Sie die monoton wachsenden und monoton fallenden Folgen aus den Beispielen in diesem Abschnitt.*

(A) **13.27.** *Ist die harmonische Folge monoton wachsend?*

Oft möchte man sich nur mit einigen Elementen einer gewissen Folge, sagen wir z.B. mit jedem zweiten, beschäftigen. Dieser Wunsch führt uns zum Begriff einer Teilfolge.

Definition 13.28 (Teilfolge)**.** Es sei $a\colon \mathbb{N}_+ \to \mathbb{R}$ ein Zahlenfolge. Eine *Teilfolge von* a ist eine Zahlenfolge der Form $a \circ \psi$, wobei $\psi\colon \mathbb{N}_+ \to \mathbb{N}_+$ eine streng monoton wachsende Abbildung ist (d.h. $n < m$ impliziert $\psi(n) < \psi(m)$ für alle $n, m \in \mathbb{N}_+$). Schreibt man a_n für die Zahlenfolge, schreiben wir $a_{\psi(n)}$ für die entsprechende Teilfolge.

Bemerkung 13.29. Eine streng monoton wachsende Abbildung ist immer injektiv.

(A) **13.30.** *Zeigen Sie, dass eine streng monoton wachsende Abbildung injektiv ist.*

Beispiel 13.31. Betrachten wir die Folge $a_n = (-1)^n$. Die Folgenglieder sind

$$-1, 1, -1, 1, -1, \dots \ .$$

Uns interessiert die Teilfolge, die aus jedem zweiten Element besteht, das heisst, wir wollen

$$1, 1, 1, 1, \dots$$

erhalten. Unser Wunsch wir durch die Abbildung

$$\psi\colon \mathbb{N}_+ \to \mathbb{N}_+ \quad n \mapsto 2n$$

zum Leben erweckt, insbesondere gilt $a_{2n} = 1$ für jede $n \in \mathbb{N}_+$.

Lemma 13.32. *Es sei $a\colon \mathbb{N}_+ \to \mathbb{R}$ eine Zahlenfolge, $\psi\colon \mathbb{N}_+ \to \mathbb{N}_+$ eine streng monoton wachsende Abbildung.*

(1) *Falls a beschränkt ist, dann auch $a \circ \psi$.*
(2) *Falls a monoton wachsend/streng monoton wachsend/monoton fallend/streng monoton fallend ist, dann besitzt $a \circ \psi$ die gleiche Eigenschaft.*

Beweis. (1) Es sei $M > 0$ eine Zahl für welche $|a_n| \leq M$ ist für alle $n \in \mathbb{N}_+$. Dann gilt $|a_{\psi(n)}| \leq M$ für alle $n \in \mathbb{N}_+$, da alle Elemente von $a \circ \psi$ auch Elemente von a sind. Somit ist auch $a \circ \psi$ beschränkt.

(2) Wir betrachten den Fall, wenn a monoton wachsend ist, alle andere Fälle lassen sich ähnlich beweisen. Es sei $n \in \mathbb{N}_+$ beliebig. Wir sollen zeigen, dass $(a \circ \psi)(n) \leq (a \circ \psi)(n+1)$ gilt. Es gilt $k \stackrel{\text{def}}{=} \psi(n+1) - \psi(n) > 0$, weil ψ streng monoton wachsend ist. Da a monoton wachsend ist, gilt

$$(a \circ \psi)(n) \ = \ a(\psi(n)) \ \leq \ a(\psi(n) + k) \ = \ a(\psi(n+1)) \ = \ (a \circ \psi)(n+1) \ ,$$

wie gewollt.

□

(A) **13.33.** *Betrachten Sie die arithmetische Folge $a_n = 2 + 3n$. Finden Sie Teilfolgen, die ebenfalls arithmetische Folgen sind und finden Sie Teilfolgen, die es nicht sind. Finden Sie eine Regelmäßigkeit?*

Die folgende Aussage ergibt eine nicht-triviale Eigenschaft von Zahlenfolgen. Der Beweis ist elementar, aber weit von trivial entfernt.

Satz 13.34. *Jede Zahlenfolge enthält eine monotone Teilfolge.*

Beweis. (*) □

13.3. **Konvergenz von Folgen.** Wir möchten so oft wie möglich statt Folgen lieber mit Zahlen arbeiten. Deswegen suche wir zu Folgen Zahlen, die sie möglichst gut beschreiben. Wir werden sehen, dass das nicht immer möglich ist, aber falls schon, dann erhalten wir ein sehr gutes Werkzeug. Unsere Überlegungen beruhen auf dem folgende Axiom der reellen Zahlen.

Axiom 13.35 (Archimedisches Axiom)**.** *Für jede reelle Zahl α existiert eine natürliche Zahl n mit $n > \alpha$.*

Das Archimedische Axiom verwenden wir häufig in der folgenden äquivalenten Form.

Korollar 13.36. *Für jede reelle Zahl $\epsilon > 0$ existiert eine positive ganze Zahl n, sodass*

$$0 < \frac{1}{n} < \epsilon \ .$$

Dieses Korollar besagt, dass es keine 'kleinste positive reelle Zahl' gibt.

Beweis. Für die reellen Zahlen n und ϵ sind die Aussagen $\frac{1}{n} < \epsilon$ und $\frac{1}{\epsilon} < n$ äquivalent. Letzteres ist das Archimedische Axiom mit $\alpha \stackrel{\text{def}}{=} \frac{1}{\epsilon}$. □

Die folgende Definition ist fundamental für die ganze Mathematik und die Natur- und Ingenieurwissenschaften. Sie beschreibt Folgen, die von einer einzigen Zahl gut bestimmt werden.

Definition 13.37 (Konvergenz von Folgen)**.** Es sein (a_n) eine Folge reeller Zahlen. Wir sagen, dass (a_n) *konvergent* ist, falls eine Zahl $A \in \mathbb{R}$ mit der folgenden Eigenschaft existiert: Für jedes $\epsilon > 0$ existiert ein $N_\epsilon \in \mathbb{N}_+$, sodass

$$|A - a_n| < \epsilon \quad \text{falls } n \geq N_\epsilon.$$

Ist dies gegeben, dann nennen wir die Zahl A den *Grenzwert von* (a_n). Die Tatsache, dass die Folge (a_n) konvergent mit Grenzwert A ist notieren wir wie folgt: auch als

$$\lim_{n\to\infty} a_n \ = \ A.$$

Bemerkung 13.38. Man kann die Konvergenz von Folgen auch ohne Indizes formulieren: Eine Folge (a_n) ist konvergent mit Grenzwert A genau dann, wenn für jede positive reelle Zahl $\epsilon > 0$ nur endlich viele Elemente a_n der Folge (a_n) existieren, so dass $|a_n - A| \geq \epsilon$.

Beispiel 13.39. Eine konstante Folge $a_n = c$ für alle $n \in \mathbb{N}_+$ ist konvergent mit Grenzwert c.

Beispiel 13.40. Wir betrachten die Folge $a_n = \frac{1}{n}$. Wir werden zeigen, dass sie konvergent mit Grenzwert 0 ist, anders ausgedrückt $\frac{1}{n} \to 0$.

Es sei $\epsilon > 0$ eine beliebige reelle Zahl. Wir müssen einen Index $N_\epsilon \in \mathbb{N}_+$ suchen, so dass aus $n \geq N_\epsilon$

$$\left|\frac{1}{n} - 0\right| < \epsilon$$

folgt. Es gilt

$$\left|\frac{1}{n} - 0\right| \ = \ \left|\frac{1}{n}\right| \ = \ \frac{1}{n} \ ,$$

und

$$\frac{1}{n} < \epsilon \quad \Leftrightarrow \quad n > \frac{1}{\epsilon} \ .$$

Es reicht also $N_\epsilon \stackrel{\text{def}}{=} \lceil \frac{1}{\epsilon} \rceil$ zu wählen. Da es uns gelungen ist, für jede $\epsilon > 0$ ein passendes N_ϵ zu finden, haben wir bewiesen, dass $\frac{1}{n} \to 0$.

Proposition 13.41. *Es seien (a_n) und (b_n) Zahlenfolgen, die sich auf endlich vielen Stellen unterscheiden. Dann ist (a_n) genau dann konvergent, wenn (b_n) konvergent ist und unter dieser Annahme gilt*

$$\lim_{n\to\infty} a_n \;=\; \lim_{n\to\infty} b_n \;.$$

Beweis. (*) □

Bemerkung 13.42. Im Licht von Proposition 13.41 ist die folgende Eigenschaft 'besser' als konstant zu sein: Eine Zahlenfolge heißt *quasikonstant* oder *quasistationär*, wenn sie irgendwann konstant wird. Das heißt, es existiert ein $N \in \mathbb{N}_+$, sodass $a_n = a_N$ für alle $n \geq N$. Zum Beispiel ist die Folge

$$a_n \;=\; \begin{cases} 2 & \text{für } 1 \leq n \leq 10 \\ 1 & \text{für } n \geq 11 \end{cases}$$

quasistationär.

(A) **13.43.** *Beweisen Sie, dass jede quasistationäre Folge konvergent ist.*

Die folgende Aussage ist spannend: Egal wie die Folgenglieder einer konvergenten Folge vertauscht werden, die Konvergenz bleibt erhalten.

Proposition 13.44. *Es sei $a\colon \mathbb{N}_+ \to \mathbb{R}$ eine konvergente Zahlenfolge mit Grenzwert A und $\phi\colon \mathbb{N}_+ \to \mathbb{N}_+$ eine bijektive Abbildung. Dann ist auch die Folge $a \circ \phi\colon \mathbb{N}_+ \to \mathbb{R}$ konvergent mit Grenzwert A.*

Beweis. (*) □

Proposition 13.45. *Es seien $(a_n), (b_n)$ konvergente Zahlenfolgen mit $(a_n) \to A$ und $(b_n) \to B$. Dann gelten die folgenden Grenzwertsätze:*

(1) *$(a_n + b_n)$ ist konvergent mit $(a_n + b_n) \to A + B$;*
(2) *$(a_n - b_n)$ ist konvergent mit $(a_n - b_n) \to A - B$;*
(3) *für eine beliebige Zahl $c \in \mathbb{R}$ ist (ca_n) konvergent mit $(ca_n) \to cA$;*
(4) *$(a_n b_n)$ ist konvergent mit $(a_n b_n) \to AB$;*
(5) *falls $B \neq 0$ und $b_n \neq 0$ für alle $n \in \mathbb{N}_+$, dann ist auch $(\frac{a_n}{b_n})$ konvergent und $(\frac{a_n}{b_n}) \to \frac{A}{B}$.*

Beweis. (1) Aus der Annahme $(a_n) \to A$ und $(b_n) \to B$ folgt, dass für jedes $\epsilon > 0$ Indizes $N_a, N_b \in \mathbb{N}_+$ existieren mit der Eigenschaft, dass

$$|a_n - A|, |b_n - B| < \epsilon \;\text{ für } n \geq N_a, N_b.$$

Wir werden jetzt untersuchen, was diese Beobachtung für die Folge $a_n + b_n$ bedeutet. Dazu betrachten wir die (positive) Differenz von $a_n + b_n$ und $A + B$:

$$\begin{aligned} |(a_n + b_n) - (A + B)| &= |(a_n - A) + (b_n - B)| \\ &\leq |a_n - A| + |b_n - B| \\ &< \epsilon + \epsilon = 2\epsilon \;\text{ für } n \geq N_a, N_b. \end{aligned}$$

Bei der ersten Ungleichung haben wir die Dreiecks-Ungleichung für den Absolutbetrag ausgenutzt, bei der zweiten unsere Wahl von N_a und N_b (und die Tatsache, dass so eine Wahl durch die Konvergenz $(a_n) \to A$ und $(b_n) \to B$ möglich ist).

Wenn wir am Anfang des ganzen Prozesses Indizes N'_a, N'_b wählen, sodass $|a_n - A|, |b_n - B| < \frac{\epsilon}{2}$ gilt für $n \geq N'_a, N'_b$, dann erhalten wir am Ende

$$|(a_n + b_n) - (A + B)| < \epsilon \quad \text{für } n \geq N'_a, N'_b$$

und damit ist die Aussage bewiesen.

(2) Der Beweis ist der gleiche wie für die Summe von Folgen.

(3) Diesen Beweis überlassen wir dem Leser.

(4) Erneut werden wir versuchen die Konvergenz von $(a_n b_n)$ auf die Konvergenz der Folgen $(a_n), (b_n)$ zurückzuführen. Dieses Mal fangen wir mit der Rechnung an und die Suche nach dem richtigen Index wird erst danach kommen:

$$\begin{aligned} |a_n b_n - AB| &= |a_n b_n - (a_n B - a_n B) - AB| \\ &= |(a_n b_n - a_n B) + (a_n B - AB)| \\ &= |a_n(b_n - B) + (a_n - A)B| \\ &\leq |a_n(b_n - B)| + |(a_n - A)B| \\ &= |a_n| \cdot |b_n - B| + |a_n - A| \cdot |B| \end{aligned}$$

Bei der Ungleichung haben wir die Dreiecks-Ungleichung für den Absolutbetrag benutzt und danach die Multiplikativität des Absolutbetrags.

Da die Folge (a_n) konvergent ist, ist sie auch beschränkt und somit existiert eine Zahl $M > 0$ mit $|a_n| \leq M$ für alle $n \in \mathbb{N}_+$. Es ergibt sich

$$|a_n b_n - AB| \leq M \cdot |b_n - B| + |a_n - A| \cdot |B| \ .$$

Falls wir die Differenz $|a_n b_n - AB|$ unter eine vorgegebene Zahl ϵ bekommen wollen, dann reicht es wenn

$$M \cdot |b_n - B| < \frac{\epsilon}{2} \quad \text{und} \quad |a_n - A| \cdot |B| < \frac{\epsilon}{2}$$

erfüllt sind. Diese zwei Ungleichungen ergeben die Aussage.

(5) (*)

□

(A) **13.46.** *Bestimmen Sie, welche der folgenden Folgen konvergent sind und für diejenigen, die es sind, bestimmen Sie die Grenzwerte:*

$$1 + \frac{1}{n} \ , \ 2 - \frac{2}{n} \ , \ \left(1 + \frac{1}{n}\right)\left(3 - \frac{4}{n}\right) \ .$$

Lemma 13.47. *Es seien $(a_n^{(1)}), \ldots, (a_n^{(k)})$ konvergente Folgen mit jeweiligen Grenzwerten $A_1, \ldots, A_k$. Dann gelten*

(1) *$(a_n^{(1)}) + \ldots + (a_n^{(k)})$ ist konvergent mit Grenzwert $A_1 + \ldots + A_k$,*

(2) *$(a_n^{(1)}) \cdot \ldots \cdot (a_n^{(k)})$ ist konvergent mit Grenzwert $A_1 \cdot \ldots \cdot A_k$.*

Beweis. Folgt aus Proposition 13.45 mittels vollständige Induktion über k. □

Beispiel 13.48. Es sei $\alpha \in \mathbb{R}$ und k eine positive ganze Zahl. Dann gilt

$$a_n = \frac{\alpha}{n^k} \to 0 \ .$$

Die Aussage folgt mit der Hilfe von Lemma 13.47.

Hausaufgabe 13.49. *Geben Sie einen direkten Beweis für Beispiel 13.48 mithilfe der Definition der Konvergenz.*

Hausaufgabe 13.50. *Schreiben Sie einen vollständigen Beweis für Proposition 13.45 Teil (2) und (3).*

Beispiel 13.51. Wir betrachten jetzt die Folge

$$a_n = \frac{n^2 - 100n + 2000}{2n^2 + 1} .$$

Weder der Zähler noch der Nenner ist als Folge gesehen konvergent (s. zum Beispiel Proposition 13.55 unten), Proposition 13.45 lässt sich also nicht direkt anwenden. Es hilft der folgende Trick:

$$a_n = \frac{n^2 - 100n + 2000}{2n^2 + 1} = \frac{n^2(1 - \frac{100}{n} + \frac{2000}{n^2})}{n^2(2 + \frac{1}{n^2})} = \frac{1 - \frac{100}{n} + \frac{2000}{n^2}}{2 + \frac{1}{n^2}} .$$

Die Folge $1 - \frac{100}{n} + \frac{2000}{n^2}$ ist laut Proposition 13.45 konvergent mit Grenzwert $1 - 0 + 0 = 1$, die Folge $2 + \frac{1}{n^2}$ ist aus dem gleichem Grund konvergent mit Grenzwert $2 - 0 = 2$. Aus Proposition 13.45 (4) folgt, dass

$$a_n = \frac{n^2 - 100n + 2000}{2n^2 + 1} = \frac{1 - \frac{100}{n} + \frac{2000}{n^2}}{2 + \frac{1}{n^2}}$$

konvergent ist mit Grenzwert $\frac{1}{2}$.

(A) **13.52.** *Bestimmen Sie den Grenzwert der Folge*

$$a_n = \frac{7n^3 - 12200n + 2000121}{4n^3 - n^2 + 1} .$$

Satz 13.53. *Es seien*

$$f(X) = a_d X^d + \ldots + a_0 \quad \textit{und} \quad g(X) = b_e X^e + \ldots + b_0$$

Polynome von Grad $d \geq 0$ und $e \geq 0$ (insbesondere gilt $a_d, b_e \neq 0$). Für die Folge

$$a_{f/g}(n) = \frac{a_d n^d + \ldots + a_0}{b_e n^e + \ldots + b_0}$$

haben wir die folgenden Möglichkeiten:

(1) *Falls $d > e$, dann ist die Folge $a_{f/g}(n)$ unbeschränkt, insbesondere nicht konvergent.*
(2) *Falls $d = e$, dann ist die Folge $a_{f/g}(n)$ konvergent mit Grenzwert*

$$\lim_{n\to\infty} a_{f/g}(n) = \frac{a_d}{b_e} .$$

(3) *Falls $d < e$, dann ist die Folge $a_{f/g}(n)$ eine Nullfolge, es heißt, sie ist konvergent und*

$$\lim_{n\to\infty} a_{f/g}(n) = 0 .$$

Beweis. (*) □

(A) **13.54.** *Verwenden Sie Satz 13.53 um zu bestimmen, welche der folgenden Folgen konvergent sind als auch zur Bestimmung der Grenzwerte:*

$$\frac{2n+1}{3-4n} , \quad \frac{n+1000}{n^2} , \quad \frac{100000n + 12345}{n^3} , \quad \frac{n^5}{10000n^4 + 1000000n^3 + 1} .$$

Proposition 13.55. *Es sei (a_n) eine konvergente Folge. Dann ist (a_n) auch beschränkt.*

Beweis. Nehmen wir an, dass $a_n \to A$ und wählen $\epsilon > 0$ beliebig (wir könnten zum Beispiel $\epsilon = 1$ wählen). Nach der Definition der Konvergenz gibt es einen Index $N_\epsilon \in \mathbb{N}_+$ mit

$$|a_n - A| < \epsilon \text{ falls } n \geq N_\epsilon.$$

Anders ausgedrückt gilt

$$A - \epsilon < a_n < A + \epsilon$$

für alle $n \geq N_\epsilon$. Daraus folgt dann

$$|a_n| \leq \max\{|A - \epsilon|, |A + \epsilon|\}$$

für alle $n \geq N_\epsilon$. Dann gilt aber auch

$$|a_n| \leq \max\{|a_1, \ldots, |a_{N_\epsilon - 1}|, |A - \epsilon|, |A + \epsilon|\}$$

für alle $n \geq 1$, was die Definition von beschränkt ist. □

Mittlerweile wissen wir, dass nicht alle beschränkte Folgen konvergent sind, ein gutes Beispiel ist die Folge $a_n = (-1)^n$.

Satz 13.56 (Monotone Konvergenz/Bolzano–Weierstraß)**.** (1) *Eine beschränkte und monoton wachsende (monoton fallende) Folge ist konvergent.*
(2) *Jede beschränkte Folge enthält eine konvergente Teilfolge.*

Beweis. (*) □

Beispiel 13.57 (Geometrische Folge)*.* Es sei $q \in \mathbb{R}$ eine reelle Zahl. Die geometrische Folge zur Basis q ist definiert als

$$a_n \stackrel{\text{def}}{=} q^n.$$

Anhand von konkreten Beispielen sieht man, dass sich die geometrische Folge sehr unterschiedlich verhalten kann, abhängig davon, was der Wert von q ist.

Zum Beispiel für $q = 0$ ist $q^n = 0^n = 0$ für alle $n \in \mathbb{N}_+$ und somit ist die entsprechende geometrische Folge die konstante Folge 0, daher konvergiert sie gegen 0. Im Fall $q = -1$ erhalten wir $q^n = (-1)^n$ und die Folge ist zwar beschränkt, konvergiert aber nicht. Falls $q = 1/2$, dann ist die Folge gegeben durch

$$1, \frac{1}{2}, \frac{1}{4}, \ldots, \frac{1}{2^n}, \ldots$$

und konvergiert auf ersten Blick gegen 0, was aber noch gezeigt werden müsste.

Das eigentliche Konvergenzverhalten der geometrischen Folge ist wie folgt

$$\begin{aligned} q^n = 1^n = 1 &\text{ konvergiert mit Grenzwert 1} && \text{falls} && q = 1\ , \\ q^n = (-1)^n &\text{ konvergiert nicht} && \text{falls} && q = -1\ , \\ q^n &\text{ konvergiert mit Grenzwert 0} && \text{falls} && |q| < 1\ , \\ q^n &\text{ konvergiert nicht} && \text{falls} && |q| > 1\ . \end{aligned}$$

13.4. **Eine sehr wichtige Folge.** In diesem Abschnitt werden wir die Folge

$$a_n \;=\; \left(1+\frac{1}{n}\right)^n$$

besser kennenlernen. Wir werden sehen, dass wir die Konvergenz von a_n nachweisen können, ohne den genauen Grenzwert zu kennen.

Proposition 13.58. *Für jede Zahl $n \in \mathbb{N}_+$ gilt*

$$2 \;\leq\; \left(1+\frac{1}{n}\right)^n \;\leq\; 4\ ,$$

insbesondere ist die Folge $\left(1+\frac{1}{n}\right)^n$ beschränkt.

Beweis. (*) □

Satz 13.59. *Die Folge*

$$a_n \;=\; \left(1+\frac{1}{n}\right)^n$$

ist streng monoton wachsend, und damit konvergent.

Beweis. (*) □

13.5. **Übungsaufgaben.**

13.6. **Weiterführende Literatur.**

Symbolenlegende

$\mathbb{N}$: die Menge der natürlichen Zahlen $0, 1, 2, \ldots$. Natürliche Zahlen sind die Anzahl von Elementen von endlichen Mengen. Da die leere Menge endlich ist, ist für uns $0 \in \mathbb{N}$.

$\mathbb{N}_+$: die Menge von positiven ganzen Zahlen, das heißt, $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. **Vorsicht:** in einigen Lehrbücher (und darunter viele deutschsprachigen) sind natürliche Zahlen so definiert, dass 0 *keine* natürliche Zahl ist. In solchen Büchern schreibt man $\mathbb{N}$ wo wir $\mathbb{N}_+$ schreiben würden, und $\mathbb{N}_0$ wo wir $\mathbb{N}$ schreiben würden. Bitte aufpassen.

$\mathbb{Z}$: die Menge der ganzen Zahlen $0, \pm 1, \pm 2, \ldots$. Wie gezeigt können Sie positiv, negativ, oder 0 sein. Unter den ganzen Zahlen kann man $+, -, \times$ ausführen, aber teilen ohne Rest geht nicht immer.

$\mathbb{Q}$: die Menge der rationalen Zahlen oder Brüche. Sie können ebenfalls positiv, negativ, oder 0 sein, und können immer in Bruchform a/b geschrieben werden, wobei $a, b \in \mathbb{Z}$, und $b \neq 0$ sein muß.

$\mathbb{R}$: die Menge der reellen Zahlen (alle Zahlen, die wir bisher kennengelernt haben). Sie können positiv, negativ, oder 0 sein. Es gibt viel mehr reelle Zahlen als rationale. Zum Beispiel ist $\sqrt{2} \in \mathbb{R}$, aber $\sqrt{2} \notin \mathbb{Q}$.

Literatur